Referentenentwurf

des Bundesministeriums des Innern

Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts

A. Problem und Ziel

Der Gesetzentwurf soll das Nachrichtendienstrecht umfassend reformieren und nachhaltig fortentwickeln.

B. Lösung

Der Gesetzentwurf verfolgt drei übergeordnete Ziele:

Zum einen sollen die Vorgaben der verfassungsgerichtlichen Rechtsprechung umgesetzt werden. Das Gericht hat seit 2022 grundlegende Vorgaben zum Nachrichtendienstrecht getroffen, die durch Neufassung der Gesetze aufgegriffen und weiterentwickelt werden.

Darüber hinaus sollen in Anbetracht der verschärften Bedrohungslage im In- und Ausland die Aufklärungs- und Weiterverarbeitungsfähigkeiten des Bundesamtes für Verfassungsschutz und des Bundesnachrichtendienstes modernisiert und gestärkt werden. Dies ist erforderlich, um den von der nachrichtendienstlichen Bedrohungsaufklärung bezweckten Schutz herausragender Rechtsgüter des Gemeinwohls umfassend zu gewährleisten.

Zudem soll die Kontrolle über die Tätigkeit der Nachrichtendienste gestärkt und effizienter ausgestaltet werden. Diesem Zweck dient die Zusammenführung der Kontrollzuständigkeiten beim Unabhängigen Kontrollrat, dessen Tätigkeit in dem Gesetz über die Rechtskontrolle durch den Unabhängigen Kontrollrat künftig in einem eigenen Stammgesetz geregelt wird.

Die zum Erreichen dieser Ziele notwendigen, umfassenden Änderungen bedingen die Neuverkündung von Bundesverfassungsschutzgesetz und Gesetz über den Bundesnachrichtendienst. Wie bereits im Gesetz über den Militärischen Abschirmdienst erfolgt, werden die Gesetze dabei entflochten, so dass im BND-Gesetz die bisherigen zum Teil wenig klaren Verweisungen auf das Bundesverfassungsschutzgesetz durch eigene, aufgabenspezifische Regelungen ersetzt.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Der Gesetzentwurf führt beim Bundesnachrichtendienst - soweit bezifferbar - zu einmaligen Haushaltsausgaben ohne Erfüllungsaufwand in Höhe von mindestens 40 Mio. Euro sowie jährlichen Haushaltsausgaben ohne Erfüllungsaufwand von mindestens 35 Mio. Euro pro Jahr. Letztere sind abhängig von der Entwicklung der weltweiten Krisen- und Bedrohungslagen und können höher ausfallen.

Der Mehrbedarf wird Gegenstand des Weiteren Haushaltsaufstellungsverfahrens zum geheimen Wirtschaftsplan des Bundesnachrichtendienstes und entsprechend zum Zuschusstitel an den Bundesnachrichtendienst (Kapitel 0414) für die Jahre 2027ff sein.

Der Gesetzentwurf führt beim Bundesamt für Verfassungsschutz - soweit bezifferbar - zu jährlichen Haushaltsausgaben ohne Erfüllungsaufwand in Höhe von rd. 2 Mio. €. Diese sind abhängig von der Entwicklung der inländischen Krisen- und Bedrohungslage und können höher ausfallen.

Der finanzielle Mehrbedarf des Bundesamts für Verfassungsschutz wird aus den vorhandenen Ansätzen des Bundesamts für Verfassungsschutz (Kapitel 0626) getragen.

Aufgrund der zusätzlichen Zuständigkeiten des Unabhängigen Kontrollrates und dem damit einhergehenden und notwendigen Aufwuchs der Verwaltungsinfrastruktur entstehen im Einzelplan 22 einmalige Ausgaben in Höhe von schätzungsweise 1,6 Mio. Euro. Dies beinhaltet vornehmlich Ausgaben im Bereich der IT-Infrastruktur und der erforderlichen Arbeitsmittel.

Die jährlichen Mehrausgaben im Einzelplan 22 werden auf ca. 8,86 Mio. Euro geschätzt, wobei hiervon ca. 0,91 Mio. Euro auf die entstehenden Personalkosten in der Verwaltung (zehn neue Dienstposten, davon sieben im höheren Dienst, zwei im gehobenen Dienst und einer im mittleren Dienst anfallen) und 1,30 Mio. Euro auf die erforderlichen Mittel für Sacheinzel- und Gemeinkosten und Versorgung entfallen.

Einsparungen ergeben sich demgegenüber durch den Wegfall der Zuständigkeiten der Bundesbeauftragten für den Datenschutz (Einzelplan 21) und die Informationsfreiheit und der G10-Kommission (Einzelplan 02, Kapitel 0216). Diese sind im Rahmen der Haushaltsaufstellung zu prüfen.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht kein zusätzlicher Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entstehen zusätzliche Aufwände durch das Bedienen von Ersuchen des Bundesnachrichtendienstes (§§ 12ff.) in Höhe von etwa 50 T Euro pro Jahr. Die Aufwände werden erstattet.

Beim Bundesamt für Verfassungsschutz sind für die Ersuchen keine validen Schätzungen möglich, aber auch hier werden Aufwände – wie beim BND – erstattet.

E.3 Erfüllungsaufwand der Verwaltung

Für die Anpassung der IT-Strukturen entstehen im Bundesnachrichtendienst einmalige Erfüllungsaufwände im Umfang von etwa 40 Mio. Euro Nach erfolgter Anpassung der IT-Strukturen entstehen zugehörige betriebliche Aufwände im Umfang von jährlich etwa 15 Mio. Euro. Zudem besteht bereits ab Inkrafttreten des Gesetzes ein jährlicher Erfüllungsaufwand von ebenfalls etwa 20 Mio. Euro, insbesondere zur Umsetzung der neuen Befugnisse im Bereich der Eigensicherung. Der jährliche Erfüllungsaufwand ist abhängig von der Entwicklung der weltweiten Krisen- und Bedrohungslagen und kann höher ausfallen. Mit

der Umsetzung des Gesetzes entstehen personelle und finanzielle (Mehr-)Aufwände bei dem Unabhängigen Kontrollrat.

Der Erfüllungsaufwand für den Unabhängigen Kontrollrat wird auf einmalig 1,6 Mio. Euro und jährlich 6,65 Mio. Euro geschätzt.

Für die Anpassung der IT-Strukturen entstehen beim Bundesamt für Verfassungsschutz einmalige Erfüllungsaufwände im Umfang von rd. 94 Mio. €. Nach erfolgter Anpassung der IT-Strukturen entstehen zugehörige betriebliche Aufwände im Umfang von jährlich etwa 269 Mio. €. Zudem besteht bereits ab Inkrafttreten des Gesetzes ein einmaliger Erfüllungsaufwand von rd. 51 Mio. €, insbesondere zur Umsetzung der neuen Befugnisse im Bereich der Eigensicherung. Ferner entstehen dem Bundesamt für Verfassungsschutz zusätzliche Erfüllungsaufwände in Höhe von rd. 25 Mio. € jährlichen Personalkosten sowie rd. 8 Mio. € jährlichen Sacheinzelkosten. Der jährliche Erfüllungsaufwand ist abhängig von der Entwicklung der inländischen Krisen- und Bedrohungslage und kann höher ausfallen.

Das Gesetz veranlasst keinen Erfüllungsaufwand im Landesvollzug.

F. Weitere Kosten

Der Gesetzentwurf wirkt sich nicht auf sonstige Kosten für die Wirtschaft, Kosten für soziale Sicherungssysteme, Auswirkungen auf Einzelpreise und das Preisniveau, insbesondere auf das Verbraucherpreisniveau, aus.

Referentenentwurf des Bundesministeriums des Innern

Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Inhaltsübersicht

Artikel 1 Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG)

Artikel 2 Gesetz über den Bundesnachrichtendienst (BND-Gesetz – BNDG)

Artikel 3 Gesetz über die Rechtskontrolle durch den Unabhängigen Kontrollrat (UKRat-Gesetz – UKRatG)

Artikel 4 Änderung des Bundesverfassungsschutzgesetzes zum 1. Januar 2030

Artikel 5 Änderung des Gesetzes über die Kontrolle von Kriegswaffen

Artikel 6 Änderung des Informationsfreiheitsgesetzes

Artikel 7 Änderung des Beamtenversorgungsgesetzes

Artikel 8 Änderung des Bundesbesoldungsgesetzes

Artikel 9 Änderung des Bundespersonalvertretungsgesetzes

Artikel 10 Änderung des Vereinsgesetzes

Artikel 11 Änderung des Bundeskriminalamtgesetzes

Artikel 12 Änderung des Hochschulstatistikgesetzes

Artikel 13 Änderung des Aufenthaltsgesetzes

Artikel 14 Änderung der Verwaltungsgerichtsordnung

Artikel 15 Änderung der Abgabenordnung

Artikel 16 Änderung des Zollverwaltungsgesetzes

Artikel 17 Änderung des Geldwäschegesetzes

Artikel 18 Änderung des Zehnten Buches Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz

Artikel 19 Folgeänderungen …

Artikel 20 Außerkrafttreten

Artikel 21 Inkrafttreten

Anlage 1 (zu § 48 Absatz 2 Nummer 2 BVerfSchG)

Anlage 2 (zu § 81 Absatz 2 Nummer 2 BNDG)

Artikel 1

Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz

(Bundesverfassungsschutzgesetz – BVerfSchG)

Inhaltsübersicht

Abschnitt 1
Aufgaben und Zusammenarbeit der Verfassungsschutzbehörden

§ 1 Zusammenarbeitspflicht

§ 2 Aufgaben der Verfassungsschutzbehörden

§ 3 Begriffsbestimmungen

§ 4 Bedrohungsaufklärung durch das Bundesamt für Verfassungsschutz

§ 5 Zentralstellenaufgaben des Bundesamtes für Verfassungsschutz

§ 6 Gegenseitige Unterrichtung der Verfassungsschutzbehörden; nachrichtendienstliches Informationssystem

§ 7 Weisungsrechte des Bundes

Abschnitt 2
Aufklärung

Unterabschnitt 1
Allgemeine Informationsgewinnung, Mitwirkungspflichten

§ 8 Allgemeine Datenerhebung

§ 9 Datenerhebung bei Dritten

§ 10 Übermittlung durch inländische öffentliche Stellen

§ 11 Verpflichtende Ersuchen an geschäftsmäßige Diensteanbieter

§ 12 Verpflichtende Ersuchen bei informationstechnischen Angriffen

§ 13 Verpflichtende Ersuchen an Anbieter von Telekommunikationsdiensten

§ 14 Verpflichtende Ersuchen an Anbieter von Postdiensten

§ 15 Verpflichtende Ersuchen an Verfügungsberechtigte von Einrichtungen zur Videoüberwachung

Unterabschnitt 2
Nachrichtendienstliche Mittel

§ 16 Datenerhebungen mit nachrichtendienstlichen Mitteln

§ 17 Internetermittlungen auf vertiefter Vertrauensbasis

§ 18 Vertrauenspersonen

§ 19 Verdeckte Bedienstete

§ 20 Längerfristige optische und akustische Überwachung

§ 21 Längerfristige Bewegungsüberwachung

§ 22 Überwachung von Brief-, Post- und Telekommunikationsverkehren

§ 23 Auslesen informationstechnischer Geräte

§ 24 Auslesen technischer Spuren von informationstechnischen Angriffen

§ 25 Eingriff in die Integrität privater informationstechnischer Systeme

§ 26 Abgegrenzter Eingriff in die Integrität privater informationstechnischer Systeme

§ 27 Wohnraumüberwachung

§ 28 Einsatzsicherung

§ 29 Besonderer Einsatz nachrichtendienstlicher Mittel

§ 30 Allgemeine Schranken nachrichtendienstlicher Mittel

§ 31 Schutz des Kernbereichs privater Lebensgestaltung

§ 32 Schutz von zeugnisverweigerungsberichtigten Berufsgeheimnisträgern

Unterabschnitt 3
Verfahren bei besonderen Maßnahmen

§ 33 Anordnung von Maßnahmen

§ 34 Unabhängige Vorabkontrolle

§ 35 Mitteilung an betroffene Personen

Unterabschnitt 4
Weiterverarbeitung von Daten

§ 36 Weiterverarbeitung

§ 37 Qualifizierte Auswertung

§ 38 Datenpflege in Dateisystemen

§ 39 Akten

§ 40 Protokolldaten

§ 41 Errichtungsanordnungen

Unterabschnitt 5

Gemeinsame automatisierte Auswertung

§ 42 Gemeinsame automatisierte Auswertung mit inländischen öffentlichen Stellen

§ 43 Gemeinsame Dateisysteme mit ausländischen Nachrichtendiensten

§ 44 Teilnahme an gemeinsamen Dateisystemen ausländischer Nachrichtendienste

A b s c h n i t t 3
Ü b e r m i t t l u n g

§ 45 Information von Öffentlichkeit und Fachkreisen

§ 46 Übermittlung an inländische öffentliche Stellen zur Gefahrenabwehr

§ 47 Übermittlung an inländische öffentliche Stellen zum administrativen Rechtsgüterschutz

§ 48 Übermittlung an Strafverfolgungsbehörden zur Strafverfolgung

§ 49 Übermittlung an inländische öffentliche Stellen ohne Möglichkeit operativer Anschlussmaßnahmen

§ 50 Übermittlung an inländische öffentliche Stellen von Daten aus Gefahrenaufklärung

§ 51 Übermittlung an inländische nichtöffentliche Stellen

§ 52 Übermittlungsverbote

§ 53 Minderjährigenschutz bei Inlandsübermittlung

§ 54 Weiterverarbeitung durch Empfänger

§ 55 Übermittlung an ausländische sowie über- und zwischenstaatliche Stellen

§ 56 Ohne Ausübung besonderer Befugnisse gewonnene personenbezogene Daten

§ 57 Übermittlung zum Schutz der betroffenen Person

§ 58 Weitere Verfahrensregelungen

§ 59 Nachberichtspflicht

A b s c h n i t t 4
S c h u t z m a ß n a h m e n

§ 60 Schutzmaßnahmen

§ 61 Anordnung von Schutzmaßnahmen

§ 62 Unterstützung von Schutzmaßnahmen

§ 63 Besondere Kontrolle der Durchführung von Schutzmaßnahmen

A b s c h n i t t 5
W e i t e r e R e g e l u n g e n z u r E i g e n s i c h e r u n g

§ 64 Schutz des Eigensicherungsbereichs

§ 65 Verfahren im Eigensicherungsbereich

§ 66 Schutz vor unbemannten Fluggeräten

§ 67 Ergänzende Regelungen zur Verarbeitung personenbezogener Daten

§ 68 Mitbestimmung bei Maßnahmen der Eigensicherung

Abschnitt 6
Allgemeiner Datenschutz und Rechtskontrolle

§ 69 Anwendung des Bundesdatenschutzgesetzes

§ 70 Unabhängige Rechts- und Datenschutzkontrolle

§ 71 Auskunft an betroffene Personen

Abschnitt 7
Schlussvorschriften

§ 72 Kontrolle und Durchsetzung von Unternehmenspflichten

§ 73 Besondere Anzeige- und Genehmigungspflicht für ausgeschiedene Bedienstete

§ 74 Strafvorschriften

§ 75 Ordnungswidrigkeiten

§ 76 Spannungs- und Verteidigungsfall

§ 77 Anwendung durch Landesbehörden für Verfassungsschutz

§ 78 Verordnungsermächtigung

§ 79 Einschränkung von Grundrechten

§ 80 Übergangsvorschriften

Abschnitt 1

Aufgaben und Zusammenarbeit der Verfassungsschutzbehörden

§ 1

Zusammenarbeitspflicht

(1) Der Bund und die Länder sind verpflichtet, beim Schutz der freiheitlichen demokratischen Grundordnung sowie des Bestandes und der Sicherheit des Bundes und der Länder zusammenzuarbeiten. Die Zusammenarbeit besteht auch in gegenseitiger Unterstützung und Hilfeleistung.

(2) Für die Zusammenarbeit unterhält der Bund ein Bundesamt für Verfassungsschutz als Bundesoberbehörde. Es untersteht dem Bundesministerium des Innern. Es darf einer polizeilichen Dienststelle nicht angegliedert werden.

(3) Für die Zusammenarbeit der Länder mit dem Bund und der Länder untereinander beim Schutz nach Absatz 1 unterhält jedes Land eine Behörde. Mehrere Länder können eine gemeinsame Behörde unterhalten.

§ 2

Aufgaben der Verfassungsschutzbehörden

(1) Aufgabe der Verfassungsschutzbehörden des Bundes und der Länder ist, folgenden Bestrebungen und Tätigkeiten entgegenzuwirken:

1. Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben,

2. Bestrebungen im Geltungsbereich dieses Gesetzes, die

   a) durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden,

   b) gegen den Gedanken der Völkerverständigung (Artikel 9 Absatz 2 des Grundgesetzes), insbesondere gegen das friedliche Zusammenleben der Völker (Artikel 26 Absatz 1 des Grundgesetzes) gerichtet sind,

   c) gegen die Sicherheit der Europäischen Union, der Nordatlantischen Vertragsunion oder einer anderen internationalen Organisation, der die Bundesrepublik Deutschland angehört, gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Organe oder der Mitglieder der Organe der Europäischen Union oder der internationalen Organisation zum Ziele haben,

3. Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht, die

   a) sicherheitsgefährdend sind, indem sie gegen die in den Nummern 1 und 2 genannten Rechtsgüter gerichtet sind,

   b) geheimdienstlich sind, indem die Zurechenbarkeit zur fremden Macht planmäßig verschleiert wird.

(2) Die Verfassungsschutzbehörden des Bundes und der Länder wirken den Bestrebungen und Tätigkeiten nach Absatz 1 entgegen, indem sie

1. über die Bestrebungen und Tätigkeiten informieren und

2. diese dazu bereits frühzeitig aufklären.

Die Verfassungsschutzbehörden des Bundes und der Länder können auch beim Ausstieg aus einer Beteiligung an Bestrebungen unterstützen. Sie sind an die allgemeinen Rechtsvorschriften gebunden (Artikel 20 des Grundgesetzes).

(3) Bestrebungen und Tätigkeiten nach Absatz 1 muss die Verfassungsschutzbehörde vorbehaltlich des Satzes 2 aufklären, wenn zu ihnen tatsächliche Anhaltspunkte vorliegen. Die Entschließung zur Aufklärung liegt im Ermessen der Verfassungsschutzbehörde bei

1. Bestrebungen und Tätigkeiten nach Absatz 1 Nummer 2 Buchstabe c, auch in Verbindung mit Nummer 3 Buchstabe a,

2. Bestrebungen nach Absatz 2 Nummer 1 und 2, die von Einzelpersonen ausgehen.

(4) Zur Eigensicherung schützt das Bundesamt für Verfassungsschutz seine Bediensteten, verdeckte Hilfspersonen, Einrichtungen, Gegenstände und

geheimhaltungsbedürftigen Informationen vor Tätigkeiten, die geeignet sind, ihre ordnungsgemäße Aufgabenwahrnehmung zu beeinträchtigen.

(5) Über eine Information nach Absatz 1 Satz 1 Nummer 2 hinaus wirken die Verfassungsschutzbehörden des Bundes und der Länder mit bei

1. der Überprüfung von Personen in gesetzlich bestimmten Fällen,

2. der Geheimschutzbetreuung von nichtöffentlichen Stellen, bei Bedarf durch deren sicherheitsmäßige Bewertung, soweit im Einzelfall erforderlich auch unter Einbezug der Erkenntnisse der Nachrichtendienste des Bundes sowie ausländischer öffentlicher Stellen, sowie

3. technischen Sicherheitsmaßnahmen zum Schutz von im öffentlichen Interesse geheimhaltungsbedürftigen Tatsachen, Gegenständen oder Erkenntnissen gegen die Kenntnisnahme durch Unbefugte.

§ 3

Begriffsbestimmungen

(1) Bestrebungen sind politisch bestimmte, zielgerichtete Verhaltensweisen in einem oder für einen Personenzusammenschluss oder von Einzelpersonen.

(2) Bestrebungen sind gerichtet gegen

1. den Bestand des Bundes oder eines Landes, wenn sie bezwecken, die Freiheit des Bundes oder eines Landes von fremder Herrschaft aufzuheben, ihre staatliche Einheit zu beseitigen oder ein zu ihm gehörendes Gebiet abzutrennen,

2. die Sicherheit des Bundes oder eines Landes, wenn sie bezwecken, den Bund, Länder oder deren Einrichtungen in ihrer Funktionsfähigkeit erheblich zu beeinträchtigen,

3. die freiheitliche demokratische Grundordnung, wenn sie bezwecken, einen Grundsatz der freiheitlichen demokratischen Grundordnung zu beseitigen oder außer Geltung zu setzen.

(3) Grundsätze der freiheitlichen demokratischen Grundordnung sind

1. die Garantie der Menschenwürde (Artikel 1 Absatz 1 des Grundgesetzes),

2. das Demokratieprinzip (Artikel 20 Absatz 1 und 2 des Grundgesetzes), insbesondere

   a) die Möglichkeit gleichberechtigter Teilnahme aller Bürgerinnen und Bürger am Prozess der politischen Willensbildung und

   b) die Rückbindung der Ausübung der Staatsgewalt an das Volk,

3. als Ausfluss des Rechtsstaatsprinzips

   a) die Rechtsbindung der öffentlichen Gewalt (Artikel 20 Absatz 3 des Grundgesetzes)

   b) die Kontrolle dieser Bindung durch unabhängige Gerichte,

   c) das Gewaltmonopol des Staates.

(4) Bedrohungen sind

1. verfassungsfeindliche Bestrebungen nach § 2 Absatz 1 Nummer 1 und 2,

2. sicherheitsgefährdende Tätigkeiten nach § 2 Absatz 1 Nummer 3 Buchstabe a,

3. geheimdienstliche Tätigkeiten nach § 2 Absatz 1 Nummer 3 Buchstabe b sowie

4. funktionsgefährdende Tätigkeiten nach § 2 Absatz 4.

(5) Beteiligte einer Bedrohung sind Personen, die

1. Bestrebungen als Einzelperson oder in einem Personenzusammenschluss betreiben,

2. Bestrebungen nachdrücklich unterstützen oder

3. sicherheitsgefährdende, geheimdienstliche oder funktionsgefährdende Tätigkeiten ausüben.

(6) Verdeckte Hilfspersonen sind Personen, die für das Bundesamt für Verfassungsschutz zur Aufklärung von Bedrohungen verdeckt tätig sind, insbesondere Gewährspersonen, Informanten und Vertrauenspersonen.

(7) Erheblich beobachtungsbedürftig sind Bedrohungen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass sie geeignet sind, die in § 2 Absatz 1 genannten Schutzgüter erheblich zu beeinträchtigen. Die Eignung ist anzunehmen, wenn zur Zielverfolgung Straftaten begangen werden. Die Eignung kann anzunehmen sein nach Maßgabe

1. der Vorgehensweise bei der Zielverfolgung, nämlich

   a) gewaltorientiert, indem Gewalt angewendet wird oder dazu Bereitschaft besteht oder Gewalt unterstützt oder befürwortet wird,

   b) zu Hass oder Willkürmaßnahmen gegen Personengruppen anstachelnd oder deren Menschenwürde durch böswillige Verächtlichmachung angreifend,

   c) in sonstiger Weise kämpferisch-aggressiv oder

   d) planmäßig verschleiernd,

2. des Aktionspotenzials der Bestrebungen oder

3. des Umfangs gesellschaftlicher Einflussnahme der Bestrebungen.

In den Fällen des Satzes 3 Nummer 1 sowie bei funktionsgefährdenden Tätigkeiten ist die Eignung in der Regel anzunehmen.

(8) Besonders erheblich beobachtungsbedürftig sind Bedrohungen, wenn tatsächliche Anhaltspunkte vorliegen für

1. verfassungsfeindliche Bestrebungen, die

   a) zur Zielverfolgung Straftaten begehen, die im Höchstmaß mit Freiheitsstrafe von mindestens 5 Jahren bedroht sind,

   b) die verfassungswidrigen Bestrebungen eines nach § 3 des Vereinsgesetzes verbotenen Vereins an dessen Stelle in einem Personenzusammenschluss fortführen, wenn der verbotene Verein erheblich beobachtungsbedürftig war,

2. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten,

3. funktionsgefährdende Tätigkeiten

   a) durch gegenwärtige oder ehemalige Bedienstete des Bundesamtes für Verfassungsschutz, verdeckte Hilfspersonen, Personen, die mit einer nach § 1 Absatz 2 oder 4 des Sicherheitsüberprüfungsgesetzes sicherheitsempfindlichen Tätigkeiten des Bundesamtes für Verfassungsschutz beauftragt sind oder waren, oder Personen, die Zugang zu den Dienststellen, Grundstücken und sonstigen Einrichtungen des Bundesamtes für Verfassungsschutz erhalten oder erhalten haben,

   b) durch unerlaubten Zugriff auf informationstechnische Systeme des Bundesamtes für Verfassungsschutz oder

   c) bei denen zur Zielverfolgung Straftaten begangen werden, die im Höchstmaß mit Freiheitsstrafe von mindestens 5 Jahren bedroht sind.

(9) Besonders gewichtige Rechtsgüter sind

1. die freiheitliche demokratischen Grundordnung und der Bestand und die Sicherheit des Bundes und der Länder sowie die Völkerverständigung und das friedliche Zusammenleben der Völker,

2. die Sicherheit der Europäischen Union und der internationalen Organisationen, denen die Bundesrepublik Deutschland angehört,

3. Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, sowie Sachen von bedeutendem Wert und bedeutende Vermögenswerte, deren Erhaltung im besonderen öffentlichen Interesse geboten ist sowie

4. das Leben, die körperliche Unversehrtheit sowie Freiheit und sexuelle Selbstbestimmung und vergleichbar besonders gewichtige Rechtsgüter einer Person,

(10) Eine konkretisierte Gefahr liegt vor, wenn sich der zum Schaden führende Kausalverlauf zwar noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, aber bereits bestimmte Tatsachen im Einzelfall auf die Entstehung einer konkreten Gefahr für ein Rechtsgut hinweisen.

(11) Besondere Befugnisse sind

1. Befugnisse zum Einsatz nachrichtendienstlicher Mittel sowie

2. sonstige Befugnisse, die eine wenigstens erheblich beobachtungsbedürftige Bedrohung voraussetzen.

§ 4

Bedrohungsaufklärung durch das Bundesamt für Verfassungsschutz

(1) Das Bundesamt für Verfassungsschutz darf Bedrohungen aufklären, wenn sie

1. sich ganz oder teilweise gegen den Bund richten,

2. gewaltorientiert (§ 3 Absatz 7 Satz 3 Nummer 1 Buchstabe a) sind,

3. sich über den Bereich eines Landes hinaus erstrecken,

4. auswärtige Belange der Bundesrepublik Deutschland berühren oder

5. eine Landesbehörde für Verfassungsschutz das Bundesamt für Verfassungsschutz um ein Tätigwerden ersucht.

Bei Bedrohungen nach § 3 Absatz 4 Nummern 1 bis 3 setzt es sich in den Fällen des Satzes 1 Nummer 1 bis 4 mit der Verfassungsschutzbehörde des Landes, in dem es tätig werden will, ins Benehmen. Das Benehmen kann für eine Reihe gleichgelagerter Fälle hergestellt werden.

(2) Eine Aufklärung von Personenzusammenschlüssen wegen verfassungsfeindlicher Bestrebungen ist nur zulässig, wenn die Bestrebungen zuvor als Beobachtungsobjekt eingestuft worden sind. Die Einstufung erfolgt durch den Präsidenten oder die Präsidentin des Bundesamtes für Verfassungsschutz. Sie erfolgt als

1. Verdachtsfall, wenn lediglich tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen vorliegen,

2. gesichert verfassungsfeindlich, wenn das Bundesamt für Verfassungsschutz nach dem Gesamtergebnis der ihm vorliegenden Informationen als gesichert bewertet, dass es sich um verfassungsfeindliche Bestrebungen handelt.

Die Einstufung ist aufzuheben, wenn tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen nicht mehr vorliegen.

(3) Im Verdachtsfall nach Absatz 2 Satz 3 Nummer 1 ist nach spätestens 3 Jahren zu überprüfen, ob weiterhin tatsächliche Anhaltspunkte für solche Bestrebungen vorliegen. Die Einstufung als Verdachtsfall ist nach Absatz 2 Satz 4 und dann aufzuheben, wenn die Beobachtungsdauer unter Berücksichtigung der erreichten und erwartbaren Verdachtsverdichtung außer Verhältnis steht zur Beobachtungsbedürftigkeit. Außer Verhältnis steht die Beobachtungsdauer in der Regel, wenn die Bestrebungen nach 5 Jahren noch nicht als gesichert verfassungsfeindlich bewertet werden. Die Fortführung einer Aufklärung als Verdachtsfall nach 5 Jahren bedarf der Zustimmung des Bundesministeriums des Innern, die für jeweils höchstens weitere 2 Jahre gilt.

(4) Das Bundesamt für Verfassungsschutz kann prüfen, ob die Voraussetzungen zur Einstufung als Beobachtungsobjekt vorliegen, wenn im Einzelfall erste Anhaltspunkte dafür vorliegen (Prüffall). Zur Erhebung personenbezogener Daten darf es keine nachrichtendienstlichen Mittel einsetzen und keine Befugnisse ausüben, die wenigstens erheblich beobachtungsbedürftige Bedrohungen voraussetzen. Aus allgemein zugänglichen Quellen darf es Informationen auch verdeckt erheben, dabei jedoch kein schutzwürdiges Vertrauen in Anspruch nehmen. Die Prüfung nach Satz 1 soll 2 Jahre nicht überschreiten. Eine längere Prüfung bedarf der Billigung durch den Präsidenten oder die Präsidentin des Bundesamtes für Verfassungsschutz, die für jeweils höchstens weitere 2 Jahre gilt.

§ 5

Zentralstellenaufgaben des Bundesamtes für Verfassungsschutz

(1) Das Bundesamt für Verfassungsschutz wertet unbeschadet der Auswertungsverpflichtungen der Landesbehörden für Verfassungsschutz zentral alle Erkenntnisse über Bedrohungen nach § 3 Absatz 4 Nummer 1 bis 3 aus. Es unterrichtet die Landesbehörden für Verfassungsschutz nach § 6 Absatz 1, insbesondere durch Querschnittsauswertungen in Form von Struktur- und Methodikberichten sowie regelmäßig durch bundesweite Lageberichte zu den wesentlichen Phänomenbereichen unter Berücksichtigung der entsprechenden Landeslageberichte.

(2) Das Bundesamt für Verfassungsschutz koordiniert die Zusammenarbeit der Verfassungsschutzbehörden. Die Koordinierung schließt insbesondere ein die Vereinbarung von

1. einheitlichen Vorschriften zur Gewährleistung der Zusammenarbeitsfähigkeit,

2. allgemeinen Arbeitsschwerpunkten,

3. Relevanzkriterien für Übermittlungen nach § 6 Absatz 1 und

4. arbeitsteiliger Durchführung der Aufgaben.

(3) Das Bundesamt unterstützt die Landesbehörden für Verfassungsschutz bei der Erfüllung ihrer Aufgaben nach § 2 insbesondere durch

1. Bereitstellung des nachrichtendienstlichen Informationssystems,

2. zentrale Einrichtungen im Bereich besonderer technischer und fachlicher Fähigkeiten,

3. Erforschung und Entwicklung von Methoden und Arbeitsweisen im Verfassungsschutz und

4. Fortbildung in speziellen Arbeitsbereichen.

(4) Die Koordination nach Absatz 2 und Unterstützung nach Absatz 3 kann den Militärischen Abschirmdienst mit dessen Einvernehmen einbeziehen.

(5) Dem Bundesamt für Verfassungsschutz obliegt der für Aufgaben nach § 2 Absatz 1 erforderliche Dienstverkehr mit zuständigen öffentlichen Stellen anderer Staaten. Die Landesbehörden für Verfassungsschutz können solchen Dienstverkehr führen

1. mit den Dienststellen der in der Bundesrepublik Deutschland stationierten Streitkräfte,

2. mit den Nachrichtendiensten angrenzender Nachbarstaaten in regionalen Angelegenheiten oder

3. mit anderen Stellen im Einvernehmen mit dem Bundesamt für Verfassungsschutz.

In den Fällen des Satzes 2 Nummer 1 und 2 informieren die Landesbehörden für Verfassungsschutz das Bundesamt für Verfassungsschutz über den Dienstverkehr.

§ 6

Gegenseitige Unterrichtung der Verfassungsschutzbehörden; nachrichtendienstliches Informationssystem

(1) Die Landesbehörden für Verfassungsschutz und das Bundesamt für Verfassungsschutz sowie der Militärische Abschirmdienst übermitteln sich unverzüglich die Informationen, die für ihre Verfassungsschutzaufgaben auf Grund tatsächlicher Anhaltspunkte zu bestimmten Bedrohungen relevant sind, einschließlich der Erkenntnisse ihrer Auswertungen. Übermittelte Daten dürfen, wenn eine übermittelnde Behörde sich dies vorbehält, nur mit Zustimmung der übermittelnden Behörde an andere Stellen als die in Satz 1 genannten Behörden weiter übermittelt werden.

(2) Zur Erfüllung ihrer Unterrichtungspflichten nach Absatz 1 verarbeiten die Verfassungsschutzbehörden sowie der Militärische Abschirmdienst Informationen im gemeinsamen nachrichtendienstlichen Informationssystem. Zur Durchführung ihrer

Mitwirkungsaufgaben nach § 2 Absatz 5 Nummer 1 sowie § 2 Absatz 3 des MAD-Gesetzes speichern sie die zur Identifikation betroffener Personen und zum Auffinden des Mitwirkungsvorganges erforderlichen Daten. Für die Verarbeitung personenbezogener Daten im nachrichtendienstlichen Informationssystem gelten die §§ 36, 37 und 38. Die Verantwortung einer speichernden Stelle im Sinne der allgemeinen Vorschriften des Datenschutzrechts trägt jede Behörde nur für die von ihr eingegebenen Daten; nur sie darf diese Daten verändern oder löschen oder deren Verarbeitung einschränken. Die eingebende Stelle muss feststellbar sein. Eine Abfrage von Daten ist nur zulässig, soweit dies zur Erfüllung von Aufgaben, mit denen der Abfragende unmittelbar betraut ist, erforderlich ist. Die Zugriffsberechtigung auf Daten, die nicht zum Auffinden von Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind, ist auf Personen zu beschränken, die mit der Erfassung von Daten oder Analysen betraut sind. Die Zugriffsberechtigung auf Unterlagen, die gespeicherte Angaben belegen, ist zudem auf Personen zu beschränken, die unmittelbar mit Arbeiten in diesem Anwendungsgebiet betraut sind.

(3) Das Bundesamt für Verfassungsschutz trifft für die gemeinsamen Dateisysteme technische und organisatorische Maßnahmen entsprechend § 64 Absatz 3 des Bundesdatenschutzgesetzes. Es hat bei jedem Zugriff für Zwecke der Datenschutzkontrolle den Zeitpunkt, die Angaben, die die Feststellung der abgefragten Datensätze ermöglichen, sowie die abfragende Stelle zu protokollieren.

§ 7

Weisungsrechte des Bundes

Das Bundesministerium des Innern kann, wenn ein Angriff auf die verfassungsmäßige Ordnung des Bundes erfolgt, den obersten Landesbehörden die für die Zusammenarbeit der Länder mit dem Bund auf dem Gebiet des Verfassungsschutzes erforderlichen Weisungen erteilen.

Abschnitt 2

Aufklärung

Unterabschnitt 1

Allgemeine Informationsgewinnung, Mitwirkungspflichten

§ 8

Allgemeine Datenerhebung

(1) Das Bundesamt für Verfassungsschutz darf die zur Erfüllung seiner Aufgaben erforderlichen Informationen einschließlich personenbezogenen Daten erheben, sofern nicht besondere Regelungen in diesem Gesetz entgegenstehen. Für die Erforderlichkeit müssen tatsächliche Anhaltspunkte im Einzelfall vorliegen, wenn die Erhebung aus allgemein zugänglichen Quellen mittels einer automatisierten Anwendung erfolgt, die

1. Daten zu einer Person systematisch zusammenführt oder

2. biometrische Merkmale mit Daten abgleicht, auf die das Bundesamt für Verfassungsschutz zur Erfüllung seiner Aufgaben zugreifen darf.

(2) Zur Durchführung einer Erhebung nach Absatz 1 Satz 2 Nummer 2 darf der Abgleich auch durch eine öffentliche oder nichtöffentliche Stelle in einem Drittstaat erfolgen, wenn der Abgleich nicht gleichermaßen durch das Bundesamt für Verfassungsschutz selbst, eine andere inländische Stelle oder eine Stelle eines Mitgliedsstaates der Europäischen Union erfolgen kann. Die im Rahmen einer Erhebung nach Absatz 1 Satz 2 Nummer 2 erhobenen Daten sind nach Durchführung des Abgleichs zu löschen, wenn sie nicht auf Grund tatsächlicher Anhaltspunkte im Einzelfall für Aufgaben des Bundesamtes für Verfassungsschutz erforderlich sind. Der Unabhängige Kontrollrat hat die Einhaltung der besonderen Vorschriften zu einer Erhebung nach Absatz 1 Satz 2 Nummer 2 mindestens alle 2 Jahre zu kontrollieren.

(3) Erhebt das Bundesamt für Verfassungsschutz personenbezogene Daten bei der betroffenen Person mit ihrer Kenntnis, so ist der Erhebungszweck anzugeben. Die betroffene Person ist auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(4) Von mehreren zur Datenerhebung geeigneten Maßnahmen hat das Bundesamt für Verfassungsschutz diejenige zu wählen, die die betroffene Person voraussichtlich am wenigsten beeinträchtigt. Eine Maßnahme darf keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht.

§ 9

Datenerhebung bei Dritten

(1) Das Bundesamt für Verfassungsschutz darf Dritte um Übermittlung von Informationen einschließlich personenbezogenen Daten ersuchen, wenn dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zur Aufklärung von Bedrohungen erforderlich ist. Das Ersuchen darf nur diejenigen personenbezogenen Daten enthalten, die für die Erteilung der Auskunft erforderlich sind. Durch das Ersuchen dürfen schutzwürdige Interessen der betroffenen Person nur in unvermeidbarem Umfang beeinträchtigt werden.

(2) Ein inländischer Dritter darf die Informationen einschließlich personenbezogener Daten übermitteln, wenn nicht besondere gesetzliche Übermittlungsregelungen entgegenstehen.

(3) Einem inländischen Dritten und seinen Beschäftigten ist verboten,

1. der betroffenen Person oder anderen Stellen Informationen über das Ersuchen oder dessen Durchführung mitzuteilen, auch im Wege gesetzlicher Verdachtsmeldungen,

2. allein auf Grund eines Ersuchens einseitige Handlungen vorzunehmen, die für die betroffene Person nachteilig sind und die über die Erteilung der Auskunft hinausgehen, insbesondere bestehende Verträge oder Geschäftsverbindungen zu beenden, ihren Umfang zu beschränken oder ein Entgelt zu erheben oder zu erhöhen.

§ 10

Übermittlung durch inländische öffentliche Stellen

(1) Inländische öffentliche Stellen haben auf Ersuchen des Bundesamtes für Verfassungsschutz ihnen vorliegende Informationen, einschließlich Personaldaten, zu

übermitteln, wenn nicht besondere gesetzliche Übermittlungsregelungen entgegenstehen. Zur Durchführung ihrer Übermittlungspflicht dürfen sie

1. Daten aus allgemein zugänglichen Quellen verarbeiten und

2. dem Bundesamt für Verfassungsschutz in geeigneten Fällen den automatisierten Abruf von Daten einrichten.

(2) Würde durch das Ersuchen dessen Zweck gefährdet oder die betroffene Person unverhältnismäßig beeinträchtigt, darf das Bundesamt für Verfassungsschutz amtliche Register einsehen. Das Bundesamt für Verfassungsschutz hat die Einsichtnahme suchfähig zu dokumentieren und dabei das Register, den Zweck und die Veranlassung anzugeben. Es muss die Dokumentation am Ende des zweiten Kalenderjahres, das dem Jahr ihrer Erstellung folgt, löschen.

(3) Im polizeilichen Informationsverbund werden auf Ersuchen des Bundesamtes für Verfassungsschutz durch die jeweilige Stelle zur verdeckten Kontrolle folgende Personen und Gegenstände ausgeschrieben, soweit dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zur Aufklärung von wenigstens erheblich beobachtungsbedürftigen Bedrohungen erforderlich ist,

1. Beteiligte dieser Bedrohung und

2. Personen, bargeldlose Zahlungsmittel und Sachen, die in einem Zusammenhang mit dieser Bedrohung stehen, der Grund zu der Annahme gibt, dass dadurch Erkenntnisse über die Bedrohungen gewonnen werden können, die nicht durch eine Ausschreibung nach Nummer 1 zu gewinnen sind.

Satz 1 gilt nach Maßgabe unmittelbar geltender Rechtsakte der Europäischen Union auch für Datenverarbeitungssysteme der Europäischen Union. Ist die Ausschreibungsfrist abgelaufen oder die Maßnahme einzustellen, so ist die Ausschreibung unverzüglich zu löschen. Das Bundesamt für Verfassungsschutz hat Ersuchen zu protokollieren.

(4) Inländische öffentliche Stellen dürfen von sich aus dem Bundesamt für Verfassungsschutz Informationen einschließlich personenbezogener Daten übermitteln, wenn ihnen tatsächliche Anhaltspunkte zu Bedrohungen vorliegen, besondere gesetzliche Übermittlungsregelungen nicht entgegenstehen und nicht offenkundig ist, dass die Information für die Verfassungsschutzbehörde nicht erforderlich ist. Unter den Voraussetzungen des Satzes 1 zur Übermittlung verpflichtet sind

1. der Bundesnachrichtendienst,

2. das Bundesamt für Sicherheit in der Informationstechnik,

3. Justizvollzugsbehörden, die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien, die Behörden des Zollfahndungsdienstes sowie andere Zolldienststellen, soweit diese Aufgaben nach dem Bundespolizeigesetz wahrnehmen,

4. das Bundesamt für Migration und Flüchtlinge,

5. Finanzbehörden sowie

6. sonstige öffentliche Stellen, jedoch im Falle von verfassungsfeindlichen Bestrebungen nur, wenn sie im Sinne von § 3 Absatz 7 Nummer 1 Buchstaben a und b gewaltorientiert oder volksverhetzend vorgehen.

Sofern öffentliche Stellen der Länder zur Übermittlung von Informationen an die jeweilige Landesbehörde für Verfassungsschutz verpflichtet sind, sind sie nicht verpflichtet diese Informationen auch an das Bundesamt für Verfassungsschutz zu übermitteln.

(5) Unterliegen übermittelte personenbezogene Daten einer besonderen gesetzlichen Zweckbindung, so ist diese bei der Weiterverarbeitung zu beachten. Personenbezogene Daten, die mit Maßnahmen erhoben worden sind, die den in den §§ 25 und 27 geregelten Maßnahmen entsprechen, dürfen nur nach Maßgabe dieser Vorschriften weiterverarbeitet werden.

(6) Die Zuständigkeit und das Verfahren für die Entscheidung des Bundesamtes für Migration und Flüchtlinge zu Übermittlungen nach Absatz 4 Satz 2 Nummer 4 sind in einer Dienstvorschrift zu regeln, die der Zustimmung des Bundesministeriums des Innern bedarf. Nach Absatz 4 Satz 2 Nummer 4 übermittelte personenbezogene Daten dürfen nach § 55 auch dann nicht weiter übermittelt werden, wenn überwiegende schutzwürdige Belange Dritter entgegenstehen. Vor einer Übermittlung an eine Stelle des Herkunftsstaates ist das Bundesamt für Migration und Flüchtlinge zu beteiligen.

(7) Die Übermittlungspflichten nach Absatz 1 und Absatz 4 Satz 2 gelten nicht für

1. den Bundesnachrichtendienst, wenn überwiegenden Sicherheitsinteressen entgegenstehen,

2. die in Absatz 4 Satz 1 Nummer 3 genannten Stellen, wenn überwiegende Gründe des Schutzes verdeckt eingesetzter Personen oder des Schutzes operativer Maßnahmen entgegenstehen.

§ 11

Verpflichtende Ersuchen an geschäftsmäßige Diensteanbieter

(1) Auf Ersuchen des Bundesamtes für Verfassungsschutz nach § 9 Absatz 1 Satz 1 sind verpflichtet, Auskunft zu ihren Diensten zu erteilen

1. diejenigen, die geschäftsmäßig

   a) Dienste des Güter- oder Personenverkehrs,

   b) Digitale Dienste oder

   c) technische Dienste nach § 2 Absatz 1 Nummer 9 des Zahlungsdiensteaufsichtsgesetzes

   ausführen oder an deren Ausführung geschäftsmäßig mitwirken,

2. Kraftfahrzeughersteller oder Kraftfahrzeugwerkstätten zu Telemetriedaten,

3. die Verpflichteten nach § 2 Absatz 1 des Geldwäschegesetzes, wenn sie nicht durch Rechtsverordnung nach § 2 Absatz 2 des Geldwäschegesetzes vom Anwendungsbereich Geldwäschegesetzes ausgenommen oder entsprechend § 30 Absatz 3 Satz 3 und 4 des Geldwäschegesetzes zur Verweigerung der Auskunft berechtigt sind.

(2) Zur Auskunft verpflichtet sind Stellen nach Absatz 1, die in Deutschland eine Niederlassung haben oder in Deutschland Leistungen erbringen oder an solchen Leistungen mitwirken. Diese Stellen sind auch zur Geheimhaltung nach § 9 Absatz 3 verpflichtet. Die

Geheimhaltungspflicht gilt nicht für Stellen, die keine Niederlassung in Deutschland haben, wenn das Recht des Staates, in dem sie ihren Hauptsitz haben, ihr entgegensteht.

(3) Die Auskunftspflicht ist beschränkt auf jeweils vorhandene

1. Informationen über den angebotenen Dienst und

2. personenbezogene Daten

   a) die der Verpflichtete für die Begründung, inhaltliche Ausgestaltung und Beendigung des Nutzungsverhältnisses mit dem Nutzer des angebotenen Dienstes speichert (Bestandsdaten), im Falle des Absatzes 1 Nummer 2 auch zu wirtschaftlich Berechtigten,

   b) über die Nutzung des Dienstes durch den Nutzer, einschließlich Inhalte von Nutzungen und bei Nutzung anfallende Informationen (qualifizierte Auskunft).

Eine Verpflichtung zur Speicherung von Daten besteht nur, soweit dies im Einzelfall zur Erfüllung eines Ersuchens erforderlich ist.

(4) Ein Ersuchen an Kraftfahrzeugwerkstätten nach Absatz 1 Nummer 2 ist nur zulässig, wenn ein Ersuchen an den Kraftfahrzeughersteller nicht oder nicht ohne Gefährdung des Zwecks der Maßnahme möglich ist. Ein Ersuchen an Stellen nach Absatz 1 Satz 1 Nummer 1 Buchstabe c zu Passwörtern oder andere Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, darf nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. Ein Ersuchen an Stellen nach Absatz 1 Nummer 3 um Kontoinformationen ist unzulässig, wenn die Auskunft vom Bundeszentralamt für Steuern nach § 93b Absatz 2 der Abgabenordnung erlangt werden kann.

(5) Ein Ersuchen um eine qualifizierte Auskunft ist nur zulässig

1. im Fall wenigstens erheblich beobachtungsbedürftiger Bedrohungen und

2. nur zu

   a) Personen, zu denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie an einer solchen Bedrohung beteiligt sind, auch indem sie Leistungen für Beteiligte in Anspruch nehmen,

   b) Personen, die in einem Zusammenhang mit einer solchen Bedrohung stehen, der Grund zu der Annahme gibt, dass durch die Maßnahme Erkenntnisse über die Bedrohung gewonnen werden können, die nicht gleichermaßen durch ein Ersuchen nach Buchstabe b zu gewinnen sind, und

   c) verdeckten Hilfspersonen.

(6) Ein Ersuchen um künftig anfallende Daten ist auf höchstens 1 Jahr zu befristen. Im Ersuchen ist zur Begründung gegenüber dem Verpflichteten lediglich die Rechtsgrundlage anzugeben. Ersuchen erfolgen schriftlich, wenn dies erforderlich ist, um dem Verpflichteten die Erfüllung seiner Verpflichtung zu ermöglichen. In Ersuchen ist auch auf die Pflichten nach § 9 Absatz 3 hinzuweisen sowie darauf, dass das Ersuchen nicht die Aussage beinhaltet, dass sich die betroffene Person rechtswidrig verhalten habe oder ein darauf gerichteter Verdacht bestehen müsse.

(7) Für die Entschädigung der Verpflichteten finden § 2 Absatz 1 und 4 und § 23 Absatz 1 und 2 des Justizvergütungs- und -entschädigungsgesetzes entsprechend Anwendung. Das Bundesamt für Verfassungsschutz kann mit den Verpflichteten besondere

Entschädigungsvereinbarungen treffen, deren Höhe sich an den nachgewiesenen tatsächlichen Kosten orientiert, wenn diese nach Satz 1 wegen besonderer Umstände nicht angemessen vergütet werden. Besondere Umstände liegen in der Regel nicht vor, wenn die Auskunft durch Auswertung von strukturiert gespeicherten Daten erfolgt.

§ 12

Verpflichtende Ersuchen bei informationstechnischen Angriffen

(1) Anbieter, die informationstechnische Systeme geschäftsmäßig Dritten zur Nutzung überlassen und in Deutschland eine Niederlassung haben oder in Deutschland Leistungen erbringen, sind verpflichtet, dem Bundesamt für Verfassungsschutz auf Ersuchen Auskunft über technische Informationen zur Aufklärung eines informationstechnischen Angriffs zu geben. Das Ersuchen kann sich insbesondere beziehen auf

1. den Verkehrsfluss zu bestimmten Kennungen, für die tatsächliche Anhaltspunkte bestehen, dass sie der Angreifer nutzt (maliziöse Kennungen),

2. Schadprogramme oder sonstige Angriffswerkzeuge und deren Einsatz, einschließlich Steuerungs- oder Protokolldateien, sowie auf Spuren, die technisch mit dem Angriff verbunden sind, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass das informationstechnische System für Angriffe genutzt wurde.

Sind in dem informationstechnischen System des Verpflichteten Daten gespeichert, die durch den Angriff beschafft worden sind, hat der Verpflichtete dem Bundesamt für Verfassungsschutz auch hierzu Auskunft zu geben.

(2) Wenn dem Verpflichteten eine Auskunft nach Absatz 1 Satz 2 Nummer 2 technisch nicht möglich oder zumutbar ist, ist er zur Auskunft nicht verpflichtet. In diesem Fall ist er verpflichtet, dem Bundesamt für Verfassungsschutz auf Ersuchen eine Kopie der Teile des informationstechnischen Systems herauszugeben, deren Auswertung zum Aufspüren der in Absatz 1 Satz 2 Nummer 2 bezeichneten Informationen erforderlich ist.

(3) Das Bundesamt für Verfassungsschutz darf um Übermittlung nach Absatz 1 nur ersuchen, wenn

1. sie im Einzelfall auf Grund tatsächlicher Anhaltspunkte erforderlich ist, um einen möglichen Angriff auf Telekommunikations- oder Datenverarbeitungssysteme aufzuklären, der unter Nutzung eines informationstechnischen Systems des Verpflichteten durchgeführt worden ist und

2. tatsächliche Anhaltspunkte dafür bestehen, dass der Angriff als Mittel einer Bedrohung dient, die wenigstens erheblich beobachtungsbedürftig ist.

Für die Herausgabe einer Kopie nach Absatz 2 Satz 2 gilt Satz 1 mit der Maßgabe, dass der Angriff als Mittel einer Bedrohung dient, die besonders erheblich beobachtungsbedürftig ist. Mit dem Ersuchen aufzuklären sind insbesondere die zum Angriff genutzte Infrastruktur und Technik sowie das Vorgehen und die Angriffsziele. Nach Maßgabe der Anordnung kann auch um Übermittlung künftig anfallender Daten ersucht werden.

(4) Das Bundesamt für Verfassungsschutz prüft die erhobenen Daten unverzüglich darauf, ob sie für die Aufklärung des Angriffs erforderlich sind, und löscht die nicht erforderlichen Daten unverzüglich. Bei Kopien nach Absatz 2 prüft das Bundesamt für Verfassungsschutz unverzüglich, ob neben den in Absatz 1 Satz 2 Nummer 2 bezeichneten Informationen noch weitere Daten erhoben worden sind und löscht diese weiteren Daten unverzüglich, soweit es sich nicht um Daten handelt, die durch den Angriff beschafft worden sind.

Die Löschung kann unterbleiben, wenn die Trennung von den Informationen, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unvertretbarem Aufwand möglich ist. Diese weiteren Daten dürfen nicht genutzt werden.

(5) Sind im informationstechnischen System des Verpflichteten Angriffswerkzeuge oder Daten, die durch den Angriff beschafft worden sind, gespeichert, darf der Verpflichtete diese nach Herstellung einer Sicherungskopie löschen. Eine Sicherungskopie ist dem Bundesamt für Verfassungsschutz herauszugeben.

(6) Kann nachträglich ausgeschlossen werden, dass ein Angriff im Rahmen einer Bedrohung vorlag, so hat das Bundesamt für Verfassungsschutz die nach Absatz 2 Satz 2 herausgegebene Kopie in der Verarbeitung einzuschränken. Die Daten dürfen nur noch zum Schutz von Interessen des betroffenen Nutzers des Dienstes verarbeitet werden. Das Bundesamt für Verfassungsschutz hat die Daten zu löschen

1. im Falle einer Mitteilung an die betroffene Person 6 Monate nach Mitteilung, wenn der betroffene Nutzer des Dienstes kein Interesse an weiterer Speicherung geltend gemacht hat, frühestens jedoch zum Ende des Kalenderjahres, das dem Jahr der Speicherung folgt,

2. im Falle des endgültigen Absehens von einer Mitteilung nach § 35 Absatz 3 unverzüglich.

(7) § 11 Absatz 6 und 7 ist anzuwenden.

§ 13

Verpflichtende Ersuchen an Anbieter von Telekommunikationsdiensten

(1) Auf Ersuchen des Bundesamtes für Verfassungsschutz nach § 9 Absatz 1 Satz 1 sind diejenigen, die öffentlich zugängliche Telekommunikationsdienste erbringen oder daran geschäftsmäßig mitwirken, verpflichtet, Auskunft zu ihren Diensten zu erteilen. § 11 Absatz 2, 3, 6 und 7 sind anzuwenden.

(2) Ein Ersuchen ist unzulässig, soweit die Auskunft im automatisierten Auskunftsverfahren von der Bundesnetzagentur nach § 173 Absatz 4 des Telekommunikationsgesetzes erlangt werden kann. Die Auskunft zu Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, darf nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. Wird um Auskunft anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse ersucht, sind die Rechtsgrundlage und die tatsächlichen Anhaltspunkte, die das Auskunftsverlangen veranlassen, aktenkundig zu machen.

(3) Ein Ersuchen um eine qualifizierte Auskunft ist nur zulässig

1. im Fall wenigstens erheblich beobachtungsbedürftiger Bedrohungen und nur

2. zu Personen nach § 22 Absatz 3.

Für Ersuchen zu Umständen von Telekommunikation genügt deren räumlich und zeitlich hinreichende Bezeichnung, sofern anderenfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre.

(4) Ersuchen zu Inhalten interpersoneller Telekommunikationsdienste sind nur zulässig

1. im Fall besonders erheblich beobachtungsbedürftiger Bedrohungen und nur

2. zu Personen nach § 22 Absatz 3 und nur,

3. wenn die Erforschung des Sachverhalts mit anderen Mitteln, mit Ausnahme von Maßnahmen nach den §§ 25 und 27 aussichtslos oder wesentlich erschwert wäre.

Die Verpflichteten müssen auf solches Ersuchen die ihnen zur Übermittlung anvertrauten Inhalte ausleiten und die Überwachung und Aufzeichnung der Telekommunikation ermöglichen, auch durch Zugangsgewährung zu ihren Einrichtungen während ihrer üblichen Geschäftszeiten.

(5) Im Falle einer vollziehbaren Anordnung nach §§ 23 bis 26 müssen die Verpflichteten auf Ersuchen die Einbringung von technischen Mitteln zur Durchführung einer Maßnahme des Bundesamtes für Verfassungsschutz durch Unterstützung bei der Umleitung von Telekommunikation ermöglichen

1. durch Mitteilung der zur Erbringung in den umgeleiteten Datenstrom erforderlichen Informationen über die Strukturen der von ihm betriebenen Telekommunikationsnetze und Telekommunikationsanlagen sowie die von ihm erbrachten Telekommunikationsdienste,

2. durch sonstige Unterstützung bei der Umleitung einschließlich der Gewährung des Zugangs zu seinen Einrichtungen während seiner üblichen Geschäftszeiten sowie der Ermöglichung der Aufstellung und des Betriebs von Geräten für die Durchführung der Maßnahme.

(6) Die nach Absatz 1 Verpflichteten haben sicherzustellen, dass die Geheimschutzmaßnahmen zum Schutz als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufter Informationen gemäß der nach § 35 Absatz 1 des Sicherheitsüberprüfungsgesetzes zu erlassenden allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz in der jeweils geltenden Fassung getroffen werden. Sie haben geeignetes Personal vorzuhalten, das zu einer einfachen Sicherheitsüberprüfung bereit ist. Bei qualifizierten Ersuchen oder deren Ankündigung haben die nach Absatz 1 Verpflichteten unverzüglich die Personen, die mit der Durchführung der Maßnahme betraut werden sollen,

1. auszuwählen,

2. einer einfachen Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz unterziehen zu lassen und

3. über Mitteilungsverbote nach § 9 Absatz 3 Nummer 1 sowie die Strafbarkeit eines Verstoßes nach § 73 Absatz 1 zu belehren; die Belehrung ist aktenkundig zu machen.

Mit der Durchführung eines qualifizierten Ersuchens dürfen nur Personen betraut werden, die nach Maßgabe des Satzes 3 Nummer 2 und 3 überprüft und belehrt worden sind. Das Bundesamt für Verfassungsschutz kann Ausnahmen von Satz 4 zulassen. Das Bundesministerium des Innern kann anordnen, dass Sicherheitsüberprüfungen bereits als organisatorische Vorkehrung zur künftigen unverzüglichen Umsetzung von Überwachungsmaßnahmen durchzuführen sind.

(7) Gegen Ersuchen nach Absatz 3 und 4 und deren Vollzug ist vor der Mitteilung an die betroffene Person der Rechtsweg für diese ausgeschlossen.

§ 14

Verpflichtende Ersuchen an Anbieter von Postdiensten

(1) Auf Ersuchen des Bundesamtes für Verfassungsschutz nach § 9 Absatz 1 Satz 1 sind diejenigen, die geschäftsmäßig Postdienste, einschließlich Warensendungen, erbringen oder daran geschäftsmäßig mitwirken, verpflichtet, Auskunft zu ihren Diensten zu erteilen. § 11 Absatz 2, 3, 6 und 7 und § 13 Absatz 3 Satz 1, Absatz 6 und 7 gelten entsprechend. Abgeordnetenpost von Mitgliedern des Europäischen Parlaments, des Deutschen Bundestages oder eines Landesparlaments darf nicht in eine Maßnahme einbezogen werden, die sich gegen einen Dritten richtet.

(2) Zur Auskunft über Postinhalte sind Ersuchen nur im Falle besonders erheblich beobachtungsbedürftiger Bedrohungen zulässig und nur, wenn die Erforschung des Sachverhalts mit anderen Mitteln, mit Ausnahme von Maßnahmen nach den §§ 25 und 27 aussichtslos oder wesentlich erschwert wäre. Zur Auskunft haben die Verpflichteten Sendungen, die ihnen zum Einsammeln, Weiterleiten oder Ausliefern anvertraut sind, dem Bundesamt für Verfassungsschutz auszuhändigen.

§ 15

Verpflichtende Ersuchen an Verfügungsberechtigte von Einrichtungen zur Videoüberwachung

(1) Verfügungsberechtigte privater und öffentlicher Einrichtungen zur Videoüberwachung des öffentlich zugänglichen Raums haben auf Ersuchen des Bundesamtes für Verfassungsschutz

1. die Mitbenutzung der Einrichtung durch das Bundesamt für Verfassungsschutz zu ermöglichen und ihm zu diesem Zweck den Zutritt zu den Räumlichkeiten der Einrichtung zu gewähren,

2. Daten der Videoüberwachung in Echtzeit an das Bundesamt für Verfassungsschutz auszuleiten und

3. gespeicherte Bild- und Tonaufzeichnungen aus Videoüberwachung dem Bundesamt für Verfassungsschutz zu übermitteln.

Die Verpflichtung beschränkt sich auf den Einsatz der bei dem Verpflichteten vorhandenen technischen Mittel.

(2) Ein Ersuchen nach Absatz 1 Satz 1 ist nur im Fall wenigstens erheblich beobachtungsbedürftiger Bedrohungen zulässig. Führt das Ersuchen zu einer § 20 Absatz 2 entsprechenden längerfristigen optischen und akustischen Überwachung einer Person, so ist es nur im Fall besonders erheblich beobachtungsbedürftiger Bedrohungen zulässig. Ein Ersuchen um Übermittlung gespeicherter Bild- und Tonaufzeichnungen ist zeitlich einzugrenzen.

(3) Die nach Absatz 1 Satz 1 Nummer 3 übermittelten Bild- und Tonaufzeichnungen sind zu löschen, wenn

1. die Voraussetzungen nach Absatz 2 Satz 1 oder 2 nicht mehr vorliegen oder

2. die Aufzeichnungen zur Aufgabenerfüllung nicht mehr erforderlich sind.

Unterabschnitt 2

Nachrichtendienstliche Mittel

§ 16

Datenerhebungen mit nachrichtendienstlichen Mitteln

(1) Das Bundesamt für Verfassungsschutz darf Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung (nachrichtendienstliche Mittel) einsetzen, soweit dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zur Gewinnung von Erkenntnissen über Bedrohungen oder die zu deren Aufklärung erforderlichen verdeckten Hilfspersonen erforderlich ist. Dazu darf es insbesondere

1. durch eigene Bedienstete verdeckt ermitteln,

2. verdeckte Hilfspersonen einsetzen,

3. technische Mittel verdeckt einsetzen sowie

4. Sachen heimlich in Besitz zu nehmen, um sie nach den dafür geltenden Befugnissen auszuwerten.

Eine nach Satz 2 Nummer 4 in Besitz genommene Sache ist dem Eigentümer oder dem rechtmäßigen Inhaber der tatsächlichen Gewalt nach Abschluss der heimlichen Auswertung zurückzugeben, wenn keine überwiegenden Sicherheitsinteressen einer Rückgabe entgegenstehen.

(2) Bei der Verpflichtung von verdeckten Hilfspersonen ist § 1 Absatz 3 des Verpflichtungsgesetzes mit der Maßgabe anzuwenden, dass auch von der Unterzeichnung der Niederschrift durch die verpflichtete Person abgesehen werden kann, wenn dies im Interesse der inneren oder äußeren Sicherheit der Bundesrepublik Deutschland geboten ist.

(3) Das Bundesamt für Verfassungsschutz darf zur verdeckten Aufgabenwahrnehmung und zur Eigensicherung Legenden zur Tarnung von Bediensteten, verdeckten Hilfspersonen und Einrichtungen nutzen und Tarnpapiere und Tarnkennzeichen herstellen. Die für die Herstellung der Papiere und Kennzeichen zuständigen Behörden sind verpflichtet, dem Bundesamt für Verfassungsschutz bei der Beschaffung und Herstellung dieser Tarnmittel Hilfe zu leisten.

(4) Das Bundesamt für Verfassungsschutz hat die nachrichtendienstlichen Mittel in einer Dienstvorschrift abschließend zu benennen. Sind in den §§ 17 bis 27 nicht geregelte Mittel ihrer Art nach insbesondere unter Berücksichtigung der Ausnutzung dauerhafter persönlicher Vertrauensbeziehungen, einer weitgehenden Erfassung der Persönlichkeit oder des Anfallens höchstprivater Informationen vergleichbar gewichtig eingreifend wie Befugnisse, die eine erhebliche oder besonders erhebliche Beobachtungsbedürftigkeit voraussetzen, so dürfen sie nur zur Erprobung und nur dann in die Dienstvorschrift aufgenommen werden, wenn die Weiterverarbeitung der gewonnenen personenbezogenen Daten beschränkt wird

1. auf die Erprobung des Mittels,

2. die Aufklärung besonders erheblich beobachtungsbedürftiger Bedrohungen und

3. die Abwehr einer konkretisierten Gefahr für besonders gewichtige Rechtsgüter.

Die Erprobung ist höchstens 4 Jahre zulässig. Die Dienstvorschrift bedarf der Zustimmung des Bundesministeriums des Innern und in Bezug auf die Einhaltung der Vorgaben des Satzes 2 des Unabhängigen Kontrollrates. Das Bundesministerium des Innern unterrichtet das Parlamentarische Kontrollgremium über die Dienstvorschrift.

(5) Nachrichtendienstliche Mittel dürfen sich gezielt nur gegen Personen richten, zu denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie

1. Beteiligte einer Bedrohung sind oder

2. in einem Zusammenhang mit einer Bedrohung stehen, der Grund zu der Annahme gibt, dass durch die Maßnahme Erkenntnisse über die Bedrohung gewonnen werden können, die nicht gleichermaßen durch Maßnahmen nach Nummer 1 zu gewinnen sind.

Wenn es sich bei der Tätigkeit, die der Bedrohung zugrunde liegt, um eine Tätigkeit für einen ausländischen Staat handelt, dürfen zur Aufklärung von Bedrohungen nach § 3 Absatz 4 Nummer 2 und 3 sich nachrichtendienstliche Mittel auch gegen Personen richten, die für diesen Staat hoheitliche Aufgaben wahrnehmen. Zur Gewinnung von Erkenntnissen über die zur Aufklärung von Bedrohungen erforderlichen verdeckten Hilfspersonen dürfen sich nachrichtendienstliche Mittel auch gegen diese Personen richten. Maßnahmen, die nur bei besonders erheblich beobachtungsbedürftigen Bedrohungen zulässig sind, dürfen sich nicht gegen Personen nach Satz 1 Nummer 2 richten und gegen verdeckte Hilfspersonen nur auf Grund tatsächlicher Anhaltspunkte für deren funktionsgefährdende Tätigkeit. Der Maßnahme steht nicht entgegen, wenn andere Personen unvermeidbar mit betroffen sind.

(6) [Unter den Voraussetzungen eines Einsatzes nachrichtendienstlicher Mittel darf das Bundesamt für Verfassungsschutz zu dessen Vorbereitung und Durchführung Gebäude und Räume, die keine Wohnung sind, auch ohne Wissen des Inhabers betreten. Im Falle einer Wohnung gilt dies nur bei konkretisierter Gefahr für besonders gewichtige Rechtsgüter und nur auf Grund besonderer Anordnung. Für Wohnraumüberwachung und Einsatzsicherung gelten die §§ 27 und 28.]

§ 17

Internetermittlungen auf vertiefter Vertrauensbasis

Das Bundesamt für Verfassungsschutz darf über Internetlegenden bestehende Kontakte eigener Bediensteter zu einer Zielperson nur im Fall wenigstens erheblich beobachtungsbedürftiger Bedrohungen durch Treffen mit der Zielperson in physischer Präsenz oder durch mindestens dreimalige wirtschaftliche Zuwendungen zugunsten der Zielperson festigen.

§ 18

Vertrauenspersonen

(1) Über die Verpflichtung von Privatpersonen, deren planmäßige, dauerhafte Zusammenarbeit mit dem Bundesamt für Verfassungsschutz Dritten nicht bekannt ist (Vertrauenspersonen), entscheidet die Amtsleitung oder eine dazu ermächtigte Abteilungsleitung. Als Vertrauenspersonen zur Aufklärung von verfassungsfeindlichen Bestrebungen dürfen nicht Personen angeworben und eingesetzt werden, die

1. nicht voll geschäftsfähig, insbesondere minderjährig sind,

2. von den Geld- oder Sachzuwendungen für die Tätigkeit auf Dauer als alleinige Lebensgrundlage abhängen würden,

3. an einem Aussteigerprogramm teilnehmen,

4. Mitglied des Europäischen Parlaments, des Deutschen Bundestages, eines Landesparlaments oder Bedienstete eines solchen Mitglieds sind oder

5. im Bundeszentralregister mit einer Verurteilung wegen eines Verbrechens oder zu einer Freiheitsstrafe, deren Vollstreckung nicht zur Bewährung ausgesetzt worden ist, eingetragen sind.

Ist der Einsatz zur Aufklärung besonders erheblich beobachtungsbedürftiger Bestrebungen unerlässlich, kann die Amtsleitung eine Ausnahme zulassen von Satz 1 Nummer 1 bei einer Person, die mindestens 16 Jahre alt ist, von Satz 1 Nummer 2 für einen zeitlich zu begrenzenden Einsatz und von Satz 1 Nummer 5 bei einer Person, die nicht als Täter eines Totschlags (§§ 212 und 213 des Strafgesetzbuches) oder einer allein mit lebenslanger Haft bedrohten Straftat verurteilt worden ist. Im Fall einer Ausnahme von Satz 1 Nummer 1 sind bei der Führung des Jugendlichen Belange der Fürsorge besonders zu berücksichtigen. Im Fall einer Ausnahme von Satz 1 Nummer 5 ist der Einsatz nach höchstens 6 Monaten zu beenden, wenn er zur Erforschung der Bedrohungen nicht zureichend gewichtig beigetragen hat. Wird der Einsatz nicht beendet, ist im Weiteren die Qualität der gelieferten Informationen fortlaufend zu bewerten.

(2) Das Bundesamt für Verfassungsschutz darf nur dann, wenn wenigstens erheblich beobachtungsbedürftige Bedrohungen vorliegen, Vertrauenspersonen

1. im jeweiligen Aufklärungsfeld länger als 6 Monate, beginnend mit den Beschaffungsaufträgen, einsetzen oder

2. gegen Personen nach § 16 Absatz 5 Satz 1 Nummer 2 einsetzen.

Der gezielte Einsatz gegen eine Person, zu der die Vertrauensperson eine besonders persönliche Vertrauensbeziehung unterhält, ist nur im Fall von besonders erheblich beobachtungsbedürftigen Bedrohungen zulässig.

(3) In den §§ 53 und 53a der Strafprozessordnung genannte Berufsgeheimnisträger und mitwirkende Personen dürfen nicht in dieser Eigenschaft zur Beschaffung von Informationen, die dem Zeugnisverweigerungsrecht unterliegen, eingesetzt werden.

(4) Im Einsatz dürfen zum Zweck der Informationsgewinnung keine intimen Beziehungen oder vergleichbar engste persönliche Bindungen begründet oder fortgeführt werden. Entstehen solche Bindungen zu einer Person, so ist der Einsatz gegen diese abzubrechen. Das Bundesamt für Verfassungsschutz hat darauf hinzuwirken, dass die Vertrauensperson zur Einsatzdurchführung gespeicherte kernbereichsrelevante Informationen löscht und ihm solche Informationen nicht an das Bundesamt für Verfassungsschutz übermittelt. Wird dem Bundesamt für Verfassungsschutz bekannt, dass die Vertrauensperson im Einsatz kernbereichsrelevante Informationen gewonnen hat, so hat es diesen Umstand auch unabhängig von einer Übermittlung von Inhalten zu dokumentieren. Darüber hinaus gilt zum Kernbereichsschutz § 31.

(5) Vertrauenspersonen dürfen weder zur Gründung von verfassungsfeindlichen Bestrebungen noch zur steuernden Einflussnahme auf diese eingesetzt werden. Sie dürfen in solchen Personenzusammenschlüssen oder für solche Personenzusammenschlüsse, einschließlich strafbaren Vereinigungen, eingesetzt werden, um deren Bestrebungen aufzuklären. Im Übrigen ist im Einsatz eine Beteiligung der Vertrauensperson an Bedrohungen zulässig, wenn sie

1. nicht in Individualrechte eingreift,

2. von den an den Bedrohungen Beteiligten derart erwartet wird, dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich ist, und

3. nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts steht.

Sofern zureichende Anhaltspunkte dafür bestehen, dass die Vertrauensperson im Einsatz rechtswidrig einen Straftatbestand von erheblicher Bedeutung verwirklicht hat, soll ihr Einsatz unverzüglich beendet und die Strafverfolgungsbehörde unterrichtet werden. Über Ausnahmen nach Satz 4 entscheidet die Amtsleitung.

(6) Die Staatsanwaltschaft kann von der Verfolgung von im Einsatz begangenen Vergehen absehen, wenn die Tat von den übrigen Beteiligten derart erwartet wurde, dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich war. Dabei ist das Verhältnis der Bedeutung der Aufklärung des Sachverhalts zur Schwere der begangenen Straftat und Schuld des Täters zu berücksichtigen. Ein Absehen von der Verfolgung ist ausgeschlossen, wenn eine höhere Strafe als 1 Jahr Freiheitsstrafe zu erwarten ist. Ein Absehen von der Verfolgung ist darüber hinaus stets ausgeschlossen, wenn zu erwarten ist, dass die Strafe nicht zur Bewährung ausgesetzt werden würde. Bei Vergehen, die mit einer im Mindestmaß erhöhten Strafe bedroht sind und bei denen die durch die Tat verursachten Folgen nicht gering sind, bedarf es der Zustimmung des für die Eröffnung des Hauptverfahrens zuständigen Gerichts. Ist die Klage bereits erhoben, so kann das Gericht in jeder Lage des Verfahrens unter den Voraussetzungen des Satzes 1 mit Zustimmung der Staatsanwaltschaft und des Angeschuldigten das Verfahren einstellen. Die Sätze 1 bis 6 gelten auch in Fällen der Landesbehörden für Verfassungsschutz.

(7) Eine Vertrauensperson darf zum Eigenschutz ihre Tätigkeit als Vertrauensperson gegenüber Dritten verleugnen. Dies gilt nicht in Strafverfahren oder parlamentarischen Verfahren. In Strafverfahren ist ausgeschlossen, über die Tatsache einer Tätigkeit als Vertrauensperson Beweis zu erheben.

§ 19

Verdeckte Bedienstete

(1) Für den Einsatz von eigenen Bediensteten, die unter einer ihnen verliehenen und auf Dauer angelegten Legende handeln (Verdeckte Bedienstete), gilt § 18 Absatz 2 bis 7 entsprechend. Jeder Einsatz gegen eine bestimmte Person, der auf die Herstellung von Vertrauensbeziehungen angelegt ist, ist nur im Fall wenigstens erheblich beobachtungsbedürftiger Bedrohungen zulässig.

(2) Verdeckte Bedienstete dürfen unter Verwendung ihrer Legende eine Wohnung mit dem Einverständnis des Berechtigten betreten. Das Einverständnis darf nicht durch ein über die Nutzung der Legende hinausgehendes Vortäuschen eines Zutrittsrechts herbeigeführt werden.

§ 20

Längerfristige optische und akustische Überwachung

(1) Das Bundesamt für Verfassungsschutz darf nur im Fall wenigstens erheblich beobachtungsbedürftiger Bedrohungen gegen bestimmte Personen

1. Observationen durchführen, auch unter Einsatz unterstützender technischer Mittel,

a) durchgehend 48 oder mehr Stunden,

b) an 7 oder mehr Tagen innerhalb eines Zeitraums von 30 Tagen oder

2. mit technischen Mitteln zur optischen oder akustischen Überwachung das Verhalten im nicht öffentlich zugänglichen Raum aufzeichnen.

(2) Das Bundesamt für Verfassungsschutz darf nur im Fall besonders erheblich beobachtungsbedürftiger Bedrohungen gegen bestimmte Personen

1. Observationen durchgehend 7 Tage oder länger, auch unter Einsatz unterstützender technischer Mittel, durchführen oder

2. mit technischen Mitteln zur optischen oder akustischen Überwachung das Verhalten im nicht öffentlich zugänglichen Raum aufzeichnen, wenn mit der Erfassung von höchstprivaten Informationen zu rechnen ist.

(3) Die Absätze 1 und 2 gelten nicht bei Maßnahmen zum Schutz eingesetzter Personen. Eine technische Datenerhebung aus Wohnungen ist nur nach § 27 zulässig.

§ 21

Längerfristige Bewegungsüberwachung

(1) Technische Mittel zur Standortfeststellung bestimmter Personen darf das Bundesamt für Verfassungsschutz einsetzen

1. nur im Fall wenigstens erheblich beobachtungsbedürftiger Bedrohungen

a) 7 Tage oder länger im durchgehenden Einsatz,

b) an 14 oder mehr einzelnen Tagen innerhalb eines Zeitraums von 30 Tagen im täglich durchgehenden Einsatz oder

c) in einer Weise, die ein den Buchstaben a und b in der Persönlichkeitsrelevanz gleichwertiges Bewegungsprofil ergibt.

2. nur im Fall besonders erheblich beobachtungsbedürftiger Bedrohungen

a) 30 Tage oder länger im durchgehenden Einsatz,

b) an 5 oder mehr Wochen innerhalb eines Zeitraums von 60 Tagen im wöchentlich durchgehenden Einsatz oder

c) in einer Weise, die ein den Buchstaben a und b in der Persönlichkeitsrelevanz gleichwertiges Bewegungsprofil ergibt.

(2) Der Einsatz ist im Sinne des Absatzes 1 durchgehend, wenn er ermöglicht, die Bewegung der Person über den Zeitraum zusammenhängend zu überwachen.

§ 22

Überwachung von Brief-, Post- und Telekommunikationsverkehren

(1) Das Bundesamt für Verfassungsschutz darf nur im Falle besonders erheblich beobachtungsbedürftiger Bedrohungen Brief- und Postsendungen öffnen und einsehen sowie Telekommunikationsverkehre überwachen und aufzeichnen. Die Überwachung ist auch im Falle erheblich beobachtungsbedürftiger Bedrohungen zulässig, wenn sie beschränkt ist auf

1. Umstände der Brief-, Post- und Telekommunikationsverkehre oder

2. Inhalte von Telekommunikationsdiensten (§ 3 Nummer 61 des Telekommunikationsgesetzes), die nicht interpersonelle Telekommunikationsdienste sind.

Inhalte interpersoneller Kommunikation dürfen bei der Überwachung nur erhoben werden, wenn die Erforschung des Sachverhalts mit anderen Mitteln, mit Ausnahme von Maßnahmen nach den §§ 25 und 27, aussichtslos oder wesentlich erschwert wäre. In Brief- und Postsendungen darf das Bundesamt für Verfassungsschutz auch technische Mittel einbringen, um Informationen zur Aufklärung der Bedrohung zu gewinnen, wenn es zum Einsatz des technischen Mittels befugt ist. Abgeordnetenpost von Mitgliedern des Europäischen Parlaments, des Deutschen Bundestages oder eines Landesparlaments darf nicht in eine Maßnahme einbezogen werden, die sich gegen eine dritte Person richtet.

(2) Die Überwachung von Telekommunikationsverkehren ist begrenzt auf die Erhebung von Inhalten und Umständen der Informationsübermittlung an Dritte oder von Dritten (Kommunikation). Die Weiterverarbeitung sonstiger personenbezogener Daten, die durch die überwachte Telekommunikation übertragen werden, ist nur unter den Voraussetzungen der §§ 23, 25 und 26 zulässig. Im Übrigen löscht das Bundesamt für Verfassungsschutz solche sonstigen personenbezogenen Daten und protokolliert dies. Auf verbundene Daten ist § 23 Absatz 6 anzuwenden. Das Löschungsprotokoll ist nach § 31 Absatz 7 Satz 3 Nummer 1 und 2 zu löschen. Ein Eingriff in die Integrität privater informationstechnischer Systeme ist nur unter den Voraussetzungen von §§ 25 und 26 zulässig. Bei einem Eingriff in die Integrität anderer informationstechnischer Geräte ist § 23 Absatz 4 anzuwenden.

(3) Die Maßnahme darf sich nur richten gegen Personen, zu denen tatsächliche Anhaltspunkte dafür vorliegen, dass

1. sie Beteiligte der aufzuklärenden Bedrohung sind,

2. sie für Beteiligte Mitteilungen entgegennehmen oder weitergeben oder

3. im Falle der Erhebung von Telekommunikationsdaten Personen nach Nummer 1 oder 2 ihren Anschluss benutzen.

Tatsächlicher Anhaltspunkt, Beteiligter zu sein, ist auch die Teilnahme an einer Kommunikationsgruppe, zu der tatsächliche Anhaltspunkte bestehen, dass sie im Wesentlichen zur Kommunikation für Zwecke der Bedrohung genutzt wird.

(4) Das Bundesamt für Verfassungsschutz prüft unverzüglich und im Abstand von höchstens 2 Jahren, ob die erhobenen personenbezogenen Daten für die Zwecke nach § 1 Absatz 1 erforderlich sind. Soweit die Daten für diese Zwecke oder eine zulässige Übermittlung nicht erforderlich sind, sind Aufzeichnungen unverzüglich zu löschen. Die Löschung ist zu protokollieren. Das Protokoll ist zu löschen

1. im Falle einer Mitteilung an die betroffene Person 6 Monate nach der Mitteilung, wenn der Betroffene kein Interesse an weiterer Speicherung für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Beschränkungsmaßnahme geltend gemacht hat,

frühestens jedoch zum Ende des zweiten Kalenderjahres, das dem Jahr der Protokollierung folgt,

2. im Falle des endgültigen Absehens von einer Mitteilung nach § 35 Absatz 3 unverzüglich.

Die Löschung kann unterbleiben, wenn die Trennung der nicht erforderlichen personenbezogenen Daten von den Informationen, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unvertretbarem Aufwand möglich ist. Diese weiteren Daten dürfen nicht genutzt werden.

(5) Gegen Anordnung und Vollzug der Maßnahmen ist der Rechtsweg vor der Mitteilung an die betroffene Person ausgeschlossen.

§ 23

Auslesen informationstechnischer Geräte

(1) Das Bundesamt für Verfassungsschutz darf in informationstechnische Geräte nur im Fall wenigstens erheblich beobachtungsbedürftiger Bedrohungen nachrichtendienstlich eingreifen. Nachrichtendienstlich eingreifen ist

1. die Zugangsverschaffung mit nachrichtendienstlichen Mitteln zum Auslesen gespeicherter personenbezogener Daten,

2. das Auslesen gespeicherter personenbezogener Daten nach

   a) Zugangsverschaffung nach Nummer 1 oder

   b) Erhalt des informationstechnischen Geräts von einem ausländischen Nachrichtendienst.

Das Bundesamt für Verfassungsschutz prüft die erlangten Daten darauf, ob sie für die Aufklärung der Bedrohungen erforderlich sind, und löscht die nicht erforderlichen Daten unverzüglich.

(2) Ist bei einer Maßnahme, die nicht zur Aufklärung besonders erheblich beobachtungsbedürftiger Bedrohungen erfolgt, nach den Umständen des Einzelfalls zu erwarten, dass die auszulesenden Informationen auch Informationen enthalten werden, die nach Absatz 3 besonders schutzwürdig sind, sind die ausgelesenen Daten ohne vorherige Kenntnisnahme dem Aufsichtsbediensteten (§ 31 Absatz 5 Satz 2) zur Vorprüfung vorzulegen. Er entscheidet über eine Beschränkung der Weiterverarbeitung nach Absatz 3.

(3) Ergeben die ausgelesenen Daten umfassende Informationen über Lebensbereiche einer Person oder systematisch gesammelte höchstprivate Informationen, so dürfen diese Daten zum Zweck der Maßnahme nur weiterverarbeitet werden, wenn die Maßnahme wegen einer besonders erheblich beobachtungsbedürftigen Bedrohung erfolgt. Ist dies nicht der Fall, sind Daten, die nicht zur Abwehr einer konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut nach § 46 zu übermitteln sind, unverzüglich zu löschen.

(4) An dem informationstechnischen System dürfen nur solche Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind. Sie sind bei Beendigung der Maßnahme, soweit technisch und ohne Gefährdung des Zwecks der Maßnahme möglich, automatisiert rückgängig zu machen. Dies gilt nicht wenn tatsächlichen Anhaltspunkte im Einzelfall dafür vorliegen, dass die Veränderung in absehbarer Zeit erneut zur Durchführung einer nachrichtendienstlichen Maßnahme erforderlich ist. Das eingesetzte Mittel ist nach

dem Stand der Technik gegen unbefugte Nutzung zu schützen. Bei jedem Einsatz sind zu dokumentieren

1. die Bezeichnung des technischen Mittels und der Zeitraum seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

4. die Organisationseinheit, die die Maßnahme durchführt.

(5) Ein nachrichtendienstlicher Eingriff in die Integrität privater informationstechnischer Systeme ist nur unter den Voraussetzungen der §§ 25, 26 zulässig. Die Weiterverarbeitung der aus dem informationstechnischen Gerät ausgelesenen Daten, um aus ihnen ein Verhaltens- oder Persönlichkeitsprofil zu erstellen, ist nur unter den Voraussetzungen des § 25 zulässig.

(6) Eine Löschung nach Absatz 1 Satz 2 oder Absatz 3 Satz 2 kann unterbleiben, wenn die Trennung der nicht erforderlichen personenbezogenen Daten von anderen Informationen, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unvertretbarem Aufwand möglich ist. Diese weiteren Daten dürfen nicht genutzt werden.

§ 24

Auslesen technischer Spuren von informationstechnischen Angriffen

(1) Soweit in den Fällen des § 12 die Informationen nicht oder nicht ohne Gefährdung des Zwecks der Maßnahme durch Übermittlung des Verpflichteten gewonnen werden können, darf das Bundesamt für Verfassungsschutz zur Erhebung der Informationen in das informationstechnische System des Verpflichteten nachrichtendienstliche eingreifen. Die Ausleitung einer Kopie der Teile des informationstechnischen Systems, deren Auswertung zum Aufspüren der Informationen erforderlich ist, ist nur zulässig, wenn das Aufspüren im informationstechnischen System nicht oder nicht ohne Gefährdung des Zwecks der Maßnahme möglich ist. Auf die erhobenen Daten ist § 12 Absatz 4 und 6 anzuwenden. Zum Schutz des informationstechnischen Systems und zur Dokumentation der Maßnahme ist § 23 Absatz 4 anzuwenden.

(2) Stellt das Bundesamt für Verfassungsschutz bei einer Maßnahme nach Absatz 1 Angriffswerkzeuge oder Daten, die durch den Angriff beschafft worden sind, fest, darf es sie im informationstechnischen System nach Herstellung einer Sicherungskopie löschen, wenn geeignete polizeiliche Hilfe nicht rechtzeitig erlangt werden kann.

§ 25

Eingriff in die Integrität privater informationstechnischer Systeme

(1) In ein privates informationstechnisches System darf das Bundesamt für Verfassungsschutz vorbehaltlich des § 26 nur nachrichtendienstlich eingreifen im Falle einer konkretisierten Gefahr für besonders gewichtige Rechtsgüter durch eine besonders erheblich beobachtungsbedürftige Bedrohung. Privat ist ein informationstechnisches System, wenn es als eigenes privat genutzt wird und aufgrund seiner technischen Funktionalität allein oder durch technische Vernetzung Daten derart vorhalten kann, dass Umfang und Vielfalt der Daten einen Einblick in wesentliche Teile der Lebensgestaltung der Person oder ein aussagekräftiges Bild der Persönlichkeit ermöglichen. Die Maßnahme ist nur zulässig, wenn

die Erforschung des Sachverhalts auf andere Weise mit Ausnahme von Maßnahmen nach § 27 aussichtslos oder wesentlich erschwert wäre und geeignete polizeiliche Hilfe für das gefährdete Rechtsgut ansonsten nicht rechtzeitig erlangt werden kann.

(2) Eine Maßnahme nach Absatz 1 darf sich nur gegen Personen richten, zu denen tatsächliche Anhaltspunkte vorliegen, dass

1. sie an der konkretisierten Gefahr beteiligt sind oder

2. in ihrem informationstechnischen System von Personen nach Nummer 1 Informationen verarbeitet werden und die zur Aufklärung der Gefahr erforderlichen Informationen nicht gleichermaßen nach Nummer 1 zu gewinnen sind.

Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidlich betroffen werden.

(3) Das Bundesamt für Verfassungsschutz prüft und löscht die nach Absatz 1 erhobenen personenbezogenen Daten gemäß § 22 Absatz 4 mit der Maßgabe, dass an die Stelle der Zwecke nach § 1 Absatz 1 die Zwecke nach Absatz 5 treten.

(4) Die verbleibenden Daten sind zu kennzeichnen. Die Amtsleitung oder eine von ihr dazu ermächtigte Abteilungsleitung des Bundesamtes für Verfassungsschutz kann anordnen, dass bei der Übermittlung auf die Kennzeichnung verzichtet wird, wenn dies unerlässlich ist, um die Geheimhaltung einer Maßnahme nicht zu gefährden, und der Unabhängige Kontrollrat zugestimmt hat. Bei Gefahr im Verzug kann die Übermittlung bereits vor der Zustimmung erfolgen. Wird die Zustimmung versagt, ist die Kennzeichnung durch den Übermittlungsempfänger unverzüglich nachzuholen. Der Empfänger gekennzeichneter Daten prüft unverzüglich, ob die Daten zu löschen sind. Er trifft angemessene organisatorische Vorkehrungen, dass künftig zu löschende Daten gelöscht werden. Das Bundesamt für Verfassungsschutz hat den Übermittlungsempfänger von diesen Pflichten zu unterrichten.

(5) Das Bundesamt für Verfassungsschutz darf die nach Absatz 1 erhobenen personenbezogenen Daten nur weiterverarbeiten, einschließlich übermitteln,

1. soweit dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist zur Abwehr einer konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut oder

2. wenn bestimmte Tatsachen den Verdacht einer in § 100b Absatz 2 der Strafprozessordnung bezeichneten Straftat begründen und soweit die Daten zur Verfolgung dieser Straftat erforderlich sind.

(6) Zum Schutz des informationstechnischen Systems und zur Dokumentation der Maßnahme ist § 23 Absatz 4 anzuwenden.

§ 26

Abgegrenzter Eingriff in die Integrität privater informationstechnischer Systeme

(1) In ein privates informationstechnisches System darf das Bundesamt für Verfassungsschutz zur abgegrenzten Datenerhebung nur im Falle erheblich beobachtungsbedürftiger Bedrohungen nachrichtendienstlich eingreifen. Abgegrenzt ist eine Datenerhebung, die auf Erkenntnisse aus bestimmten abgegrenzten Teilen der Datenverarbeitung im informationstechnischen System und hierbei auf bestimmte Arten von Daten zielt. Durch eine Mehrzahl von Eingriffen dürfen nicht die Voraussetzungen des § 25 umgangen werden.

(2) Eine abgegrenzte Datenerhebung nach Absatz 1 Satz 1 ist nur im Fall besonders erheblich beobachtungsbedürftiger Bedrohungen zulässig, wenn sie auf die Erfassung zielt von

1. Inhaltsdaten interpersoneller Kommunikation, die ohne Begrenzung auf einzelne Kommunikationsvorgänge erhoben werden sollen, oder

2. Daten, die vergleichbar gewichtige Einblicke in die Lebensführung ermöglichen.

Daten im Sinne des Satzes 1 Nummer 2 sind insbesondere umfassende bildliche Dokumentationen.

(3) Wird im Falle des Absatzes 2 Satz 1 Nummer 1 die laufende Nutzung von Internetzugangsdiensten und interpersonellen Telekommunikationsdiensten überwacht, darf sich die Maßnahme nur gegen Personen nach § 22 Absatz 3 richten.

(4) Bei Maßnahmen nach Absatz 1 Satz 1 ist technisch sicherzustellen, dass nur die Daten erhoben werden, auf die die Maßnahme zielt. Ist dies in Ausnahmefällen nicht möglich, löscht das Bundesamt für Verfassungsschutz sonstige Daten unverzüglich und protokolliert dies. Auf verbundene Daten ist § 23 Absatz 5 anzuwenden. Das Löschungsprotokoll ist nach § 22 Absatz 5 Satz 4 Nummer 1 und 2 zu löschen. Bei der Überwachung von Telekommunikation gilt § 22 Absatz 4 und 5 entsprechend.

(5) Eine Auswertung zur Erstellung von Verhaltens- und Persönlichkeitsprofilen zur Bewertung des individuellen Bedrohungspotenzials einer Person ist nur unter den Voraussetzungen des § 25 zulässig.

(6) Zum Schutz des informationstechnischen Systems und zur Dokumentation der Maßnahme ist § 23 Absatz 4 anzuwenden.

§ 27

Wohnraumüberwachung

(1) Das Bundesamt für Verfassungsschutz darf ohne Wissen der betroffenen Person mit technischen Mitteln personenbezogene Daten aus einer Wohnung erheben und aufzeichnen, wenn

1. dies im Einzelfall zur Abwehr einer dringenden Gefahr für besonders gewichtige Rechtsgüter erforderlich ist,

2. die Erforschung des Sachverhalts durch das Bundesamt für Verfassungsschutz mit anderen Mitteln aussichtslos oder wesentlich erschwert wäre,

3. geeignete polizeiliche Hilfe für das bedrohte Rechtsgut ansonsten nicht rechtzeitig erlangt werden kann und

4. auf Grund tatsächlicher Anhaltspunkte, insbesondere zu der Art der zu überwachenden Räumlichkeiten und dem Verhältnis der zu überwachenden Personen zueinander, anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden.

(2) Die Maßnahme darf sich nur gegen eine Person richten, zu der tatsächliche Anhaltspunkte dafür vorliegen, dass sie an der dringenden Gefahr beteiligt ist. In die Überwachung einbezogen werden dürfen nur

1. die Wohnung dieser Person,

2. eine andere Wohnung, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass diese Person sich dort zur Zeit der Überwachung aufhält und diese Maßnahme für die Erforschung des Sachverhalts relevante Informationen ergeben wird, die nicht durch eine Überwachung der Wohnung der Person nach Nummer 1 zu gewinnen sind.

(3) Auf die erlangten Aufzeichnungen sind zur Prüfung der Erforderlichkeit und zur Löschung § 22 Absatz 4 mit der Maßgabe anzuwenden, dass die Daten für die Zwecke nach Absatz 4 erforderlich sein müssen. Für die Kennzeichnung der verbleibenden Daten gilt § 25 Absatz 4.

(4) Das Bundesamt für Verfassungsschutz darf die nach Absatz 1 Satz 1 erhobenen personenbezogenen Daten nur weiterverarbeiten, einschließlich übermitteln,

1. soweit dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist zur Abwehr einer dringenden Gefahr für ein besonders gewichtiges Rechtsgut oder

2. wenn bestimmte Tatsachen den Verdacht einer in § 100b Absatz 2 der Strafprozessordnung bezeichneten Straftat begründen, jedoch beschränkt auf Informationen aus akustischer Überwachung und nur soweit diese zur Verfolgung dieser Straftat erforderlich sind.

Aufgezeichnete Daten dürfen nur nach Zustimmung oder Freigabe gemäß § 31 Absatz 6 genutzt oder übermittelt werden.

§ 28

Einsatzsicherung

(1) Sind Bedienstete des Bundesamtes für Verfassungsschutz oder verdeckte Hilfspersonen im nachrichtendienstlichen Einsatz nach diesem Unterabschnitt tätig, darf das Bundesamt für Verfassungsschutz unmittelbaren Zwang anwenden, soweit dies erforderlich ist, um eine gegenwärtige Gefahr für ihr Leben, ihre körperliche Unversehrtheit oder ihre Freiheit oder für eingesetzte Sachen von bedeutendem Wert abzuwehren. Satz 1 ist auch anzuwenden, wenn die Bediensteten des Bundesamtes für Verfassungsschutz während des Einsatzes nach diesem Unterabschnitt eine solche Gefahr für Dritte oder deren Sachen feststellen. Für die Anwendung von unmittelbarem Zwang gelten die §§ 4, 5, 8 und 10 Absatz 1 Nummer 1 und 2 sowie der §§ 12 bis 14 des Gesetzes über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes entsprechend. Unmittelbaren Zwang anwenden dürfen nur Bedienstete des Bundesamtes für Verfassungsschutzes, die nach einer besonderen Schulung durch die Amtsleitung mit Eigensicherungsaufgaben betraut wurden (besondere Vollzugskräfte).

(2) Sind Bedienstete des Bundesamtes für Verfassungsschutz oder verdeckte Hilfspersonen zur heimlichen Informationsgewinnung in einer Wohnung tätig, darf das Bundesamt für Verfassungsschutz im Beisein der eingesetzten Person oder im unmittelbaren zeitlichen Zusammenhang mit dem Einsatz personenbezogene Daten heimlich mit technischen Mitteln aus der Wohnung erheben und aufzeichnen, soweit dies zur Abwehr von Gefahren für das Leben, die körperliche Unversehrtheit oder die Freiheit der eingesetzten Person unerlässlich ist. Das Bundesamt für Verfassungsschutz darf die erhobenen personenbezogenen Daten nur weiterverarbeiten, einschließlich übermitteln,

1. zur Eigensicherung nach Satz 1,

2. zur sonstigen Gefahrenabwehr sowie

3. zur Strafverfolgung.

§ 29

Besonderer Einsatz nachrichtendienstlicher Mittel

Werden nachrichtendienstliche Mittel, soweit ihr Einsatz nicht bereits in den §§ 17 bis 28 geregelt ist, ausnahmsweise so eingesetzt, dass sie unter Berücksichtigung der Ausnutzung dauerhafter persönlicher Vertrauensbeziehungen, einer weitgehenden Erfassung der Persönlichkeit oder des Anfallens höchstprivater Informationen vergleichbar gewichtig sind

1. wie die erheblich eingreifenden Maßnahmen nach § 17, § 18 Absatz 2 Satz 1, auch in Verbindung mit § 19, sowie nach § 20 Absatz 1, § 21 Absatz 1 Satz 1 Nummer 1, § 22 Absatz 1 Satz 2 und § 23 Absatz 1, so dürfen sie nur im Fall wenigstens erheblich beobachtungsbedürftiger Bedrohungen durchgeführt werden.

2. wie die besonders erheblich eingreifenden Maßnahmen nach § 18 Absatz 2 Satz 2, auch in Verbindung mit § 19, sowie nach § 20 Absatz 2, § 21 Absatz 1 Satz 1 Nummer 2, § 22 Absatz 1 Satz 1 (Erhebung von Kommunikationsinhalten) und § 23 Absatz 3, so dürfen sie nur im Fall besonders erheblich beobachtungsbedürftiger Bedrohungen durchgeführt werden.

§ 30

Allgemeine Schranken nachrichtendienstlicher Mittel

(1) In Individualrechte darf nur nach Maßgabe spezieller Befugnisse eingegriffen werden.

(2) Der Einsatz nachrichtendienstlicher Mittel ist unzulässig, wenn die Erforschung des Sachverhalts auf andere, die betroffene Person oder ein rechtlich geschütztes öffentliches Interesse weniger beeinträchtigende Weise möglich ist. Eine geringere Beeinträchtigung ist in der Regel anzunehmen, wenn die Information aus allgemein zugänglichen Quellen oder durch eine Übermittlung nach den §§ 8 bis 13 gewonnen werden kann.

(3) Die Beeinträchtigung rechtlich geschützter Interessen durch Anwendung eines nachrichtendienstlichen Mittels darf nicht erkennbar außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhaltes stehen.

(4) Eine Maßnahme ist unverzüglich zu beenden, wenn ihr Zweck erreicht ist oder sich ergibt, dass der Zweck nicht oder nicht auf diese Weise erreicht werden kann.

§ 31

Schutz des Kernbereichs privater Lebensgestaltung

(1) Der Einsatz nachrichtendienstlicher Mittel zur Erhebung personenbezogener Daten ist unzulässig,

1. wenn der Einsatz zur Erlangung von Erkenntnissen über den Kernbereich privater Lebensgestaltung (kernbereichsrelevante Informationen) erfolgt, oder

2. soweit tatsächliche Anhaltspunkte dafür vorliegen, dass durch den Einsatz allein kernbereichsrelevante Informationen gewonnen werden würden.

Bei einer Planung des Einsatzes ist darauf hinzuwirken, dass die Erlangung kernbereichsrelevanter Informationen vermieden wird. Beim Einsatz von Vertrauenspersonen und Verdeckten Bediensteten gilt § 18 Absatz 4. Beim Eingriff in private informationstechnische Systeme nach den §§ 25 und 26 ist, soweit technisch möglich, technisch sicherzustellen, dass kernbereichsrelevante Informationen nicht erhoben werden.

(2) Wird für das Bundesamt für Verfassungsschutz erkennbar, dass durch den Einsatz eines nachrichtendienstlichen Mittels kernbereichsrelevante Informationen erlangt werden, so hat es den Einsatz zu unterbrechen. Wird das nachrichtendienstliche Mittel in einer Weise eingesetzt, dass bei einer Unterbrechung eine Gefährdung von Leib, Leben oder Freiheit einer Person oder der weiteren Einsetzbarkeit des nachrichtendienstlichen Mittels droht, so hat eine Unterbrechung erst dann zu erfolgen, sobald dies ohne Gefährdung möglich ist. Ist für das Bundesamt für Verfassungsschutz zu erwarten, dass bei einer Fortführung des Einsatzes nicht nur am Rande kernbereichsrelevante Informationen erhoben werden, so hat er diesen Einsatz abzubrechen. Die Unterbrechung und die Fortsetzung zur Abwendung einer Gefährdung sind unter Angabe der Gründe zu dokumentieren.

(3) Abweichend von Absatz 2 dürfen beim Einsatz technischer Mittel automatische Aufzeichnungen ohne unmittelbare Kenntnisnahme fortgesetzt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass lediglich vorübergehend kernbereichsrelevante Informationen erlangt werden.

(4) Zur Prüfung auf kernbereichsrelevante Informationen sind unverzüglich vorzulegen

1. Aufzeichnungen nach Absatz 3,

2. Aufzeichnungen aus Maßnahmen nach § 27,

3. sonstige durch den Einsatz eines nachrichtendienstlichen Mittels erlangte Informationen, soweit Zweifel bestehen, ob es sich um kernbereichsrelevante Informationen handelt, insbesondere, wenn Daten in einem unmittelbaren Zusammenhang mit solchen Daten stehen, die als kernbereichsrelevant identifiziert wurden.

Die Vorlagepflicht entfällt, wenn die Daten unverzüglich gelöscht werden.

(5) Die Vorlage nach Absatz 4 erfolgt an den

1. Unabhängigen Kontrollrat, wenn die Informationen durch Maßnahmen nach den §§ 25 bis 27 erlangt worden sind,

2. Aufsichtsbediensteten im Übrigen.

Aufsichtsbediensteter ist ein von der Amtsleitung mit der Entscheidung nach Satz 1 besonders beauftragter Bediensteter, der die Befähigung zum Richteramt hat und auf den in dieser Funktion § 6 Absatz 3 des Bundesdatenschutzgesetzes anzuwenden ist; für den Fall dass keine Beauftragung durch die Amtsleitung erfolgt ist, ist Aufsichtsbediensteter der behördliche Datenschutzbeauftragte.

(6) Die nach Absatz 4 vorzulegenden Informationen dürfen erst mit Zustimmung der Stelle, der sie nach Absatz 5 vorzulegen sind, genutzt werden. Informationen, die dem Unabhängigen Kontrollrat vorzulegen sind, kann der Aufsichtsbedienstete bis zur Entscheidung des Unabhängigen Kontrollrats vorläufig zur Weiterverarbeitung freigeben, wenn Gefahr im Verzug besteht.

(7) Hat das Bundesamt für Verfassungsschutz kernbereichsrelevante Informationen gewonnen, so dürfen diese Daten nicht genutzt werden; sie sind unverzüglich zu löschen.

Die Tatsache ihrer Erhebung und Löschung ist zu protokollieren. Die Protokolldaten sind zu löschen

1. im Falle einer Mitteilung an die betroffene Person 6 Monate nach Mitteilung, wenn die betroffene Person kein Interesse an weiterer Speicherung für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Beschränkungsmaßnahme geltend gemacht hat, frühestens jedoch zum Zeitpunkt nach Nummer 3,

2. im Falle des endgültigen Absehens von einer Mitteilung nach § 35 Absatz 4 unverzüglich,

3. im Übrigen am Ende des zweiten Kalenderjahres, das dem Kalenderjahr der Protokollierung folgt.

§ 32

Schutz von zeugnisverweigerungsberichtigten Berufsgeheimnisträgern

(1) Eine Maßnahme gegen einen Rechtsanwalt, Kammerrechtsbeistand oder Berufsgeheimnisträger, der in § 53 Absatz 1 Satz 1 Nummer 1, 2, oder 4 der Strafprozessordnung genannt ist, ist unzulässig, wenn sie voraussichtlich Informationen erbringen würde, über die diese Person das Zeugnis verweigern dürfte.

(2) Bei einer Maßnahme gegen einen in § 53 Absatz 1 Satz 1 Nummer 3 bis 3b oder 5 der Strafprozessordnung genannten Berufsgeheimnisträger, im Falle von § 53 Absatz 1 Satz 1 Nummer 3 der Strafprozessordnung mit Ausnahme von Rechtsanwälten und Kammerrechtsbeiständen, bei der voraussichtlich Erkenntnisse erlangt würden, über die diese Person das Zeugnis verweigern dürfte, sind das öffentliche Interesse an den von dieser Person wahrgenommenen Aufgaben und das Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Die Maßnahme ist nur zulässig, wenn sie

1. zur Aufklärung wenigstens erheblich beobachtungsbedürftiger Bedrohungen erfolgt und

2. keinen Nachteil herbeiführt, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht.

Für Rechtsanwälte oder Kammerrechtsbeistände gilt Absatz 1.

(3) Die Absätze 1 und 2 sind entsprechend anzuwenden auf die in § 53a der Strafprozessordnung genannten Personen.

(4) Die Absätze 1 bis 3 sind nicht anzuwenden, wenn die Maßnahme wegen tatsächlicher Anhaltspunkte dafür, dass die Person an den aufzuklärenden Bedrohungen beteiligt ist, durchgeführt wird.

(5) Hat das Bundesamt für Verfassungsschutz von einer in den Absätzen 1 bis 3 genannten Person Informationen gewonnen, die von ihr nach den Absätzen 1 bis 4 nicht gezielt erhoben werden dürfen, ist § 31 Absatz 7 darauf anzuwenden.

Unterabschnitt 3

Verfahren bei besonderen Maßnahmen

§ 33

Anordnung von Maßnahmen

(1) Maßnahmen sind anzuordnen von

1. der Abteilungsleitung oder einem von ihr besonders beauftragten Bediensteten, der sie entweder allgemein vertritt oder die Befähigung zum Richteramt hat, wenn die Maßnahme nur bei wenigstens erheblich beobachtungsbedürftigen Bedrohungen zulässig ist,

2. der Amtsleitung oder der von ihr dazu beauftragten Abteilungsleitung bei

   a) Maßnahmen, die nur bei besonders erheblich beobachtungsbedürftigen Bedrohungen zulässig sind,

   b) der Einsichtnahme in informationstechnische Geräte und Weiterverarbeitung gewonnener Informationen in den Fällen des § 23 Absatz 2 und 3,

   c) Volleingriffen in informationstechnische Systeme (§ 25),

   d) heimlichem Betreten von Wohnungen (§ 16 Absatz 6 Satz 2), technischen Datenerhebungen aus Wohnungen (§§ 27, 28 Absatz 2), zweckändernder Weiterverarbeitung von zur Eigensicherung aus Wohnungen erhobenen Daten (§ 28 Absatz 2 Satz 2 Nummer 2 und 3),

   e) besonderen Maßnahmen nach § 16 Absatz 4 Satz 2 und § 29.

Sind zur Durchführung von Maßnahmen nach den §§ 23 bis 26 vorbereitende technische Maßnahmen erforderlich, die in die Integrität eines informationstechnischen Systems eingreifen, sind diese ohne Erhebung personenbezogener Daten bereits vor Anordnung zulässig, wenn ansonsten der Erfolg der Maßnahme gefährdet wäre.

(2) Die Anordnung muss enthalten

1. den Aufklärungsgegenstand, im Fall einer gegen eine Person gerichteten Maßnahme die Person, soweit möglich mit Namen und Anschrift,

2. Art, Umfang, Dauer des Einsatzes und Befristung der Anordnung,

3. beim Eingriff in das Brief-, Post- und Telekommunikationsgeheimnis durch Maßnahmen nach den §§ 13, 14 und 22 im Fall

   a) des § 22 Absatz 3 Nummer 3 Buchstabe c die Rufnummer oder eine andere Kennung eines zu überwachenden Anschlusses,

   b) der Überwachung des Brief- oder Postverkehrs eine Bezeichnung der Sendungen, die der Anordnung unterliegen sollen,

4. beim Eingriff in Informationstechnik (§§ 23 bis 26) eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,

5. bei der technischen Datenerhebung aus Wohnungen (§§ 27, 28 Absatz 2) die zu überwachende Wohnung oder die zu überwachenden Wohnräume.

Der Aufklärungsgegenstand kann auch durch räumlich und zeitlich eingegrenzte Ereignisse bezeichnet werden. Für den Einsatz von Internetermittlungen, Vertrauenspersonen und Verdeckten Bediensteten ist das Aufklärungsfeld anzugeben, dessen Erforschung der Einsatz dient. Ist die Maßnahme gegen eine verdeckt eingesetzte Person gerichtet, sind keine Angaben zu machen, die die Feststellung von deren Identität ermöglichen.

(3) Die Anordnung nach Absatz 2 kann auch zulassen, dass die Maßnahme

1. gegen weitere Personen durchgeführt werden darf, wenn die Maßnahme der Aufklärung eines bestimmten Sachverhaltes dient und nach nachrichtendienstlichen Erfahrungen mit weiteren Beteiligten an diesem Sachverhalt zu rechnen ist,

2. im Falle des Absatzes 2 Satz 1 Nummer 3 Buchstabe a auf weitere Anschlüsse der Person erstreckt werden kann, wenn nach nachrichtendienstlichen Erfahrungen damit zu rechnen ist, dass auch diese von Beteiligten oder Nachrichtenmittlern genutzt werden.

(4) Anordnungen sind zu befristen auf höchstens

1. 1 Jahr

   a) beim Einsatz zu Internetermittlungen auf vertiefter Vertrauensbasis (§ 17),

   b) beim Einsatz von Vertrauenspersonen (§ 18) oder Verdeckten Bediensteten (§ 19)

   c) bei Übermittlungspflichten von Unternehmen (§§ 11 bis 14),

   d) bei der Überwachung von Brief-, Post und Telekommunikationsverkehren (§ 22),

   e) beim Auslesen informationstechnischer Geräte (§ 23) oder technischer Spuren von informationstechnischen Angriffen (§ 24) und begrenzten Eingriffen in die Integrität privater informationstechnischer Systeme (§ 26),

2. 6 Monate bei

   a) sonstigen Maßnahmen, die nur bei wenigstens erheblich beobachtungsbedürftigen Bedrohungen zulässig sind,

   b) Eingriffen in die Integrität privater informationstechnischer Systeme nach § 25,

3. 3 Monate bei sonstigen Maßnahmen, die nur bei besonders erheblich beobachtungsbedürftigen Bedrohungen zulässig sind, sowie besonderen Maßnahmen nach § 16 Absatz 4 Satz 2 und § 29,

4. 1 Monat bei technischen Datenerhebungen aus Wohnungen (§§ 27, 28 Absatz 2) und bei der zweckändernden Weiterverarbeitung von zur Eigensicherung erhobenen Daten (§ 28 Absatz 2 Satz 2).

Verlängerungen um jeweils höchstens denselben Zeitraum sind zulässig, wenn die Voraussetzungen der Anordnung fortbestehen. Liegen die Voraussetzungen für die Anordnung nicht mehr vor oder ist der Zweck der Anordnung erreicht oder ergibt sich, dass er nicht erreicht werden kann, so ist die Maßnahme auch vor Ablauf der Frist einzustellen und die Anordnung aufzuheben.

(5) Die Anordnung ist mit Sachverhalt und Begründung, einschließlich Rechtsgrundlage, aktenkundig zu machen. Ihre Durchführung ist zu dokumentieren.

§ 34

Unabhängige Vorabkontrolle

(1) Anordnungen dürfen erst mit Feststellung ihrer Rechtmäßigkeit durch den Unabhängigen Kontrollrat vollzogen werden bei

1. [heimlichem Betreten von Wohnungen (§ 16 Absatz 6 Satz 2),]

2. verdeckten Ermittlungen zur Informationserhebung im Internet unter Ausnutzung eines persönlichen Vertrauensverhältnisses, wenn nach einer Kontaktnahme in physischer Präsenz oder nach dreimaliger wirtschaftlicher Zuwendung zugunsten einer Person (§ 17) die Maßnahme, die sich gegen diese Person richtet, länger als 6 Monate fortgesetzt wird,

3. Vertrauenspersonen und Verdeckten Bediensteten, wenn

   a) die Einsatzzeit 6 Monate überschreitet oder

   b) sie gezielt gegen eine Personen nach § 16 Absatz 5 Satz 1 Nummer 2 eingesetzt werden oder

   c) sie gegen eine Person eingesetzt werden, zu der sie eine besondere persönliche Vertrauensbeziehung unterhalten (§ 18 Absatz 3 Satz 2, auch in Verbindung mit § 19),

4. besonders erheblich eingreifender optischer und akustischer Überwachung (§ 20 Absatz 2) und entsprechendem Ersuchen an Verfügungsberechtigte von Einrichtungen zur Videoüberwachung (§ 15 Absatz 2 Satz 2),

5. besonders erheblich eingreifenden technischen Mitteln der Bewegungsüberwachung (§ 21 Absatz 1 Nummer 2),

6. Eingriffen in Brief-, Post und Telekommunikationsgeheimnis

   a) durch qualifizierte Auskünfte nach den §§ 13 und 14 in Verbindung mit § 11 Absatz 5 sowie

   b) durch Überwachung nach § 22, im Falle des Telekommunikationsgeheimnisses bei der Überwachung von interpersoneller Kommunikation und den Fällen, die nach § 22 Absatz 2 Satz 2 nur unter den Voraussetzungen des § 23 Absatz 2 und 3 oder der §§ 25, 26 Absatz 2 Satz 1 zulässig sind,

7. Auslesen informationstechnischer Geräte und Weiterverarbeitung gewonnener Informationen in den Fällen des § 23 Absatz 2 und 3,

8. Erhebung einer Kopie der technischen Spuren von IT-Angriffen (§ 12 Absatz 2, § 24 Absatz 1 Satz 2),

9. Eingriffen in private informationstechnische Systeme in den Fällen des § 25 und des § 26 Absatz 2 Satz 1,

10. besonderen Maßnahmen nach § 16 Absatz 4 Satz 2 und § 29,

11. Maßnahmen unter Eingriff in nach § 32 Absatz 2 geschützte Berufsgeheimnisse.

§ 33 Absatz 1 Satz 2 gilt entsprechend.

(2) Werden Maßnahmen gemäß § 33 Absatz 3 nachträglich auf weitere Personen oder Anschlüsse erstreckt, sind diese Erweiterungen dem unabhängigen Kontrollrat zur Entscheidung über die Rechtmäßigkeit vorzulegen. Die Vorlage muss spätestens mit Ablauf der Anordnung erfolgen. Stellt der Unabhängige Kontrollrat die Rechtswidrigkeit einer Erweiterung fest, ist § 31 Absatz 3 Satz 4 bis 6 des UKRat-Gesetzes anzuwenden.

(3) Würde anderenfalls der Zweck der Maßnahme vereitelt oder wesentlich erschwert, kann die Amtsleitung oder eine von ihr dazu beauftragte Abteilungsleitung vor Feststellung der Rechtmäßigkeit nach Absatz 1 die vorläufige Vollziehbarkeit nach Maßgabe von § 31 des UKRat-Gesetzes anordnen. Vor Feststellung der Rechtmäßigkeit nach Absatz 1 dürfen Informationen aus Maßnahmen nach den §§ 25, 27 nur zur Abwehr einer gegenwärtigen Gefahr und zur Strafverfolgung nur bei Flucht- oder Verdunkelungsgefahr übermittelt werden.

(4) Eine Anordnung, die eine Wohnungsüberwachung (§ 27) betrifft, darf erst vollzogen werden, wenn das Bundesverwaltungsgericht deren Rechtmäßigkeit festgestellt hat. Daten, die zur Einsatzsicherung aus Wohnungen erhoben wurden (§ 28 Absatz 2), dürfen für andere Zwecke (§ 28 Absatz 2 Satz 2 Nummer 2 und 3) erst weiterverarbeitet werden, wenn das Bundesverwaltungsgericht die Rechtmäßigkeit der Eigensicherungsanordnung festgestellt hat. Absatz 3 ist entsprechend anzuwenden.

(5) Beteiligte des Feststellungsverfahrens nach Absatz 4 ist das Bundesamt für Verfassungsschutz. Es legt dem Bundesverwaltungsgericht die Anordnung vor. Stehen besondere Gründe des Geheimschutzes der Vorlage an das Bundesverwaltungsgericht entgegen, wird die Vorlage dadurch bewirkt, dass die Anordnung dem Bundesverwaltungsgericht in vom Bundesamt für Verfassungsschutz bestimmten Räumlichkeiten zur Verfügung gestellt wird. Das Bundesverwaltungsgericht kann den Sachverhalt durch Anhörung des Bundesamtes für Verfassungsschutz erforschen. Im Einverständnis des Bundesamtes für Verfassungsschutz kann der Vorsitzende oder Berichterstatter anstelle des Senats entscheiden. Gegen eine nach Satz 5 getroffene Entscheidung steht dem Bundesamt für Verfassungsschutz innerhalb von 2 Wochen nach Bekanntgabe die Beschwerde zu, auf die der Senat entscheidet. Das Verfahren des Bundesverwaltungsgerichts unterliegt den Vorschriften des materiellen Geheimschutzes. Die Mitglieder des Bundesverwaltungsgerichts sind zur Geheimhaltung verpflichtet. Für das nichtrichterliche Personal gelten die Regelungen des personellen Geheimschutzes.

§ 35

Mitteilung an betroffene Personen

(1) Das Bundesamt für Verfassungsschutz hat Personen, gegen die es eine in § 34 Absatz 1 Satz 1 Nummer 1 und 4 bis 11 und Absatz 4 aufgeführte Maßnahme durchgeführt hat, nach deren Einstellung mitzuteilen, dass es diese Maßnahme eingesetzt hat. Bei Maßnahmen nach § 34 Absatz 1 Nummer 10 und 11 erfolgt die Mitteilung nur, wenn technische Mittel eingesetzt worden sind. Hat das Bundesamt für Verfassungsschutz personenbezogene Daten übermittelt, erfolgt die Mitteilung im Benehmen mit dem Empfänger.

(2) Eine Mitteilung nach Absatz 1 erfolgt nicht, wenn

1. die Identität der Person oder eine zustellfähige Anschrift unbekannt ist und die Anschrift auch nicht durch Abruf aus einem Register ermittelbar ist,

2. bei Maßnahmen zur Aufklärung von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten nicht nachträglich ausgeschlossen werden kann, dass eine solche Tätigkeit für eine fremde Macht vorlag,

3. bei der Vorbereitung oder Durchführung der Maßnahme eine von einer Sicherheitsbehörde verdeckt eingesetzte Person tätig war und nicht ausgeschlossen werden kann, dass die Mitteilung zum Bekanntwerden ihrer Zusammenarbeit mit einer Sicherheitsbehörde führen kann; dies ist in der Regel auszuschließen bei verdeckt zur Observation eingesetzten Bediensteten,

4. der Mitteilung überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen oder

5. eine Mitteilung nach Absatz 3 zurückzustellen ist und die Gründe mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft vorliegen werden.

(3) Die Mitteilung nach Absatz 1 wird zurückgestellt, solange

1. eine Gefährdung des Zwecks der Maßnahme nicht ausgeschlossen werden kann oder

2. der Eintritt überwiegender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist.

(4) Von einer Mitteilung nach Absatz 1 wird endgültig abgesehen, wenn

1. eine der Voraussetzungen nach Absatz 3 vorliegt und die Daten nach § 38 Absatz 1 zu löschen sind,

2. die Mitteilung bereits 5 Jahre nach Absatz 3 zurückgestellt ist und auf absehbare Zeit die Gründe der Zurückstellung erwartbar fortbestehen.

(5) Der Zustimmung des Unabhängigen Kontrollrates bedürfen die

1. Nicht-Mitteilungen nach Absatz 2 Nummer 3 bis 5 sowie das endgültige Absehen von einer Mitteilung nach Absatz 4,

2. weitere Zurückstellung nach Absatz 3, wenn 12 Monate nach Einstellung der Maßnahme vergangen sind, wobei der Unabhängige Kontrollrat die Dauer der weiteren Zurückstellung zu bestimmen hat.

(6) Die Gründe einer Entscheidung nach den Absätzen 2 bis 4 sind aktenkundig zu machen.

Unterabschnitt 4

Weiterverarbeitung von Daten

§ 36

Weiterverarbeitung

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten weiterverarbeiten, wenn dies zur Erfüllung seiner Aufgaben erforderlich ist. Eine Weiterverarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist im Übrigen nur zulässig, wenn

1. dies im Einzelfall erforderlich ist zur

   a) Erfüllung seiner Aufgaben nach § 2 oder

   b) Durchführung von arbeits- und disziplinarrechtlichen Maßnahmen oder von Maßnahmen nach dem Sicherheitsüberprüfungsgesetz gegen seine gegenwärtigen oder ehemaligen Bediensteten wegen einer strafbaren Handlung oder wegen sicherheitserheblichen Erkenntnissen,

2. § 25 Absatz 5, § 27 Absatz 4 und § 28 Absatz 2, auch in Verbindung mit § 34 Absatz 3 Satz 2, nicht entgegenstehen und

3. im Fall von Übermittlungen die Voraussetzungen nach dem 3. Abschnitt vorliegen.

Zweckbindungen nach den in Satz 2 Nummer 2 genannten Vorschriften sind durch technische oder organisatorische Maßnahmen zu sichern. Sind mit personenbezogenen Daten, die weiterverarbeitet werden dürfen, weitere Daten der betroffenen Person oder eines Dritten so verbunden, dass eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, ist die Speicherung auch dieser Daten zulässig. Die weiteren Daten nach Satz 4 dürfen nicht genutzt werden.

(2) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten in einem Dateisystem nur speichern, wenn

1. tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffene Person

   a) an einer Bedrohung beteiligt ist,

   b) in einem Zusammenhang mit einer an einer Bedrohung beteiligten Person steht, der Grund zu der Annahme gibt, dass durch die Auswertung Erkenntnisse für die Aufklärung der Bedrohung gewonnen werden können,

   c) durch Bedrohungen gefährdet ist,

   d) zur Erforschung von Bedrohungen beitragen kann,

2. Informationen vorliegen, die darauf zu prüfen sind, ob sie als tatsächliche Anhaltspunkte nach Nummer 1 zu bewerten sind,

3. die Speicherung nicht strukturiert zur Person erfolgt und erforderlich ist zur

   a) Eigensicherung oder

   b) Erforschung von Bedrohungen,

4. dies im Einzelfall für Aufgaben nach § 2 Absatz 5 erforderlich ist oder

5. dies zur Entwicklung und Anwendung von Datenverarbeitungsprogrammen erforderlich ist.

Personenbezogene Daten, die nach Satz 1 Nummer 2 zur Prüfung gespeichert sind, dürfen nur zu dieser Prüfung weiterverarbeitet werden. Personenbezogene Daten, die zum Zweck des Satz 1 Nummer 5 gespeichert sind, dürfen nur zu diesem Zweck und zur Sicherung einer ordnungsgemäßen Datenverarbeitung weiterverarbeitet werden.

(3) Absatz 2 gilt nicht für pseudonymisierte Daten. Zu gespeicherten pseudonymisierten Daten darf ein Personenbezug nur unter den Voraussetzungen des Absatzes 2 Satz 1 Nummer 1 hergestellt werden.

§ 37

Qualifizierte Auswertung

(1) Das Bundesamt für Verfassungsschutz darf mittels einer qualifizierten Auswertung Erkenntnisse nur abrufen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall zur Aufklärung von Bedrohungen erforderlich ist. Eine qualifizierte Auswertung ist eine Verarbeitung von in Dateiensystemen des Bundesamtes für Verfassungsschutz gespeicherten personenbezogenen Daten mittels einer automatisierten Anwendung, die durch Verknüpfung neue Erkenntnisse über die Persönlichkeit einer Person oder ihre Beziehungen zu anderen Personen oder zu Objekten gewinnt.

(2) Eine qualifizierte Auswertung darf abgerufen werden

1. nur bei Erforderlichkeit zur Aufklärung wenigstens erheblich beobachtungsbedürftiger Bedrohungen, wenn sie erfolgt

   a) zur Gewinnung von tatsächlichen Anhaltspunkten für eine Beteiligung von Personen, zu denen individuell kein Anlass zu solcher Prüfung bestand,

   b) zur Erstellung von Verhaltens- und Persönlichkeitsprofilen für die umfassende Bewertung des individuellen Bedrohungspotenzials einer Person oder

   c) zu sonstigen personenbezogenen Vorhersagen oder zu personenbezogenen Empfehlungen oder Entscheidungen, wenn dazu ein maschinengestütztes System eingesetzt wird, das anpassungsfähig auf einen autonomen Betrieb angelegt ist,

2. nur bei Erforderlichkeit zur Aufklärung besonders erheblich beobachtungsbedürftiger Bedrohungen, wenn sie erfolgt zur Gewinnung höchstprivater Erkenntnisse,

3. nach Maßgabe des § 21, wenn sie zur Gewinnung eines Bewegungsprofils erfolgt, das einem Bewegungsprofil nach § 21 gleichwertig ist, dies unter Berücksichtigung

   a) des Zeitraums, über den das Bewegungsprofil zusammenhängend erstellt wird,

   b) der zeitlichen Abstände der Standortdaten und

   c) ihrer geodätischen Genauigkeit.

(3) Stellt der unabhängige Kontrollrat fest, dass eine vom Bundesamt für Verfassungsschutz eingesetzte qualifizierte Auswertung, die nicht in Absatz 2 aufgeführt ist, einer in Absatz 2 aufgeführten qualifizierten Auswertung nach den Folgen der Auswertung und der gewonnenen Persönlichkeitserkenntnis, insbesondere zu Verhalten, das nicht der Bedrohung dient, gleichkommt, gelten deren Voraussetzungen auch für die nicht aufgeführte qualifizierte Auswertung.

(4) Liegen die in den Absätzen 1 und 2 genannten Voraussetzungen vor, darf Eine qualifizierte Auswertung gezielt zu einer Person nur abgerufen werden,

1. entsprechend § 16 Absatz 5 oder

2. zur Gewinnung tatsächlicher Anhaltspunkte für die Beteiligung an einer Bedrohung.

(5) Ein Abruf ist mit Zeitpunkt, Eingabe und abrufender Stelle zu protokollieren. Ist eine Protokollierung nicht möglich, trifft das Bundesamt für Verfassungsschutz geeignete technische oder organisatorische Maßnahmen, um eine datenschutzrechtliche Kontrolle zu ermöglichen. Der Unabhängige Kontrollrat hat die Einhaltung der Vorschriften über den

Datenschutz bei der qualifizierten automatisierten Auswertung mindestens alle 2 Jahre zu kontrollieren.

(6) Eine qualifizierte Auswertung darf eine geheimdienstliche Intervention nur beschränkt auf Maßnahmen nach § 60 Absatz 2 Nummer 1 Buchstabe b oder d automatisiert veranlassen und nur, wenn solche Maßnahmen zur Abwehr eines informationstechnischen Angriffs erforderlich sind.

(7) Anwendungen, die anpassungsfähig auf einen autonomen Betrieb angelegt sind,

1. dürfen in einem Drittstaat nur beschafft werden, wenn keine gleich geeignete Anwendung des Bundesamtes für Verfassungsschutz selbst, einer anderen inländischen Stelle oder einer Stelle eines Mitgliedstaates der Europäischen Union verfügbar ist,

2. müssen ein angemessenes Niveau an Genauigkeit, Robustheit und Cybersicherheit erreichen,

3. dürfen keine diskriminierenden Algorithmen herausbilden oder verwenden,

4. sind auf ordnungsgemäßes Funktionieren durch das Bundesamt für Verfassungsschutz stichprobenartig zu überprüfen.

§ 38

Datenpflege in Dateisystemen

(1) Das Bundesamt für Verfassungsschutz muss personenbezogene Daten in Dateisystemen

1. berichtigen, wenn sie unrichtig sind,

2. löschen, wenn

   a) ihre Speicherung unzulässig ist oder

   b) ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist.

Die Löschung unterbleibt, wenn

1. die Daten mit weiteren Daten der betroffenen Person oder eines Dritten so verbunden sind, dass eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, oder

2. Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden.

Unterbleibt die Löschung nach Satz 2, dürfen die Daten nur noch im Interesse der betroffenen Person oder mit ihrer Einwilligung genutzt oder übermittelt werden.

(2) Das Bundesamt für Verfassungsschutz prüft bei der Einzelfallbearbeitung und zu strukturiert zur Person gespeicherten Daten nach festgesetzten Fristen, ob die Daten zu berichtigen oder zu löschen sind. Die Frist beträgt höchstens

1. 2 Jahre, wenn ausschließlich Daten vor Vollendung des 18. Lebensjahres vorliegen,

2. 5 Jahre im Übrigen.

(3) Das Bundesamt für Verfassungsschutz löscht personenbezogene Daten, die es im Falle des § 36 Absatz 2 Satz 1 Nummer 1 Buchstabe a strukturiert zur Person gespeichert hat,

1. spätestens nach 2 Jahren, wenn ausschließlich personenbezogene Daten vor Vollendung des 16. Lebensjahres vorliegen

2. spätestens nach 5 Jahren, wenn ausschließlich personenbezogene Daten vor Vollendung des 18. Lebensjahres vorliegen,

3. im Übrigen spätestens nach 15 Jahren, wenn die Daten zur Aufklärung von verfassungsfeindlichen Bestrebungen gespeichert sind.

Im Fall des § 36 Absatz 2 Satz 1 Nummer 2 löscht das Bundesamt für Verfassungsschutz die Daten spätestens nach 2 Jahren, wenn keine wenigstens erheblich beobachtungsbedürftigen Bedrohungen aufzuklären sind, im Übrigen spätestens nach 5 Jahren. Über Ausnahmen entscheidet im Fall des Satzes 1 Nummer 3 die Abteilungsleitung, im Übrigen die Amtsleitung. In den Fällen, in denen die Amtsleitung über die Ausnahme entscheidet, ist eine Ausnahme nur einmalig für weitere 2 Jahre und beschränkt auf besonders erheblich beobachtungsbedürftige Bedrohungen zulässig.

(4) Die Fristen nach den Absätzen 2 und 3 beginnen mit dem Zeitpunkt der letzten Information, die eine Speicherung begründet.

(5) Die Absätze 1 bis 4 gelten nicht für die Datenverarbeitung in Akten und Aktenauszügen.

§ 39

Akten

(1) Das Bundesamt für Verfassungsschutz darf Akten in elektronischer Form führen. Bei jeder Abfrage aus einer elektronischen Akte sind der Zeitpunkt, die Angaben, die die Feststellung der abgefragten Daten ermöglichen, sowie Angaben zur Feststellung der abfragenden Person zu protokollieren.

(2) Stellt das Bundesamt für Verfassungsschutz fest, dass personenbezogene Daten in Akten unrichtig sind, oder wird ihre Richtigkeit von der betroffenen Person bestritten, so ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.

(3) Das Bundesamt für Verfassungsschutz hat die Verarbeitung personenbezogener Daten einzuschränken, wenn es im Einzelfall feststellt, dass ohne die Einschränkung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden und die Daten für die künftige Aufgabenerfüllung des Bundesamtes für Verfassungsschutz nicht mehr erforderlich sind. Die Daten dürfen nicht mehr genutzt oder übermittelt werden. Eine Aufhebung der Einschränkung ist möglich, wenn die Voraussetzungen der Einschränkung nachträglich entfallen.

(4) Eine Akte ist zu vernichten, wenn sie insgesamt zur Erfüllung der Aufgaben des Bundesamtes für Verfassungsschutz nicht oder nicht mehr erforderlich ist. Wird die Akte zu einem Beteiligten einer Bedrohung geführt, so gilt für die Prüfung der Erforderlichkeit und für die Vernichtung jeweils der Akte als Ganzes § 38 Absatz 2 und 3 entsprechend. Eine Vernichtung unterbleibt, wenn

1. Grund zu der Annahme besteht, dass durch die Vernichtung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden, oder

2. die Akte nach den Vorschriften des Bundesarchivgesetzes dem Bundesarchiv zur Übernahme anzubieten und zu übergeben ist.

Im Falle des Satzes 3 Nummer 1 ist die Verarbeitung der in der Akte gespeicherten personenbezogenen Daten einzuschränken. Sie dürfen nur für die Interessen, zu deren Schutz die Vernichtung unterbleibt, verarbeitet werden oder wenn die Verarbeitung zur Abwehr einer konkretisierten Gefahr für besonders gewichtige Rechtsgüter unerlässlich ist.

§ 40

Protokolldaten

Nach diesem Gesetz zu speichernde Protokolldaten dürfen nur für Zwecke der Datenschutzkontrolle oder des Geheimschutzes, einschließlich folgender Anschlussmaßnahmen, sowie zur Datensicherung und zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage verwendet werden. Ihre Auswertbarkeit ist nach dem Stand der Technik zu gewährleisten. Sie sind am Ende des 15. Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen.

§ 41

Errichtungsanordnungen

(1) Das Bundesamt für Verfassungsschutz legt für strukturierte Speicherungen, die im nachrichtendienstlichen Informationssystem oder zum Zweck qualifizierten Auswertung nach § 37 erfolgen, und für Anwendungen, die solche Auswertung durchführen, fest:

1. den Zweck der Auswertbarkeit,

2. die Voraussetzungen der Auswertung,

3. die Anlieferung oder Eingabe,

4. die Zugangsberechtigung,

5. die Dauer, für die Daten in die spezielle Auswertbarkeit einbezogen werden,

6. die Überprüfungsfristen sowie

7. die Protokollierung.

Eine Einrichtungsanordnung kann auch für eine Reihe von Speicherungen und Anwendungen allgemein erfolgen.

(2) Der Unabhängige Kontrollrat ist vor Erlass einer Errichtungsanordnung anzuhören. Wenn die Datenverarbeitung ausschließlich der Kontrolle der oder des Bundesbeauftragten für den Datenschutz unterliegt, ist diese oder dieser anstelle des Unabhängigen Kontrollrats anzuhören. Die Einrichtungsanordnung bedarf der Zustimmung des Bundesministeriums des Innern. Ist wegen der Dringlichkeit der Aufgabenerfüllung die vorherige Mitwirkung der in den Sätzen 1 und 2 genannten Stellen nicht möglich, so kann die Amtsleitung des Bundesamtes für Verfassungsschutz eine Sofortanordnung treffen. Die Mitwirkungen nach den Sätzen 1 und 2 sind unverzüglich nachzuholen. Wird die Zustimmung des Bundesministeriums den Innern nach Satz 3 nicht erteilt ist die Sofortanordnung aufzuheben.

(3) Das Bundesamt für Verfassungsschutz führt ein Verzeichnis der geltenden Errichtungsanordnungen. In angemessenen Abständen ist die Notwendigkeit des speziellen Auswertungszwecks und von Änderungen der weiteren Festlegungen zu überprüfen.

Unterabschnitt 5

Gemeinsame automatisierte Auswertung

§ 42

Gemeinsame automatisierte Auswertung mit inländischen öffentlichen Stellen

(1) Das Bundesamt für Verfassungsschutz darf mit inländischen öffentlichen Stellen eine automatisierte Auswertbarkeit von personenbezogenen Daten, die die beteiligten Stellen in ihren Dateisystemen speichern, einrichten, wenn dies für Aufgaben erforderlich ist, die dem Schutz besonders gewichtiger Rechtsgüter vor Bedrohungen dienen und durch die beteiligten Stellen ohne operative Anschlussmaßnahmen zu Lasten der betroffenen Person wahrgenommen werden. In einer Vereinbarung der beteiligten Stellen sind festzulegen:

1. Struktur und Datenmodell der beteiligten Dateisysteme,

2. technische Anforderungen für eine gemeinsame Auswertbarkeit,

3. Zwecke und Voraussetzungen der Auswertung,

4. Verwendung der gewonnenen Informationen.

(2) Das Bundesamt für Verfassungsschutz darf für die Auswertung Daten entsprechend § 36 Absatz 3 bis 5 bereitstellen. Die weiteren beteiligten Stellen dürfen Daten bereitstellen, soweit sie sie zur eigenen Auswertung für die Aufgabe nutzen dürfen. Soweit besondere Übermittlungsverbote entgegenstehen, dürfen Daten für die Auswertung nicht bereitgestellt werden. Die Auswertung ist nur zulässig, soweit sie im Einzelfall für den Einrichtungszweck erforderlich ist. Erkenntnisse der Auswertung dürfen nach Maßgabe der Voraussetzungen der §§ 46 bis 48 für die entsprechenden operativen Anschlussmaßnahmen zu Lasten der betroffenen Person genutzt werden. Im Übrigen dürfen Erkenntnisse der Auswertung nicht für operative Anschlussmaßnahmen zu Lasten der betroffenen Person genutzt werden.

(3) Betreibt das Bundesamt für Verfassungsschutz ein technisches Verbundsystem, in dem die beteiligten Stellen ihre Dateisysteme zur gemeinsamen Auswertung nach Absatz 1 führen, trifft es technische und organisatorische Maßnahmen entsprechend § 64 Absatz 3 des Bundesdatenschutzgesetzes. Gemeinsame technische Anforderungen für die Verbundteilnahme sind in der Vereinbarung nach Absatz 1 Satz 2 aufzunehmen.

§ 43

Gemeinsame Dateisysteme mit ausländischen Nachrichtendiensten

(1) Das Bundesamt für Verfassungsschutz kann für die Zusammenarbeit mit ausländischen öffentlichen Stellen, die mit nachrichtendienstlichen Aufgaben betraut sind (ausländische Nachrichtendienste), ein gemeinsames Dateisystem einrichten, wenn

1. dies zur Aufklärung bestimmter erheblich beobachtungsbedürftige Bedrohungen erforderlich ist,

2. in den teilnehmenden Staaten die Einhaltung grundlegender rechtsstaatlicher Prinzipien gewährleistet ist,

3. die Festlegungen und Zusagen nach Absatz 3 Satz 1 verlässlich sind und

4. das Bundesministerium des Innern zugestimmt hat.

Die Bedrohung kann auch gegen den Bestand oder die Sicherheit eines anderen Staates oder einer internationalen Organisation gerichtet sein. Gespeichert werden dürfen nur die zur Erforschung und Bewertung der Bedrohung erforderlichen Daten, die nur zu diesem Zweck genutzt werden dürfen. An dem gemeinsamen Dateisystem können im Rahmen ihrer Aufgaben auch der Militärische Abschirmdienst und der Bundesnachrichtendienst teilnehmen.

(2) Der ausländische Nachrichtendienst eines Staates, der weder unmittelbar an die Bundesrepublik Deutschland angrenzt noch Mitgliedstaat der Europäischen Union oder des Nordatlantikvertrages ist, kann nur zur Aufklärung besonders erheblich beobachtungsbedürftiger Bedrohungen und vergleichbarer Sicherheitsinteressen der beteiligten Staaten am gemeinsamen Dateiensystem teilnehmen. Die Teilnahme eines solchen ausländischen Nachrichtendienstes bedarf der Zustimmung des Bundesministeriums des Innern.

(3) Die Ziele der Zusammenarbeit und das Nähere der Datenverarbeitung sind vor Beginn der Zusammenarbeit zwischen den teilnehmenden Nachrichtendiensten zur Gewährleistung eines angemessenen Datenschutzniveaus und zum Ausschluss unangemessener Verwendung schriftlich festzulegen, insbesondere:

1. der Zweck des gemeinsamen Dateisystems,

2. die Voraussetzungen der Verwendungen von Daten,

3. die Prüfung und erforderlichenfalls die unverzügliche Änderung, Berichtigung und Löschung von Daten,

4. die Zusage,

   a) die Daten ohne Zustimmung des eingebenden Nachrichtendienstes nicht für einen anderen Zweck als den nach Nummer 1 zu verwenden oder an Dritte zu übermitteln,

   b) Auskunft über die Verwendung derjenigen Daten zu geben, die vom Auskunft erbittenden Nachrichtendienst eingegeben worden sind.

§ 41 gilt mit der Maßgabe, dass die Festlegungen auf das Bundesamt für Verfassungsschutz beschränkt sind und der Anordnung die Festlegung nach Satz 1 als Anlage beizufügen ist.

(4) Anzuwenden sind durch

1. das Bundesamt für Verfassungsschutz

   a) zur Speicherung § 36 unter Beachtung von § 55,

   b) zur Datenpflege § 38,

2. den Militärischen Abschirmdienst

a) zur Speicherung § 47 des MAD-Gesetzes unter Beachtung von § 38 des MAD-Gesetzes,

b) zur Datenpflege § 48 des MAD-Gesetzes,

3. den Bundesnachrichtendienst § 93 Absatz 4 des BND-Gesetzes.

Daten, deren Weiterverarbeitung einer besonderen Zweckbindung unterliegt, dürfen nur gespeichert werden, wenn das gemeinsame Dateisystem einem solchen Zweck dient und die Verarbeitung durch die anderen Teilnehmer entsprechend eingeschränkt ist. Der Abruf von Daten ist nur zu dem für das gemeinsame Dateisystem festgelegten Zweck und zur Datenpflege zulässig. Für die Verantwortung des teilnehmenden Nachrichtendienstes gilt § 6 Absatz 2 Satz 4 und 5 entsprechend.

(5) Das Bundesamt für Verfassungsschutz trifft für das gemeinsame Dateisystem die technischen und organisatorischen Maßnahmen entsprechend § 64 Absatz 3 des Bundesdatenschutzgesetzes. § 6 Absatz 3 Satz 2 und § 69 gelten nur für die vom Bundesamt für Verfassungsschutz, vom Militärischen Abschirmdienst und vom Bundesnachrichtendienst eingegebenen Daten sowie den Abruf dieser Stellen. § 71 ist mit der Maßgabe anzuwenden, dass das Bundesamt für Verfassungsschutz Auskunft nur erteilt zu den

1. von ihm eingegebenen Daten und

2. vom Militärischen Abschirmdienst oder vom Bundesnachrichtendienst eingegebenen Daten mit dem Einvernehmen der Stelle, die die Daten eingegeben hat.

§ 44

Teilnahme an gemeinsamen Dateisystemen ausländischer Nachrichtendienste

Das Bundesamt für Verfassungsschutz darf an gemeinsamen Dateisystemen, die von ausländischen Nachrichtendiensten errichtet sind, teilnehmen. § 43 Absatz 1, 2 und 4 gilt entsprechend. Dabei gilt § 43 Absatz 1 Satz 1 Nummer 2 mit der Maßgabe, dass verlässlich zuzusagen ist, dass

1. die vom Bundesamt für Verfassungsschutz eingegebenen Daten ohne seine Zustimmung nicht an Dritte übermittelt werden dürfen und nur zu dem Zweck verwendet werden dürfen, zu dem sie in die Datei eingegeben wurden, und

2. das Bundesamt für Verfassungsschutz auf Ersuchen Auskunft über die Verwendung der Daten erhält.

Das Bundesamt für Verfassungsschutz erteilt über die von ihm eingegebenen Daten entsprechend § 71 Auskunft.

Abschnitt 3

Übermittlung

§ 45

Information von Öffentlichkeit und Fachkreisen

(1) Das Bundesamt für Verfassungsschutz kann die Öffentlichkeit und Fachkreise über Bedrohungen und ihre Einstufung sowie über präventiven Wirtschafts- und Wissenschaftsschutz informieren. Über Prüffälle wird nicht berichtet. Bei Informationen über Verdachtsfälle ist darauf hinzuweisen, dass lediglich ein Verdacht vorliegt.

(2) Das Bundesministerium des Innern informiert die Öffentlichkeit über Bedrohungen nach § 3 Absatz 4 Nummer 1 bis 3 mindestens einmal jährlich in einem zusammenfassenden Bericht insbesondere zu aktuellen Entwicklungen nach Maßgabe des Absatzes 1 Satz 2 und 3. In dem Bericht sind die Zuschüsse des Bundeshaushaltes an das Bundesamt für Verfassungsschutz und die Gesamtzahl seiner Bediensteten anzugeben.

(3) Personenbezogene Daten dürfen öffentlich bekanntgegeben werden, wenn die Bekanntgabe für das Verständnis des Zusammenhanges oder der Darstellung von Organisationen oder unorganisierten Gruppierungen erforderlich ist. Ihre Bekanntgabe an Fachkreise ist zulässig, wenn dies zum Zweck der Information der Fachkreise erforderlich ist. Die Bekanntgabe ist unzulässig, wenn schutzwürdige Interessen der betroffenen Person überwiegen.

(4) Hat das Bundesamt für Verfassungsschutz wissenschaftlichen Einrichtungen zur Erforschung von Bedrohungen übermittelt, so gilt Absatz 3 entsprechend für die Veröffentlichung übermittelter Daten durch die wissenschaftliche Einrichtung. Die Veröffentlichung bedarf der Zustimmung des Bundesamtes für Verfassungsschutz.

§ 46

Übermittlung an inländische öffentliche Stellen zur Gefahrenabwehr

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an eine inländische öffentliche Stelle übermitteln, soweit dies im Einzelfall auf Grund tatsächlicher Anhaltspunkte zur Abwehr einer zumindest konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut erforderlich ist.

(2) Im Falle einer konkreten Gefahr für ein besonders gewichtiges Rechtsgut, die von einer Bedrohung nach § 3 Absatz 4 ausgeht, oder einer unmittelbar bevorstehenden Gefahr für ein besonders gewichtiges Rechtsgut ist das Bundesamt für Verfassungsschutz zur Übermittlung verpflichtet.

§ 47

Übermittlung an inländische öffentliche Stellen zum administrativen Rechtsgüterschutz

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an eine inländische öffentliche Stelle übermitteln, soweit dies auf Grund tatsächlicher Anhaltspunkte

im Einzelfall zum Schutz besonders gewichtiger Rechtsgüter vor Bedrohungen erforderlich ist

1. bei Strafvollstreckung oder Vollzug freiheitsentziehender Maßnahmen, einschließlich der Vollzugsplanung,

2. für ein Verfahren nach Artikel 18 Satz 2 oder Artikel 21 Absatz 4 des Grundgesetzes,

3. für Aufgaben nach

   a) dem Staatsangehörigkeitsrecht,

   b) dem Vereinsgesetz oder

   c) den Versammlungsgesetzen,

4. im öffentlichen Dienst und bei Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen,

   a) zur Überprüfung der Verfassungstreue von Bewerbern und Beschäftigten sowie von Reservisten der Bundeswehr,

   b) zur Durchführung von arbeits- und disziplinarrechtlichen Maßnahmen gegen gegenwärtige oder ehemaligen Beschäftigte wegen strafbarer Handlungen,

5. für Aufgaben nach dem Aufenthaltsrecht oder zur Untersagung der Ausreise,

6. zur Durchsetzung von im Bereich der Gemeinsamen Außen- und Sicherheitspolitik der Europäischen Union beschlossenen wirtschaftlichen Sanktionsmaßnahmen,

7. für Aufgaben des Außenwirtschaftsrechts,

8. für Aufgaben der Gewerbeaufsicht,

9. für Aufgaben der Finanzdienstleistungsaufsicht,

10. für gesetzliche Aufgaben des Objekt- oder Personenschutzes oder zu einer gesetzlich vorgesehenen Eignungs- oder Zuverlässigkeitsüberprüfung, insbesondere nach dem Waffenrecht, dem Jagdrecht, dem Sprengstoffrecht, dem Atomrecht, dem Luftsicherheitsrecht oder den Sicherheitsüberprüfungsgesetzen,

11. zur Verhinderung der Beschaffung von Mitteln, die geeignet und dazu bestimmt sind, die Ausführung von wenigstens erheblich beobachtungsbedürftigen Bedrohungen erheblich zu fördern,

12. zum Vollzug der Steuergesetze bei tatsächlichen Anhaltspunkten dafür, dass erhebliche nicht gerechtfertigte Steuervorteile zur Förderung der Ausführung wenigstens erheblich beobachtungsbedürftigen Bedrohungen verwendet werden.

(2) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an eine inländische öffentliche Stelle zur Vorbereitung, Durchführung oder Überprüfung einer begünstigenden Maßnahme übermitteln, wenn dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zum Schutz besonders gewichtiger Rechtsgüter erforderlich ist.

(3) In den Fällen des Absatzes 1 Nummer 4 Buchstabe a und 6 oder auf ein Ersuchen einer zuständigen Stelle im Rahmen eines gesetzlich besonders geregelten Anfrageverfahrens ist das Bundesamt für Verfassungsschutz zu der Übermittlung verpflichtet.

§ 48

Übermittlung an Strafverfolgungsbehörden zur Strafverfolgung

(1) Das Bundesamt für Verfassungsschutz übermittelt personenbezogene Daten an eine inländische Strafverfolgungsbehörde, wenn bestimmte Tatsachen den Verdacht einer besonders schweren Straftat begründen und soweit die Daten zur Verfolgung dieser Straftat erforderlich sind.

(2) Besonders schwere Straftaten sind Straftaten,

1. die im Höchstmaß mit Freiheitsstrafe von mehr als 5 Jahren bedroht sind und

2. die aus der Anlage 1 ersichtlichen Straftaten.

§ 49

Übermittlung an inländische öffentliche Stellen ohne Möglichkeit operativer Anschlussmaßnahmen

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an eine inländische öffentliche Stelle übermitteln, wenn dies auf Grund tatsächlicher Anhaltspunkte zur eigenen Aufklärung einer Bedrohung, insbesondere zur Vorbereitung oder Konkretisierung eines Auskunftsersuchens, erforderlich ist.

(2) Das Bundesamt für Verfassungsschutz übermittelt dem Bundesnachrichtendienst personenbezogene Daten, soweit sich aus ihnen Erkenntnisse über einen Vorgang im Ausland von außen- und sicherheitspolitischer Bedeutung ergeben.

(3) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an inländische öffentliche Stellen übermitteln, wenn dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zum Schutz besonders gewichtiger Rechtsgüter vor Bedrohungen für Aufgaben erforderlich ist, die die empfangende Stelle ohne operative Anschlussmaßnahmen zu Lasten der betroffenen Person wahrnimmt. Dies gilt insbesondere für die

1. Erforschung und Bewertung der Bedrohungen nach Satz 1,

2. Verbesserung der Fachkompetenz und Organisation bei der Erforschung der Bedrohungen nach Satz 1.

(4) Liegen die Voraussetzungen nach den §§ 46 und 48 nicht vor, so darf der Empfänger die übermittelten Daten nicht für operative Anschlussmaßnahmen zu Lasten der betroffenen Person nutzen.

§ 50

Übermittlung an inländische öffentliche Stellen von Daten aus Gefahrenaufklärung

Das Bundesamt für Verfassungsschutz darf personenbezogene Daten, die es zur Aufklärung konkretisierter Gefahren für besonders gewichtige Rechtsgüter gewonnen hat, an eine inländische öffentliche Stelle abweichend von den §§ 46 bis 49 auch übermitteln, wenn dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist zum Schutz besonders gewichtiger Rechtsgüter oder zur Verfolgung von Straftaten von erheblicher Bedeutung.]

§ 51

Übermittlung an inländische nichtöffentliche Stellen

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an nichtöffentliche inländische Stellen übermitteln, soweit dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist

1. zur eigenen Aufklärung von Bedrohungen, insbesondere zur Vorbereitung oder Konkretisierung eines Auskunftsersuchens,

2. zur Abwendung einer zumindest konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut,

3. zum Schutz vor Bedrohungen für folgende Zwecke:

   a) Schutz lebenswichtiger und verteidigungsrelevanter Einrichtungen und kritischer Infrastrukturen,

   b) Schutz der Sicherheit in der Informationstechnik,

   c) Schutz von Wirtschaftsunternehmen und Wissenschaftseinrichtungen vor sicherheitsgefährdenden und geheimdienstlichen Tätigkeiten,

   d) Schutz rechtlich gewährleisteter Geheimnisse,

   e) wissenschaftliche Erforschung und Bewertung von Bedrohungen,

   f) Präventions-, Ausstiegs- oder Deradikalisierungsprojekte, die finanziell oder organisatorisch mit öffentlichen Stellen kooperieren,

   g) Schutz des Kindeswohls bei der Erbringung von Leistungen und Erfüllung der Aufgaben der Kinder- und Jugendhilfe,

   h) Schutz der gesetzlichen Erziehungs- und Bildungsziele der Schulen und der Einrichtungen der Kindertagesbetreuung,

   i) Schutz der zweckgemäßen Verwendung öffentlicher Fördermittel oder sonstiger öffentlicher Vorteilszuwendungen,

4. zur Information eines Betreibers folgender Einrichtungen oder Dienste über deren gegenwärtige oder geplante Nutzung für Bedrohungen:

   a) soziale Netzwerke (§ 1 Absatz 1 des Netzwerkdurchsetzungsgesetzes)

   b) Veranstaltungsstätten,

   c) finanzbezogene Dienstleistungen der nach § 2 des Geldwäschegesetzes Verpflichteten,

   d) Schießsporteinrichtungen,

5. zur Information folgender Stellen über eine gegenwärtige oder angestrebte Beschäftigung oder Mitgliedschaft eines Beteiligten einer Bedrohung:

   a) Einrichtungen mit Freizeit-, Bildungs-, Betreuungs- und Förderungs-Angeboten für Kinder, Jugendliche oder Heranwachsende,

b) Reservistenverbände,

c) Parteien,

d) politische, gemeinnützige oder mildtätige Vereine.

Eine Übermittlung personenbezogener Daten nach Satz 1 Nummer 2 bis 5 ist unzulässig, wenn ihr Zweck in gleicher Weise auch durch Übermittlung an eine zuständige öffentliche Stelle zu erreichen ist.

(2) Eine nichtöffentliche Stelle, die personenbezogene Daten nach Absatz 1 Satz 1 Nummer 3 erhalten hat, darf die Daten für Handlungen, die für die betroffene Person eine nachteilige rechtliche Wirkung entfalten oder diese Person in anderer Weise erheblich beeinträchtigen, nur verwenden, wenn dies im Einzelfall zum Schutz eines besonders gewichtigen Rechtsguts erforderlich ist und das Bundesamt für Verfassungsschutz zustimmt. Bei einer unmittelbar bevorstehenden Gefahr ist die vorherige Zustimmung des Bundesamts für Verfassungsschutz entbehrlich. Die nichtöffentliche Stelle hat das Bundesamt für Verfassungsschutz unverzüglich über ihre Handlungen und deren Anlass zu unterrichten.

§ 52

Übermittlungsverbote

(1) Personenbezogene Daten dürfen nicht nach den §§ 46 bis 51 übermittelt werden, wenn

1. erkennbar ist, dass unter Berücksichtigung der Art der Informationen und ihrer Erhebung die schutzwürdigen Interessen der betroffenen Person das Interesse des Empfängers an der Übermittlung überwiegen,

2. überwiegende Sicherheitsinteressen, insbesondere Gründe des Schutzes verdeckt eingesetzter Personen oder des Schutzes operativer Maßnahmen, entgegenstehen oder

3. besondere gesetzliche Regelungen entgegenstehen, wobei die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, unberührt bleibt.

(2) Sofern eine Übermittlung, zu der das Bundesamt für Verfassungsschutz nach § 46 Absatz 2, § 47 Absatz 3 oder § 48 verpflichtet ist, gemäß Absatz 1 unterbleibt, sind die Gründe aktenkundig zu machen.

§ 53

Minderjährigenschutz bei Inlandsübermittlung

Das Bundesamt für Verfassungsschutz darf personenbezogene Daten über Minderjährige nur übermitteln, wenn

1. eine Weiterverarbeitung ausgeschlossen ist

   a) für eine die betroffene Person belastende operative Anschlussmaßnahme und

   b) für Handlungen, die für die betroffene Person eine nachteilige rechtliche Wirkung entfalten oder sie in anderer Weise erheblich beeinträchtigen,

2. die Übermittlung nach den §§ 46 bis 48 erfolgt und die betroffene Person mindestens 14 Jahre alt ist oder

3. die Übermittlung nach § 46 Absatz 1 erfolgt, beschränkt auf den Schutz von

   a) Leib oder Leben einer Person oder

   b) Einrichtungen der Bundesrepublik Deutschland, der Europäischen Union oder einer internationalen Organisation, der die Bundesrepublik Deutschland angehört oder für Mitgliedstaaten der Europäischen Union oder des Nordatlantikvertrages.

§ 54

Weiterverarbeitung durch Empfänger

(1) Der Empfänger prüft, ob die nach den §§ 46 bis 51 übermittelten personenbezogenen Daten für die Erfüllung seiner Aufgaben erforderlich sind. Ergibt die Prüfung, dass die Daten nicht erforderlich sind, hat er sie zu löschen. Die Löschung kann unterbleiben, wenn die Trennung von anderen Informationen, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unvertretbarem Aufwand möglich ist. Der Empfänger darf die Daten, die für die Erfüllung ihrer Aufgaben nicht erforderlich sind, jedoch nicht nutzen.

(2) Der Empfänger darf die übermittelten Daten, soweit gesetzlich nichts anderes bestimmt ist, nur verarbeiten

1. zu dem Zweck, zu dem sie ihm übermittelt wurden, oder

2. zu einem anderen Zweck, wenn sie ihm auch zu diesem Zweck übermittelt werden dürften unter der Voraussetzung, dass das Bundesamt für Verfassungsschutz der Verarbeitung zu dem abgeänderten Zweck für den Einzelfall oder eine Reihe gleichgelagerter Fälle zustimmt.

(3) Das Bundesamt für den Verfassungsschutz hat den Empfänger auf den Zweck der Übermittlung und die Zweckbindung nach Satz 1 hinzuweisen. Dies gilt nicht für Übermittlungen im Rahmen verdeckter Ermittlungen. Der Empfänger ist verpflichtet, dem Bundesamt für Verfassungsschutz auf dessen Verlangen Auskunft über die weitere Verarbeitung zu geben.

(4) Hat die Übermittlung personenbezogener Daten in einem Verfahren zur vorbeugenden Personenüberprüfung nachteilige Folgen für die betroffene Person, so schließt das Auskunftsrecht der betroffenen Person auch das Recht auf Auskunft ein, dass die Folge durch eine Übermittlung des Bundesamtes für Verfassungsschutz veranlasst ist.

§ 55

Übermittlung an ausländische sowie über- und zwischenstaatliche Stellen

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an ausländische öffentliche Stellen oder an über- oder zwischenstaatliche Stellen zur Weiterverarbeitung ohne operativer Anschlussmaßnahmen zu Lasten der betroffenen Person übermitteln, wenn dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zum Schutz besonders gewichtiger Rechtsgüter oder zum Schutz der Sicherheit eines anderen Staates oder einer über- und zwischenstaatlichen Einrichtung erforderlich ist. Eine Übermittlung zum Schutz eines anderen Staates oder zur Aufklärung von Staatsschutzdelikten, die gegen einen anderen Staat begangen worden sind, ist unbeschadet des Absatzes 2 nur zulässig, wenn

dort die grundlegenden demokratischen und rechtsstaatlichen Prinzipien sowie die elementaren Menschenrechte gewährleistet sind.

(2) Die Übermittlung unterbleibt, wenn folgende Belange entgegenstehen:

1. besondere gesetzliche Regelungen zur Verarbeitung personenbezogener Daten,

2. wesentliche auswärtige Belange der Bundesrepublik Deutschland oder

3. überwiegende schutzwürdige Interessen einer Person.

Überwiegende schutzwürdige Interessen stehen insbesondere entgegen, wenn Leib, Leben oder Freiheit einer Person oder sonstige elementare Menschenrechte gefährdet würden oder Verletzungen von elementaren rechtsstaatlichen Grundsätzen drohen. Bei der Prüfung, ob eine Übermittlung zu unterbleiben hat, berücksichtigt das Bundesamt für Verfassungsschutz insbesondere den bisherigen Umgang des Empfängers mit übermittelten Daten und die Gewährleistung eines zum Schutz der Menschenrechte angemessenen Datenschutzes. Ein die elementaren Menschenrechte wahrender Umgang mit den übermittelten Daten ist insbesondere dann nicht gewährleistet, wenn zu besorgen ist, dass die Daten zu politischer Verfolgung oder zu unmenschlicher oder erniedrigender Bestrafung oder Behandlung verwendet werden. Verbleiben auf Grund der Einschätzung Zweifel an der Vereinbarkeit der Übermittlung mit den Anforderungen nach Satz 1 Nummer 3, so dürfen die Daten nur auf der Grundlage einer belastbaren verbindlichen Zusicherung des Empfängers und nur mit Zustimmung des Bundesministeriums des Innern übermittelt werden.

(3) Die übermittelten personenbezogenen Daten dürfen weiterverarbeitet werden

1. nur zu dem Zweck, zu dem sie ihm übermittelt wurden, und

2. unbeschadet des Absatzes 4 nicht für operative Anschlussmaßnahmen zu Lasten der betroffenen Person.

Das Bundesamt für Verfassungsschutz hat den Empfänger hierauf hinzuweisen. Es hat ihn ferner darauf hinzuweisen, dass es sich vorbehält, um Auskunft über die vorgenommene Verwendung der Daten zu bitten.

(4) Das Bundesamt für Verfassungsschutz darf einer Verwendung der personenbezogenen Daten für operativer Anschlussmaßnahmen zu Lasten der betroffenen Person zustimmen

1. zur Abwehr einer zumindest konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut oder ein Rechtsgut von entsprechendem Gewicht,

2. zum administrativen Rechtsgüterschutz für Aufgaben, die den in § 47 Absatz 1 benannten entsprechen,

3. aufgrund eines durch bestimmte Tatsachen begründeten Verdachts zur Verfolgung einer besonders schweren Straftat, deren Gewicht den Straftaten nach § 48 Absatz 2 entspricht.

(5) Personenbezogene Daten einer minderjährigen Person darf das Bundesamt für Verfassungsschutz übermitteln

1. an Staaten, die unmittelbar an die Bundesrepublik Deutschland angrenzen, oder Mitgliedstaaten oder Organe der Europäischen Union oder des Nordatlantikvertrages nach § 53,

2. im Übrigen

a) zur Abwehr einer konkretisierten Gefahr nach § 46 Absatz 1, jedoch wenn die Person noch nicht 16 Jahre alt ist, beschränkt auf eine konkretisierte Gefahr für Leib oder Leben einer Person oder für Einrichtungen der Europäischen Union oder des Nordatlantikvertrages oder für Einrichtungen von deren Mitgliedstaaten,

b) bei dringendem Tatverdacht zur Strafverfolgung nach § 48,

(6) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an eine nichtöffentliche Stelle im Ausland übermitteln, wenn dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zur Abwehr einer dringenden Gefahr für ein Rechtsgut nach § 3 Absatz 8 Nummer 4 unerlässlich ist und überwiegende schutzwürdige Interessen der betroffenen Person nicht entgegenstehen.

(7) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten auch an inländische Stellen übermitteln, wenn dies zur Vorbereitung einer Übermittlung nach den Absätzen 1 bis 6 erforderlich ist. § 54 Absatz 2 ist anzuwenden.

§ 56

Ohne Ausübung besonderer Befugnisse gewonnene personenbezogene Daten

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten, die es aus allgemein zugänglichen Quellen erhoben hat, übermitteln, wenn dies zur Erfüllung seiner Aufgaben oder von Aufgaben der empfangenden Stelle erforderlich ist.

(2) Personenbezogene Daten, die es nach § 8 Absatz 1 Satz 2 aus allgemein zugänglichen Quellen gewonnenen hat, darf das Bundesamt für Verfassungsschutz übermitteln, wenn dies im Einzelfall für Zwecke der öffentlichen Sicherheit erforderlich ist.

(3) Im Übrigen darf das Bundesamt für Verfassungsschutz personenbezogene Daten, die es ohne Anwendung besonderer Befugnisse und nicht von ausländischen Nachrichtendiensten erlangt hat, an inländische öffentliche Stellen übermitteln, soweit dies im Einzelfall zum Schutz besonders gewichtiger Rechtsgüter erforderlich ist.

(4) Die in den Absätzen 2 und 3 bezeichneten personenbezogenen Daten darf das Bundesamt für Verfassungsschutz auch zur Strafverfolgung übermitteln, soweit dies im Einzelfall auf Grund tatsächlicher Anhaltspunkte erforderlich ist.

§ 57

Übermittlung zum Schutz der betroffenen Person

Das Bundesamt für Verfassungsschutz darf personenbezogene Daten auch übermitteln, wenn offensichtlich ist, dass die Übermittlung im Interesse der betroffenen Person liegt. Es darf personenbezogene Daten insbesondere für Zwecke der Jugendhilfe übermitteln.

§ 58

Weitere Verfahrensregelungen

(1) Das Bundesamt für Verfassungsschutz protokolliert den Empfänger, die Rechtsgrundlage sowie den Zeitpunkt der Übermittlung. Die Protokolldaten müssen danach auswertbar sein, ob die Übermittlung nach den §§ 46, 47, 48, 49, 50 oder 51 erfolgt ist.

(2) Sind mit personenbezogenen Daten, die übermittelt werden dürfen, weitere Daten der betroffenen Person oder eines Dritten so verbunden, dass eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen der betroffenen Person oder eines Dritten an der Geheimhaltung offensichtlich überwiegen. Der Empfänger darf diese Daten nicht nutzen.

(3) Zur Übermittlung an inländische öffentliche Stellen kann das Bundesamt für Verfassungsschutz in geeigneten Fällen automatisierte Abrufverfahren einrichten.

(4) Eine Übermittlung an nichtöffentliche Stellen bedarf der Zustimmung der Amtsleitung des Bundesamtes für Verfassungsschutz. Für Übermittlungen an inländische nichtöffentliche Stellen kann die Zustimmung auch allgemein für gleichgelagerte Fälle erfolgen. Die Übermittlung ist dem Betroffenen durch das Bundesamt für Verfassungsschutz mitzuteilen, sobald eine Gefährdung seiner Aufgabenerfüllung durch die Mitteilung nicht mehr zu besorgen ist. Die Mitteilungspflicht entfällt, wenn eine Gefährdung der Aufgabenerfüllung auch 5 Jahre nach der Übermittlung fortbesteht.

§ 59

Nachberichtspflicht

Erweisen sich personenbezogene Daten nach ihrer Übermittlung nach den Vorschriften dieses Gesetzes als unvollständig oder unrichtig, so sind sie unverzüglich gegenüber dem Empfänger zu berichtigen, es sei denn, dass dies für die Beurteilung eines Sachverhalts ohne Bedeutung ist.

A b s c h n i t t 4

S c h u t z m a ß n a h m e n

§ 60

Schutzmaßnahmen

(1) Das Bundesamt für Verfassungsschutz kann Schutzmaßnahmen vornehmen, wenn es bei seiner Aufklärung feststellt, dass eine umgehende Einwirkung erforderlich ist, um eine von einer besonderen Bedrohung ausgehende Gefährdung für ein besonders gewichtiges Rechtsgut abzuwenden. Die Vornahme einer Schutzmaßnahme ist darüber hinaus nur zulässig, wenn

1. durch Einwirkung einer anderen Stelle der Zweck der Maßnahme nicht erreicht werden kann oder

2. eine Übermittlung der zur Abwehr erforderlichen Informationen nach § 52 nicht möglich ist.

Schutzmaßnahmen sind zu dokumentieren.

(2) Schutzmaßnahmen sind das verdeckte Einwirken auf

1. Gegenstände, die für die Bedrohung gegenwärtig oder absehbar eingesetzt werden, insbesondere durch

a) Beeinträchtigung der Funktion von Tatmitteln,

b) Umleitung oder Unterbindung von Datenverkehren oder der Übertragung von Informationen, einschließlich technischer Signale und Programmdateien, sowie die Veränderung der Übertragungsinhalte,

c) Bereitstellung falscher Informationen für Beteiligte,

d) Löschung oder Verfälschung von Informationen, die für Zwecke der Bedrohung gespeichert sind,

2. Güter, die im Rahmen einer Bedrohung ausgeführt werden sollen,

a) wenn die Ausfuhr entgegen einer Ausfuhrbeschränkung erfolgt, oder

b) um eine im Einzelfall bestehende Gefahr für die in § 4 Absatz 1, auch in Verbindung mit Absatz 2 des Außenwirtschaftsgesetzes genannten Rechtsgüter abzuwenden.

Die Einwirkung darf nicht durch unmittelbaren Zwang gegen Personen erfolgen.

(3) Besondere Bedrohungen liegen vor

1. bei Bestrebungen, die darauf gerichtet sind, zur Zielverfolgung in § 129a Absatz 1 oder 2 des Strafgesetzbuches genannte Straftaten zu begehen, soweit sie derartige Straftaten planen und zudem zu erwarten ist, dass im Falle ihrer Begehung erhebliche Unruhe in großen Teilen der Bevölkerung ausgelöst wird,

2. bei sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten für eine fremde Macht, die diese systematisch im Geltungsbereich dieses Gesetzes durchführt, wenn dadurch besonders schwere Schäden drohen.

(4) Eine Einwirkung darf keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht.

§ 61

Anordnung von Schutzmaßnahmen

(1) Die Anordnung von Schutzmaßnahmen erfolgt auf Grund einer Bedrohungseinstufung (Absatz 2) und in einem festgelegten Maßnahmerahmen (Absatz 3).

(2) Die Einstufung von Bedrohungen als besondere Bedrohungen erfolgt durch die Amtsleitung und ist auf höchstens 1 Jahr zu befristen. Die Einstufung wird erst mit Feststellung ihrer Rechtmäßigkeit durch den unabhängigen Kontrollrat wirksam.

(3) Zu jeder nach Absatz 2 eingestuften Bedrohung sind durch die Amtsleitung oder die von ihr dazu beauftragte Abteilungsleitung die Arten von Schutzmaßnahmen zu bestimmen, die im Rahmen des § 60 Absatz 2 eingesetzt werden dürfen.

(4) Die Anordnung von Schutzmaßnahmen erfolgt

1. durch die Amtsleitung oder die von ihr dazu beauftragte Abteilungsleitung, wenn die Einwirkung erfolgt unter

a) Eingriff in ein privates Informationstechnisches System und nicht bereits eine Anordnung nach den §§ 25 oder 26 besteht,

b) heimlichem Betreten einer Wohnung und nicht bereits eine Anordnung nach den §§ 27 oder 28 Absatz 2 besteht,

2. im Übrigen durch die Abteilungsleitung oder einen von ihr besonders beauftragten Bediensteten, der sie entweder allgemein vertritt oder die Befähigung zum Richteramt hat.

Eine Anordnung nach Satz 1 Nummer 1 darf erst mit Feststellung ihrer Rechtmäßigkeit durch den unabhängigen Kontrollrat vollzogen werden. Sind zur Durchführung der Einwirkung vorbereitende technische Maßnahmen erforderlich, die in die Integrität eines informationstechnischen Systems eingreifen, sind diese ohne weitere Einwirkung bereits vor Anordnung zulässig.

(5) Würde in den Fällen der unabhängigen Vorabkontrolle nach Absatz 2 Satz 2 und Absatz 4 Satz 2 andernfalls der Zweck der Maßnahme vereitelt oder wesentlich erschwert, kann die Amtsleitung die Einstufung oder Anordnung für sofort vollziehbar erklären. § 31 Absatz 2 bis 4 des UKRat-Gesetzes gilt entsprechend.

§ 62

Unterstützung von Schutzmaßnahmen

Auf Ersuchen des Bundesamtes für Verfassungsschutz dürfen Dritte bei der Durchführung von Einwirkungen nach Absatz 1 Hilfe leisten. § 9 Absatz 3 gilt entsprechend. Zur Hilfe verpflichtet sind

1. öffentliche Stellen,

2. Anbieter öffentlich zugänglicher Telekommunikationsdienste und Betreiber einer Telekommunikationsanlage, mit der solche Dienste erbracht werden,

3. geschäftsmäßige Anbieter von digitalen Diensten.

Die Verpflichtung gilt nicht, wenn ein Ausnahmegrund entsprechend § 5 Absatz 3 des Verwaltungsverfahrensgesetzes vorliegt. Für eine Hilfeleistung nichtöffentlicher Stellen hat das Bundesamt für Verfassungsschutz eine angemessene Entschädigung zu leisten, deren Höhe sich an den nachgewiesenen tatsächlichen Kosten orientiert.

§ 63

Besondere Kontrolle der Durchführung von Schutzmaßnahmen

(1) Das Bundesministerium des Innern erstattet dem Parlamentarischen Kontrollgremium jährlich einen Bericht über Schutzmaßnahmen, der einen Überblick über Gesamtzahl der Maßnahmen, ihre Art und Veranlassung sowie wesentliche Ergebnisse gibt.

(2) Der Unabhängige Kontrollrat kontrolliert die Einhaltung der Vorschriften des § 60 jährlich und berichtet dem Parlamentarischen Kontrollgremium über die Ergebnisse seiner Kontrolle in seinem Tätigkeitsbericht.

Abschnitt 5

Weitere Regelungen zur Eigensicherung

§ 64

Schutz des Eigensicherungsbereichs

(1) Das Bundesamt für Verfassungsschutz hat in seinen Dienststellen, auf seinen Grundstücken und in seinen sonstigen Einrichtungen (Eigensicherungsbereich) zum Schutz vor funktionsgefährdenden Tätigkeiten spezielle Befugnisse nach Maßgabe der folgenden Absätze aus. Die Ausübung des Hausrechts bleibt hiervon unberührt.

(2) Das Bundesamt für Verfassungsschutz darf Personen, die seinen Eigensicherungsbereich betreten oder sich dort aufhalten, und von diesen Personen mitgeführte Taschen und sonstige Gegenstände sowie von diesen Personen genutzte Fahrzeuge

1. verdachtsunabhängig kontrollieren (Absatz 3 Satz1),

2. durchsuchen (Absatz 3 Satz 2), wenn tatsächliche Anhaltspunkte für funktionsgefährdende Tätigkeiten vorliegen.

Es darf die Identität von Personen, die sich im Eigensicherungsbereich aufhalten, feststellen und dazu insbesondere eine Person anhalten, sie nach ihren Personalien befragen und verlangen, dass sie mitgeführte Ausweispapiere zur Prüfung aushändigt.

(3) Eine Kontrolle nach Absatz 2 Satz 1 Nummer 1 ist die oberflächliche Suche nach Gegenständen an Personen, an oder in Taschen oder an oder in mitgeführten Gegenständen und Fahrzeugen auch unter Einsatz technischer Mittel, ohne dass ein Körperkontakt mit der betroffenen Person stattfindet. Eine Durchsuchung nach Absatz 2 Satz 1 Nummer 2 ist die zielgerichtete und planmäßige Suche, auch unter Einsatz technischer Mittel,

1. am äußeren Körper der betroffenen Person,

2. in Kleidung und Taschen der betroffenen Person,

3. an und in Fahrzeugen der betroffenen Person einschließlich der dort mitgeführten Gegenstände sowie

4. in sonstigen mitgeführten Gegenständen der betroffenen Person, die geeignet sind, amtliche Informationen unbefugt aus dem Eigensicherungsbereich zu verbringen oder Gegenstände zu funktionsgefährdenden Tätigkeiten in den Eigensicherungsbereich einzubringen.

(4) Das Bundesamt für Verfassungsschutz darf innerhalb des Eigensicherungsbereichs auch unter Einsatz technischer Mittel verdachtsunabhängig Räume einschließlich der darin vorhandenen Gegenstände kontrollieren und durchsuchen. Zur dauerhaften offenen Überwachung des Eigensicherungsbereichs, darf es optisch-elektronische Einrichtungen nach Maßgabe einer Dienstvorschrift einsetzen. Eine Videoüberwachung höchstpersönlich genutzter Räume ist unzulässig. In der Dienstvorschrift sind die Voraussetzungen, das Verfahren und Grenzen der offenen Überwachung zu regeln.

(5) Gegenstände, die sich im Eigensicherungsbereich befinden, darf das Bundesamt für Verfassungsschutz sicherstellen und untersuchen, wenn

1. tatsächliche Anhaltspunkte dafür vorliegen, dass Gegenstände für eine funktionsgefährdende Tätigkeit verwendet werden oder mit solchen Tätigkeiten gewonnen worden sind,

2. Gegenstände vorschriftswidrig in den Eigensicherungsbereich eingebracht worden sind oder

3. Gegenstände keiner bestimmten Person zuzuordnen sind und die Sicherstellung und Untersuchung zum Schutz vor einer funktionsgefährdenden Tätigkeit erforderlich ist.

Bei Geräten der Informations- und Kommunikationstechnik umfasst das Untersuchen auch das Eingreifen mit technischen Mitteln sowie das Verarbeiten der auf dem Gerät gespeicherten Informationen einschließlich personenbezogener Daten.

(6) Das Bundesamt für Verfassungsschutz darf Maßnahmen auch noch in unmittelbarer Nähe des Eigensicherungsbereichs vornehmen im Fall

1. der Absätze 2 und 5 Satz 1 Nummer 1 und 2, wenn die Person sich einer Maßnahme im Eigensicherungsbereich entzieht,

2. des Absatzes 5 Satz 1 Nummer 3, wenn ein solcher Gegenstand in unmittelbarer Nähe des Eigensicherungsbereichs aufgefunden wird.

(7) Das Bundesamt für Verfassungsschutz darf unmittelbaren Zwang anwenden

1. zur Unterbindung eines gegenwärtigen oder unmittelbar bevorstehenden oder Beendigung eines erfolgten unbefugten Zutritts zum Eigensicherungsbereich,

2. im Eigensicherungsbereich zur Abwehr einer gegenwärtigen Gefahr für das Leben oder die körperliche Unversehrtheit von Personen oder für Einrichtungen oder Sachen von bedeutendem Wert, die den Aufgaben des Bundesamtes für Verfassungsschutz gewidmet sind,

3. zur Durchsetzung von Maßnahmen nach den Absätzen 2, 5 und 6.

Unmittelbarer Zwang darf nur durch besondere Vollzugskräfte (§ 28 Absatz 1 Satz 3 Nummer 2) angewendet werden und nur entsprechend den §§ 4, 5, 8 und 10 Absatz 1 Nummer 1 und 2 sowie den §§ 12 bis 14 des Gesetzes über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes. Im Fall des Satzes 1 Nummer 3 dürfen, keine Waffen eingesetzt werden. Eine Fesselung der betroffenen Person ist nur dann zulässig, wenn Tatsachen die Annahme rechtfertigen, dass sie die mit der Durchsetzung der Maßnahme beauftragten Personen oder Dritte angreifen, Widerstand leisten oder sich der Kontrolle entziehen wird.

(8) Bei der Durchführung von Maßnahmen nach Absatz 2 sowie den Absätzen 4 bis 7 hat das Bundesamt für Verfassungsschutz unter mehreren möglichen und geeigneten Maßnahmen diejenigen zu treffen, die die betroffene Person am wenigsten beeinträchtigen. Eine Maßnahme darf nicht zu einem Nachteil führen, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht.

§ 65

Verfahren im Eigensicherungsbereich

(1) Maßnahmen nach § 64 Absatz 2 Satz 1 Nummer 2 und Absatz 5 bedürfen der Anordnung der für die Eigensicherung zuständigen Abteilungsleitung oder einer von ihr

bestimmten Vertretung. Maßnahmen nach § 64 Absatz 4 Satz 2 bedürfen der Anordnung der Amtsleitung oder einer von ihr bestimmten Vertretung.

(2) Ist eine Anordnung nach Absatz 1 Satz 1 auf Grund besonderer Eilbedürftigkeit nicht rechtzeitig zu erlangen, kann die Maßnahme auch ohne vorherige Anordnung durchgeführt werden, wenn ansonsten der Zweck der Maßnahme vereitelt oder wesentlich erschwert würde. Bei Geräten der Informations- und Kommunikationstechnik darf in diesem Fall lediglich das Gerät sichergestellt werden. Die Anordnung ist unverzüglich nachzuholen. Wird die Anordnung nach Absatz 1 Satz 1 nicht nachgeholt, so hat das Bundesamt für Verfassungsschutz unverzüglich bereits erhobene Daten zu löschen und sichergestellte Gegenstände an die betroffene Person herauszugeben.

(3) Sichergestellte Gegenstände sind unverzüglich an die betroffene Person herauszugeben, sobald der Zweck der Eigensicherung entfällt. Satz 1 gilt nicht, wenn die Gegenstände zur Einleitung oder Durchführung eines strafrechtlichen Ermittlungsverfahrens an die Strafverfolgungsbehörden weitergegeben werden müssen.

(4) Bei Maßnahmen nach § 64 Absatz 2 Satz 1 Nummer 2 hat die betroffene Person das Recht, anwesend zu sein. Über eine Durchsuchung nach § 64 Absatz 2 Satz 1 Nummer 2 oder eine Sicherstellung nach § 64 Absatz 5 Satz 1 ist auf Verlangen eine Bescheinigung über die Maßnahme und den Grund der Maßnahme zu erteilen. Maßnahmen nach § 64 Absatz 5, die in Abwesenheit der betroffenen Person durchgeführt worden sind, sind ihr schriftlich mitzuteilen, wenn hierdurch nicht der Zweck der Maßnahme gefährdet wird.

(5) Bei der Untersuchung von Geräten der Informations- und Kommunikationstechnik, die nicht ausschließlich zur dienstlichen Nutzung überlassen wurden, ist sicherzustellen, dass an dem Gerät nur Veränderungen vorgenommen werden, die für die Datenverarbeitung unerlässlich sind. Vorgenommene Veränderungen sind bei Beendigung der Maßnahme, soweit technisch möglich, rückgängig zu machen. Sichergestellte Telekommunikationsendgeräte sind abweichend von Absatz 3 Satz 1 unabhängig von dem Abschluss der Maßnahmen nach § 64 Absatz 5 an die betroffene Person spätestens nach 2 Wochen herauszugeben. Macht die betroffene Person in den Fällen des Satzes 3 Gründe glaubhaft, nach denen für sie eine Aufrechterhaltung der Sicherstellung nicht zumutbar ist, so ist das mobile Endgerät innerhalb von 48 Stunden nach Darlegung der Gründe an die betroffene Person zurückzugeben. Das Bundesamt für Verfassungsschutz darf vor der Rückgabe ein Abbild der auf dem Gerät gespeicherten Informationen einschließlich personenbezogener Daten zur Datensicherung erzeugen. Wirkt die betroffene Person nicht an der Erzeugung eines unverschlüsselten Abbildes mit, kann die Herausgabe des Gerätes solange zurückgehalten werden, bis ein unverschlüsseltes Abbild erzeugt ist.

(6) Widerspruch und Anfechtungsklage gegen Maßnahmen nach § 64 haben keine aufschiebende Wirkung.

§ 66

Schutz vor unbemannten Fluggeräten

(1) Das Bundesamt für Verfassungsschutz darf unbemannte Fluggeräte im Umfeld seiner eingesetzten Bediensteten oder verdeckten Hilfspersonen sowie seines Eigensicherungsbereichs

1. aufklären und

2. bei Annäherung auf 100 Meter an seine eingesetzten Bediensteten oder verdeckten Hilfspersonen oder bei Eindringen in das geografische Gebiet seiner Liegenschaften nach § 21h Absatz 3 Nummer 4 der Luftverkehrs-Ordnung abwehren und dazu

insbesondere geeignete technische Mittel gegen das unbemannte Fluggerät, dessen Steuerungseinheit oder Steuerungsverbindung einsetzen.

(2) Das Bundesamt für Verfassungsschutz darf ein nach Absatz 1 abgewehrtes Fluggerät sicherstellen und untersuchen. Zur Durchsetzung einer Sicherstellung darf es unmittelbaren Zwang durch unmittelbare körperliche Einwirkung auf Personen oder Sachen anwenden, jedoch nicht Hilfsmittel der körperlichen Gewalt oder Waffen einsetzen. Körperliche Gewalt nach Satz 2 darf nur durch besondere Vollzugskräfte (§ 28 Absatz 1 Satz 3 Nummer 2) angewendet werden und nur entsprechend der §§ 4 und 5 des Gesetzes über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes.

§ 67

Ergänzende Regelungen zur Verarbeitung personenbezogener Daten

(1) Das Bundesamt für Verfassungsschutz darf zur Eigensicherung Dritte um Übermittlung von Informationen einschließlich personenbezogener Daten auch ersuchen, wenn dies erforderlich ist, weil

1. Personen oder Gegenstände in den Eigensicherungsbereich gelangen sollen oder unbefugt gelangt sind oder

2. eine Maßnahme nach diesem Abschnitt durchgeführt worden und weitere Aufklärung erforderlich ist.

(2) Bei der Untersuchung sichergestellter Gegenstände ist zum Schutz des Kernbereichs privater Lebensgestaltung § 31 Absatz 1, 4 Satz 1 Nummer 3 und Absatz 7 anzuwenden.

(3) Auf eine strukturierte Speicherung zu Prüfpersonen in einem Dateisystem sind § 36 Absatz 2 Satz 1 Nummer 2, auch in Verbindung mit § 36 Absatz 2 Satz 2 und § 38 Absatz 3 Satz 2 anzuwenden. Prüfpersonen sind Personen, zu denen im Einzelfall noch keine tatsächlichen Anhaltspunkte für funktionsgefährdende Tätigkeiten bestehen, wenn sie

1. Zugang zum Eigensicherungsbereich erhalten haben oder erhalten sollen oder

2. in einem aufklärungsbedürftigen Zusammenhang stehen zu

   a) Gegenständen, die nach § 64 Absatz 5 Nummer 2 oder 3 sichergestellt worden sind, oder

   b) einem Flug eines unbemannten Fluggerätes nach § 66 Absatz 1.

§ 68

Mitbestimmung bei Maßnahmen der Eigensicherung

Die Regelungen zur Mitbestimmung in § 80 Absatz 1 Nummer 18 und 21 des Personalvertretungsgesetzes sind nicht anzuwenden auf Regelungen oder technische Einrichtungen zu Eigensicherung des Bundesamtes für Verfassungsschutz.

Abschnitt 6

Allgemeiner Datenschutz und Rechtskontrolle

§ 69

Anwendung des Bundesdatenschutzgesetzes

Bei der Erfüllung der Aufgaben nach § 2 durch das Bundesamt für Verfassungsschutz findet das Bundesdatenschutzgesetz wie folgt Anwendung:

1. § 1 Absatz 8, die §§ 4, 16 Absatz 1 und 4 und die §§ 17 bis 21 sowie § 85 finden keine Anwendung,

2. die §§ 46, 52 bis 54, 62, 64, 83, 84 sind entsprechend anzuwenden, sowie § 51 Absatz 1 bis 4 mit der Maßgabe, dass die Verarbeitung personenbezogener Daten durch das Bundesamt auf der Grundlage einer Einwilligung erfolgen kann.

§ 70

Unabhängige Rechts- und Datenschutzkontrolle

(1) Jede Person, die der Ansicht ist, bei der Verarbeitung ihrer personenbezogenen Daten oder bei Schutzmaßnahmen durch das Bundesamt für Verfassungsschutz in ihren Rechten verletzt worden zu sein, kann sich an die nach Absatz 2 zuständige Aufsichtsstelle wenden.

(2) [Zuständig für die Rechts- und Datenschutzkontrolle ist

1. der Unabhängige Kontrollrat für

   a) die Verarbeitung personenbezogener Daten bei der Durchführung der Aufgaben nach § 2 Absatz 1 bis 4, einschließlich der technischen und operativen Fachunterstützung,

   b) Schutzmaßnahmen,

2. die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit im Übrigen, insbesondere für die Verarbeitung personenbezogener Daten bei der allgemeinen Verwaltung, der Aus- und Fortbildung und der Mitwirkung nach § 2 Absatz 5.

(3) Das Nähere der Rechts- und Datenschutzkontrolle regelt

1. zum Unabhängigen Kontrollrat das Gesetz über den Unabhängigen Kontrollrat,

2. zu der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit § 16 Absatz 2 des Bundesdatenschutzgesetzes; das Bundesamt für Verfassungsschutz ist zur Unterstützung entsprechend § 36a Absatz 3 des Sicherheitsüberprüfungsgesetzes verpflichtet.

§ 71

Auskunft an betroffene Personen

(1) Das Bundesamt für Verfassungsschutz erteilt der betroffenen Person über zu ihrer Person gespeicherte Daten auf Antrag unentgeltlich Auskunft, soweit sie hierzu auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an einer Auskunft darlegt. Die Auskunft erstreckt sich nur auf Daten,

1. die strukturiert zur betroffenen Person gespeichert sind oder

2. für deren Auskunftserteilung der erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Auskunftsinteresse steht.

(2) Die Auskunftserteilung unterbleibt, soweit

1. eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung zu besorgen ist,

2. durch die Auskunftserteilung verdeckt eingesetzte Personen gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise des Bundesamtes für Verfassungsschutz zu befürchten ist,

3. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder

4. die Daten oder die Tatsache der Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.

Die Entscheidung trifft die Amtsleitung oder ein von ihr besonders beauftragter Bediensteter.

(3) Die Auskunftsverpflichtung erstreckt sich nicht auf die Herkunft der Daten und die Empfänger von Übermittlungen.

(4) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung, soweit dadurch der Zweck der Auskunftsverweigerung gefährdet würde. Die Gründe der Auskunftsverweigerung sind aktenkundig zu machen. Wird die Auskunftserteilung abgelehnt, ist die betroffene Person auf die Rechtsgrundlage für das Fehlen der Begründung und darauf hinzuweisen, dass sie sich an den Unabhängigen Kontrollrat wenden kann. Dem Unabhängigen Kontrollrat ist auf sein Verlangen Auskunft zu erteilen, soweit es sich nicht um Informationen nach § 13 Absatz 4 des UKRat-Gesetzes handelt. Mitteilungen des Unabhängigen Kontrollrates an die betroffene Person dürfen keine Rückschlüsse auf den Erkenntnisstand des Bundesamtes für Verfassungsschutz zulassen, sofern es nicht einer weitergehenden Auskunft zustimmt.

Abschnitt 7

Schlussvorschriften

§ 72

Kontrolle und Durchsetzung von Unternehmenspflichten

(1) Das Bundesministerium des Innern kann Anordnungen und andere Maßnahmen treffen, um die Einhaltung der Pflichten nach den §§ 11 bis 15 sowie der auf Grund § 78 ergangenen Rechtsverordnungen sicherzustellen. Der Verpflichtete muss auf Anforderung dem Bundesministerium des Innern die hierzu erforderlichen Auskünfte erteilen. Das Bundesministerium des Innern ist zur Überprüfung der Einhaltung der Verpflichtungen befugt, die Geschäfts- und Betriebsräume während der üblichen Betriebs- oder Geschäftszeiten zu betreten und zu besichtigen. Die Befugnisse der Bundesnetzagentur bleiben unberührt.

(2) Über die Befugnis zu Anordnungen nach Absatz 1 hinaus kann das Bundesministerium des Innern den Betrieb des Unternehmens ganz oder teilweise untersagen, wenn mildere Eingriffe zur Durchsetzung rechtmäßigen Verhaltens nicht ausreichen.

(3) Zur Durchsetzung von Maßnahmen nach den Absätzen 1 und 2 kann nach Maßgabe des Verwaltungsvollstreckungsgesetzes ein Zwangsgeld bis zu 1 Million Euro festgesetzt werden.

§ 73

Besondere Anzeige- und Genehmigungspflicht für ausgeschiedene Bedienstete

(1) § 105 Absätze 2 bis 6 des Bundesbeamtengesetzes gelten für frühere Beamte des Bundesamtes für Verfassungsschutz auch dann entsprechend, wenn es sich nicht um frühere Beamtinnen mit Versorgungsbezügen und frühere Beamte mit Versorgungsbezügen sowie um frühere Beamtinnen mit Anspruch auf Altersgeld und frühere Beamte mit Anspruch auf Altersgeld handelt.

(2) § 105 Absatz 2 bis 6 des Bundesbeamtengesetzes gelten für frühere Angestellte des Bundesamtes für Verfassungsschutz entsprechend.

§ 74

Strafvorschriften

(1) Mit Freiheitsstrafe bis zu 2 Jahren oder mit Geldstrafe wird bestraft, wer entgegen § 9 Absatz 3 Nummer 1 eine Mitteilung macht.

(2) Wird durch die Mitteilung der Zweck der Maßnahme oder werden eingesetzte Personen gefährdet, ist die Strafe Freiheitsstrafe von 3 Monaten bis zu 5 Jahren.

§ 75

Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer

1. einem vollziehbaren Ersuchen nach § 11 Absatz 1, § 12 Absatz 1 und 2, § 13 Absatz 1, auch in Verbindung mit § 14 Absatz 1 oder § 15 Absatz 1 zuwiderhandelt,

2. entgegen § 13 Absatz 6 Satz 1 nicht sicherstellt, dass eine Geheimschutzmaßnahme getroffen wird,

3. entgegen § 13 Absatz 6 Satz 3 Nummer 1 keine Personen auswählt, entgegen § 13 Absatz 6 Satz 4 eine Person betraut oder einer Anordnung nach § 13 Absatz 6 Satz 6 zuwiderhandelt oder

4. entgegen § 72 Absatz 1 Satz 2 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt.

5. entgegen § 73 in Verbindung mit § 105 Absatz 5 des Bundesbeamtengesetzes eine genehmigungspflichtige Erwerbstätigkeit oder genehmigungspflichtige sonstige Beschäftigung ohne Genehmigung aufnimmt oder

6. entgegen § 73 in Verbindung mit § 105 Absatz 2 des Bundesbeamtengesetzes eine Erwerbstätigkeit oder sonstige Beschäftigung ohne vorherige Anzeige aufnimmt oder entgegen § 73 in Verbindung mit § 105 Absatz 4 Satz 2 des Bundesbeamtengesetzes trotz vorläufiger Untersagung der Aufnahme aufnimmt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße geahndet werden.

1. bei Absatz 1 Nummer 1 bis zu dreihunderttausend Euro,

2. bei Absatz 1 Nummer 2 und 3 bis zu fünfhunderttausend Euro,

3. bei Absatz 1 Nummer 4 bis zu einhunderttausend Euro,

4. bei Absatz 1 Nummer 5 bis zu fünfzigtausend Euro,

5. bei Absatz 1 Nummer 6 bis zu zehntausend Euro.

(3) Bußgeldbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundesministerium des Innern.

§ 76

Spannungs- und Verteidigungsfall

(1) Im Spannungsfall (Artikel 80a des Grundgesetzes) und im Verteidigungsfall (Artikel 115a des Grundgesetzes) finden ergänzend die Regelungen der folgenden Absätze Anwendung.

(2) Unternehmen der gewerblichen Wirtschaft sind auf Ersuchen verpflichtet, dem Bundesamt für Verfassungsschutz Auskünfte und technische Unterstützung auch über die §§ 11 bis 15 hinaus zu leisten, wenn

1. dazu im Spannungs- oder Verteidigungsfall besonderer Bedarf besteht und

2. dies im Einzelfall für Aufgaben des Bundesamtes für Verfassungsschutz erforderlich ist.

Zum Ersuchen befugt sind das Bundesministerium des Innern oder mit seiner Zustimmung, die auch für eine Reihe gleichgelagerter Fälle erteilt werden kann, das Bundesamt für Verfassungsschutz. Die Verpflichtung ist beschränkt auf Auskünfte und technische Unterstützung, die mit den betrieblichen Mitteln des Verpflichteten erbracht werden können,

einschließlich Überlassung betrieblicher Materialien oder Zugangsgewährung zur Mitnutzung betrieblicher Mittel. Die Mitwirkungspflicht muss mit sonstigen gesetzlichen Pflichten zur Sicherstellung und Vorsorge vereinbar sein und darf das Unternehmen in seiner gewerblichen Tätigkeit nicht in einer Weise einschränken, die außer Verhältnis zu dem mit der Mitwirkung bezweckten Schutz steht. Für die Mitwirkung hat das Bundesamt für Verfassungsschutz eine angemessene Entschädigung zu leisten, deren Höhe sich an den nachgewiesenen tatsächlichen Kosten orientiert. Anbieter von öffentlich zugänglichen Telekommunikationsdiensten und geschäftsmäßigen Postdiensten sind zur Geheimhaltung nach § 13 Absatz 6 verpflichtet.

(3) Für den Einsatz nachrichtendienstlicher Mittel gelten folgende Maßgaben:

1. von Anwerbung und Einsatz als Vertrauensperson sind Personen nach § 18 Absatz 1 Satz 2 Nummer 1 bis 3 und 5 nicht ausgeschlossen,

2. Maßnahmen nach § 24 Absatz 2 und im Verteidigungsfall nach § 25 Absatz 1 und § 27 Absatz 1 sind unabhängig davon zulässig, ob eine polizeiliche Ausführung rechtzeitig möglich wäre, wobei im Fall des § 24

   a) unerheblich ist, ob die Informationen auch durch Übermittlung eines nach § 12 Verpflichteten gewonnen werden können,

   b) die Herstellung einer Sicherungskopie nicht notwendig ist, wenn dies in der Lage den Zweck der Maßnahme gefährden kann,

3. in der Anordnung von Maßnahmen sind im Verteidigungsfall Einsatzfreigaben in der Dauer nicht durch § 33 Absatz 4 beschränkt.

Im Fall des Satzes 1 Nummer 3 kann mit Wegfall des Verteidigungsfalls kann eine laufende Maßnahme vor einer neuerlichen Anordnung längstens mit der in § 33 Absatz 4 bestimmten Frist fortlaufen.

(4) Mitteilungen nach den §§ 35, 58 Absatz 4 und 65 Absatz 4 sowie Auskünfte nach § 71 an betroffene Personen unterbleiben. Abweichend von Satz 1 werden im Spannungsfall zu Maßnahmen nach § 22 Absatz 1 Satz 1 und den §§ 25, 27 Mitteilungen und deren Prüfung lediglich bis zum Ende des Spannungsfalls zurückgestellt. Dauert der Spannungsfall länger als 3 Monate, unterbleiben die Mitteilungen auch in den Fällen des Satzes 2.

(5) Die Datenpflege in Dateisystemen nach § 38 kann mit Ausnahme der Berichtigung unterbleiben. Dokumentationen und Protokollierungen nach diesem Gesetz können unterbleiben, wenn sie mit zusätzlichen Verwaltungsaufwänden verbunden sind.

(6) Übermittlungen sind auch zulässig, soweit dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist

1. für den Schutz besonders wichtiger Rechtsgüter,

2. zur Verfolgung einer Straftat, die zur Beteiligung an einer Bedrohung begangen worden ist.

(7) Zur Unterstützung unabhängiger Rechts- und Datenschutzkontrolle nach § 69 Absatz 3 ist das Bundesamt für Verfassungsschutz nur nach Entscheidung des Parlamentarischen Kontrollgremiums verpflichtet. Beim Schutz kernbereichsrelevanter Informationen kommt § 31 Absatz 4 Satz 1 Nummer 2 nicht und Absatz 5 mit der Maßgabe zur Anwendung, dass die Vorlage einheitlich an den Aufsichtsbediensteten erfolgt.

(8) Für seine Vorabkontrolle nach § 34 Absatz 1 kann der Unabhängige Kontrollrat die Rechtmäßigkeitsfeststellung für eine Reihe von Maßnahmen, die nach Art, Umständen und Umfang bestimmt sind, auch allgemein treffen und dazu Maßgaben vorsehen, wie ihm über

entsprechende Anordnungen zu berichten ist. Soweit die Bundesregierung mit Zustimmung des Parlamentarischen Kontrollgremiums festgestellt hat, dass dies zwingend notwendig ist, entfällt die Vorabkontrolle nach § 34 Absatz 1. Die Bundesregierung hat die Feststellung nach Satz 2 aufzuheben, wenn die Voraussetzungen hierfür entfallen sind oder das Parlamentarische Kontrollgremium oder der Deutsche Bundestag es verlangen.

§ 77

Anwendung durch Landesbehörden für Verfassungsschutz

(1) Auch für die Landesbehörden für Verfassungsschutz gelten die Regelungen über

1. Ausschreibungen nach § 10 Absatz 3 Satz 1,

2. Datenerhebungen über Inhalte, auch verbunden mit den Umständen, von Post- und Telekommunikationsverkehren nach den §§ 13, 14 und 22, wenn im Landesrecht eine grundsätzlich vorherige und unabhängige Anordnungskontrolle vorgesehen ist und,

3. Übermittlungen nach § 46 Absatz 2 und § 48 in Verbindung mit den §§ 52, 53, 59 unter Ausschluss von Übermittlungen zwischen Behörden desselben Bundeslandes.

(2) Auf Übermittlungen an eine Landesbehörde für Verfassungsschutz durch eine Behörde eines anderen Landes oder des Bundes ist § 10 Absatz 1 anzuwenden.

(3) Auf die Durchführung dieses Gesetzes im Landesvollzug sind die Begriffsbestimmungen des § 3 anzuwenden.

§ 78

Verordnungsermächtigung

Das Bundesministerium des Innern wird ermächtigt, durch Rechtsverordnung im Einvernehmen mit dem Bundeskanzleramt, dem Bundesministerium für Finanzen, dem Bundesministerium der Verteidigung, dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und Verbraucherschutz, dem Bundesministerium für Digitales und Staatsmodernisierung und dem Bundesministerium für Verkehr mit Zustimmung des Bundesrates das Nähere zu regeln

1. zur technischen und organisatorischen Umsetzung der Pflicht, die Einbringung von technischen Mitteln des Bundesamtes für Verfassungsschutz nach § 13 Absatz 5 zu ermöglichen,

2. zur Form von Übermittlungen nach den §§ 11 bis 14 an das Bundesamt für Verfassungsschutz, soweit dazu keine Regelungen auf Grund des § 170 des Telekommunikationsgesetzes getroffen werden, insbesondere, dass Übermittlungen ganz oder teilweise auf maschinell verwertbaren Datenträgern oder durch Datenfernübertragung übermitteln müssen, einschließlich

   a) der Voraussetzungen für die Anwendung des Verfahrens,

   b) des Näheren über Form, Inhalt, Verarbeitung und Sicherung der zu übermittelnden Daten,

   c) der Art und Weise sowie der Adressierung der Übermittlung der Daten,

d) des Umfangs und der Form der für dieses Verfahren erforderlichen besonderen Erklärungspflichten des Verpflichteten.

Zur Regelung der Datenübermittlung kann in der Rechtsverordnung auf Veröffentlichungen sachverständiger Stellen verwiesen werden. Hierbei sind das Datum der Veröffentlichung, die Bezugsquelle und eine Stelle zu bezeichnen, bei der die Veröffentlichung archivmäßig gesichert niedergelegt ist.

§ 79

Einschränkung von Grundrechten

Die Grundrechte der Versammlungsfreiheit (Artikel 8 des Grundgesetzes), des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) und der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) werden nach Maßgabe dieses Gesetzes eingeschränkt. Das Grundrecht auf körperliche Unversehrtheit (Artikel 2 Absatz 2 Satz 1 des Grundgesetzes) und Freiheit der Person (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes) wird durch § 28 Absatz 1, § 64 Absatz 7 und § 66 Absatz 2 Satz 2 eingeschränkt.

§ 80

Übergangsvorschriften

(1) Für Anordnungen nachrichtendienstlicher Maßnahmen, die auf Grundlage des § 8a Absatz 1 Satz 1 Nummer 4 des Bundesverfassungsschutzgesetzes in der bis zum […] [einsetzen: Datum des Tages, der vor dem Datum des Inkrafttretens dieses Gesetzes nach Artikel X liegt] geltenden Fassung oder des Artikel 10-Gesetzes in der bis zum […][einsetzen: Datum des Tages, der vor dem Datum des Inkrafttretens dieses Gesetzes nach Artikel X liegt] erlassen worden sind und die deren Befristung zum Zeitpunkt des Inkrafttretens dieses Gesetzes noch nicht abgelaufen ist, bestimmt sich die Anordnungsdauer entsprechend der nach § 33 Absatz 4 Satz 1 höchstzulässigen Befristung.

(2) Abweichend von den §§ 33 und 34 können Anordnungen nachrichtendienstlicher Maßnahmen bis zum [einsetzen: Angabe des Tages und Monats der Verkündung dieses Gesetzes sowie die Jahreszahl des ersten auf die Verkündung folgenden Kalenderjahres] nach den vor Inkrafttreten dieses Gesetzes geltenden Vorschriften erlassen und vollzogen werden. Dies gilt nicht für die in § 34 Absatz 1 Satz 1 Nummer 6, 9 und Absatz 4 genannten Maßnahmen.

(3) Die Mitteilungspflicht nach § 35 gilt für Maßnahmen, für die noch keine unabhängige Anordnungskontrolle nach § 34 erfolgt ist, bis zum [einsetzen: Angabe des Tages und Monats der Verkündung dieses Gesetzes sowie die Jahreszahl des ersten auf die Verkündung folgenden Jahres] nur dann, wenn bereits vor dem [einsetzen: Datum des Inkrafttretens dieses Gesetzes nach Artikel X] eine Mitteilungspflicht bestand.

(4) Die Dienstvorschrift nach § 16 Absatz 4 Satz 1 ist bis zum … [einsetzen: Datum des ersten Tages des zwölften auf die Verkündung dieses Gesetzes folgenden Kalendermonats] neu zu erlassen. In die nach Satz 1 neu zu erlassende Dienstvorschrift dürfen nachrichtendienstliche Mittel nach § 16 Absatz 4 Satz 2 nur dann zur Erprobung aufgenommen werden, wenn sie nicht bereits in der bis zum Erlass dieser Dienstvorschrift geltenden Dienstvorschrift enthalten sind oder dort enthalten waren.

(5) Solange für Datenerhebungen nach § 77 Absatz 1 Nummer 2 nach Landesrecht keine grundsätzlich vorherige und unabhängige Anordnungskontrolle besteht, ist auf diese Datenerhebungen bis längstens zum Ablauf des 31. Dezember 2029 das Artikel 10-

Gesetzes in der bis einschließlich ... [einsetzen: Datum des Tages der Verkündung dieses Gesetzes] geltenden Fassung weiter anzuwenden.

Artikel 2

Gesetz über den Bundesnachrichtendienst

(BND-Gesetz – BNDG)

Inhaltsübersicht

Abschnitt 1
Aufgaben, allgemeine Befugnisse und Vorgaben

§ 1 Bundesnachrichtendienst

§ 2 Aufgabe

§ 3 Erhebliche Bedrohungen

§ 4 Bedrohungen von herausgehobener Bedeutung

§ 5 Allgemeine Befugnisse

§ 6 Allgemeine Vorgaben

Abschnitt 2
Datenerhebung unter Mitwirkung anderer Stellen

Unterabschnitt 1
Allgemeine Befugnisse und Vorgaben für die Datenerhebung unter Mitwirkung anderer Stellen

§ 7 Befugnis zur Datenerhebung unter Mitwirkung anderer Stellen

§ 8 Mitteilungs- und Benachteiligungsverbot

§ 9 Umfang von Auskunftspflichten

Unterabschnitt 2
Datenerhebung unter Mitwirkung öffentlicher Stellen

§ 10 Übermittlung von Daten an den Bundesnachrichtendienst durch inländische öffentliche Stellen

§ 11 Verpflichtende Auskunftsersuchen gegenüber inländischen öffentlichen Stellen

Unterabschnitt 3
Datenerhebung unter Mitwirkung nichtöffentlicher Stellen

§ 12 Auskunftsersuchen gegenüber nichtöffentlichen Stellen

§ 13 Qualifizierte Ersuchen gegenüber nicht öffentlichen Stellen

§ 14 Besondere Auskunftsersuchen bei informationstechnischen Angriffen

§ 15 Ersuchen gegenüber privaten Einrichtungen der Videoüberwachung

§ 16 Pflichten bei Ersuchen an nicht öffentliche Stellen

§ 17 Anordnungen

Abschnitt 3
Einsatz nachrichtendienstlicher Mittel

Unterabschnitt 1
Allgemeine Befugnis und Vorgaben für den Einsatz nachrichtendienstlicher Mittel

§ 18 Einsatz nachrichtendienstlicher Mittel

§ 19 Besonderer Einsatz nachrichtendienstlicher Mittel

§ 20 Einsatz nachrichtendienstlicher Mittel gegen eine Person

§ 21 Schutz des Kernbereichs privater Lebensgestaltung

§ 22 Schutz von Vertraulichkeitsbeziehungen

§ 23 Vorgaben für den Einsatz nachrichtendienstlicher Verbindungen

Unterabschnitt 2
Besondere Befugnisse zum Einsatz nachrichtendienstlicher Mittel

§ 24 Einsatz nachrichtendienstlicher Verbindungen gegen eine Person

§ 25 Nutzung einer Legende auf vertiefter Vertrauensbasis

§ 26 Einsatz technischer Mittel zur längerfristigen Standortfeststellung

§ 27 Längerfristige optische und akustische Überwachung

§ 28 Maßnahmen bei Post- und Warensendungen

§ 29 Wohnraumüberwachung

Unterabschnitt 3
Besondere Befugnisse der technischen Aufklärung

§ 30 Begriffsbestimmungen der technischen Aufklärung

§ 31 Vorgaben für die strategische Aufklärung

§ 32 Erhebung von Daten im Rahmen von strategischen Aufklärungsmaßnahmen

§ 33 Einsichtnahme in Kommunikationsdaten im Rahmen von strategischen Aufklärungsmaßnahmen

§ 34 Besondere Vorgaben für die Einsichtnahme in Kommunikationsdaten mit qualifiziertem Inlandsbezug

§ 35 Telekommunikationsüberwachung

§ 36 Erhebung technischer Spuren aus informationstechnischen Systemen bei informationstechnischen Angriffen

§ 37 Erhebung von Daten aus informationstechnischen Systemen

§ 38 Abgegrenzte Erhebung von Daten aus informationstechnischen Systemen

§ 39 Vorgaben für die Erhebung von Daten aus informationstechnischen Systemen

§ 40 Datenerhebung durch eine ausländische öffentliche Stelle

§ 41 Kooperation mit ausländischen öffentlichen Stellen bei der technischen Aufklärung

§ 42 Absichtserklärung für Kooperationen mit ausländischen öffentlichen Stellen bei der technischen Aufklärung

§ 43 Übermittlung von selektierten Kommunikationsdaten im Rahmen von Kooperationen zur strategischen Aufklärung

§ 44 Übermittlung unselektierter kommunikationsbezogener Metadaten im Rahmen von Kooperationen bei der strategischen Aufklärung

§ 45 Übermittlung personenbezogener Daten im Rahmen von Kooperationen zur Telekommunikationsüberwachung oder der Erhebung gespeicherter Daten aus informationstechnischen Systemen

Unterabschnitt 4

Anordnungen

§ 46 Anordnung des Einsatzes nachrichtendienstlicher Mittel

§ 47 Anordnungen im Zusammenhang mit strategischen Aufklärungsmaßnahmen

§ 48 Anordnung sonstiger besonderer Befugnisse der technischen Aufklärung

Abschnitt 4

Erweiterte nachrichtendienstliche Maßnahmen

§ 49 Spezifische Gefährdungslage

§ 50 Grundanordnung

§ 51 Befugnis für erweiterte nachrichtendienstliche Maßnahmen

Abschnitt 5

Weiterverarbeitung personenbezogener Daten

Unterabschnitt 1

Allgemeine Weiterverarbeitungsvorschriften

§ 52 Allgemeine Befugnis zur Weiterverarbeitung

§ 53 Besondere Befugnis zum Abruf von Auswertungsprodukten mit qualifiziertem Eingriffsgewicht

§ 54 Weiterverarbeitung von personenbezogenen Daten aus informationstechnischen Speichern

§ 55 Datensätze zu minderjährigen Personen

§ 56 Prüf- und Löschpflichten

§ 57 Protokolldaten

§ 58 Verwendungseinschränkung personenbezogener Daten

§ 59 Berichtigungspflicht

§ 60 Weiterverarbeitung zu Forschungs- oder Entwicklungszwecken

§ 61 Errichtungsanordnungen für Personendatenbanken

§ 62 Akten

§ 63 Gemeinsame automatisierte Auswertung mit inländischen öffentlichen Stellen

Unterabschnitt 2

Besondere Weiterverarbeitungsvorschriften für Daten aus der technischen Aufklärung

§ 64 Besondere Kennzeichnungspflichten für Daten aus der technischen Aufklärung

§ 65 Besondere Prüfpflichten für Daten aus der technischen Aufklärung

§ 66 Besondere Löschpflichten für Daten aus der technischen Aufklärung

§ 67 Besondere Protokollierungspflichten für Daten aus der technischen Aufklärung

A b s c h n i t t 6

Ü b e r m i t t l u n g v o n p e r s o n e n b e z o g e n e n D a t e n

Unterabschnitt 1

Politische Unterrichtung und Information der Öffentlichkeit

§ 68 Politische Unterrichtung

§ 69 Information der Öffentlichkeit

Unterabschnitt 2

Vorgaben zur Übermittlung von personenbezogenen Daten durch den Bundesnachrichtendienst

§ 70 Zweckbindung der übermittelten personenbezogenen Daten

§ 71 Protokollierung der Übermittlung

§ 72 Verbundene personenbezogene Daten

§ 73 Pflicht zur Übermittlung vervollständigter oder berichtigter Daten

§ 74 Verbot der Übermittlung

§ 75 Schutz von minderjährigen Personen bei Übermittlungen

§ 76 Übermittlung im Interesse der betroffenen Person

§ 77 Vorgaben für die Übermittlung von personenbezogenen Daten aus besonderen Erhebungsarten

§ 78 Einrichtung automatisierter Abrufverfahren

Unterabschnitt 3

Übermittlung von personenbezogenen Daten durch den Bundesnachrichtendienst

§ 79 Übermittlung an inländische Nachrichtendienste

§ 80 Übermittlung an die Bundeswehr

§ 81 Übermittlung an inländische öffentliche Stellen zur Strafverfolgung

§ 82 Übermittlung an inländische öffentliche Stellen zur Gefahrenabwehr

§ 83 Übermittlung an inländische öffentliche Stellen im Gefahrenvorfeld

§ 84 Übermittlung an inländische öffentliche Stellen ohne Möglichkeit operativer Anschlussmaßnahmen

§ 85 Übermittlung an inländische nichtöffentliche Stellen

§ 86 Übermittlung an ausländische öffentliche Stellen oder an über- oder zwischenstaatliche Stellen

§ 87 Übermittlung an ausländische nichtöffentliche Stellen

§ 88 Übermittlung von sonstigen personenbezogenen Daten

Unterabschnitt 4
Gemeinsame Dateien

§ 89 Projektbezogene gemeinsame Dateien mit inländischen öffentlichen Stellen

§ 90 Führung projektbezogener gemeinsamer Dateien mit inländischen öffentlichen Stellen durch den Bundesnachrichtendienst

§ 91 Erweiterte Nutzung projektbezogener gemeinsamer Dateien mit inländischen öffentlichen Stellen

§ 92 Gemeinsame Dateien mit der Bundeswehr

§ 93 Gemeinsame Dateien mit ausländischen öffentlichen Stellen

§ 94 Führung gemeinsamer Dateien mit ausländischen öffentlichen Stellen durch den Bundesnachrichtendienst

Abschnitt 7
Ergänzende Bestimmungen und Kontrollzuständigkeiten

Unterabschnitt 1
Dienstvorschriften, Unterrichtungspflichten und Kontrollzuständigkeiten

§ 95 Dienstvorschriften

§ 96 Unterrichtung des Parlamentarischen Kontrollgremiums und des Deutschen Bundestages

§ 97 Kontrollgegenstände die der Vorabkontrolle unterliegen

§ 98 Unabhängige Kontrolle durch den Unabhängigen Kontrollrat und die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

§ 99 Anwendung anderer Gesetze

Unterabschnitt 2
Mitteilung und Auskunftsverpflichtung

§ 100 Mitteilung an betroffene Personen

§ 101 Zurückstellung der Mitteilung

§ 102 Auskunft an betroffene Personen

§ 103 Rechtswegausschluss

Abschnitt 8
Besondere Bestimmungen zur Sicherung der Bediensteten, Dienststellen und Verschlusssachen

Unterabschnitt 1
Begriffsbestimmungen und allgemeine Vorgaben

§ 104 Begriffsbestimmungen zur Sicherung der Bediensteten, Dienststellen und Verschlusssachen

§ 105 Allgemeine Vorgaben

§ 106 Besondere Sicherheitsbereiche

§ 107 Öffentliche Hinweispflichten

Unterabschnitt 2
Befugnisse zur Sicherung der Bediensteten und Dienststellen

§ 108 Betroffene Personen

§ 109 Personenüberprüfung

§ 110 Durchsuchung, Sicherstellung und Beschlagnahme

§ 111 Erweiterte Befugnisse bei qualifiziert funktionsgefährdenden Tätigkeiten

§ 112 Maßnahmen gegen den unbefugten Betrieb unbemannter Fluggeräte

§ 113 Einsatzsicherung

§ 114 Anordnung von Maßnahmen zur Sicherung der Bediensteten und Dienststellen

Unterabschnitt 3
Befugnisse zur Sicherung von Verschlusssachen

§ 115 Betroffene Personen; Mitwirkungspflicht; Belehrung

§ 116 Kontrolle und Durchsuchung von Personen, Taschen und Fahrzeugen zur Sicherung von Verschlusssachen

§ 117 Kontrolle und Durchsuchung von Räumen zur Sicherung von Verschlusssachen

§ 118 IT-Kontrollen zur Sicherung von Verschlusssachen

§ 119 Besondere Maßnahmen zur Sicherung von Verschlusssachen

§ 120 Anordnung von Maßnahmen zur Sicherung von Verschlusssachen

Unterabschnitt 4
Durchführung von Maßnahmen

§ 121 Vorgaben zur Durchführung von Maßnahmen durch unmittelbaren Zwang

§ 122 Besondere Vorgaben zur Durchführung von Maßnahmen zur Sicherung von Verschlusssachen

Unterabschnitt 5
Verarbeitung von personenbezogenen Daten aus Maßnahmen zur Sicherung von Verschlusssachen

§ 123 Besondere Bestimmungen zur Verarbeitung personenbezogener Daten

§ 124 Schutz von minderjährigen Personen

Abschnitt 9
Landes- und Bündnisverteidigung

§ 125 Verteidigungs-, Spannungs- und Zustimmungsfall

§ 126 Unterstützung durch andere Stellen

§ 127 Datenerhebung unter Mitwirkung anderer Stellen

§ 128 Einsatz nachrichtendienstlicher Mittel

§ 129 Erweiterte nachrichtendienstliche Maßnahmen

§ 130 Weiterverarbeitung personenbezogener Daten

§ 131 Übermittlung von personenbezogenen Daten

§ 132 Ergänzende Bestimmungen

§ 133 Besondere Bestimmungen zum Schutz der Bediensteten, Dienststellen und Verschlusssachen

Abschnitt 10
Unternehmenspflichten, Anzeigepflichten, Straf- und Bußgeldvorschriften

§ 134 Kontrolle und Durchsetzung von Unternehmenspflichten

§ 135 Besondere Anzeige- und Genehmigungspflicht für ausgeschiedene Bedienstete des Bundesnachrichtendienstes

§ 136 Strafvorschriften

§ 137 Bußgeldvorschriften

Abschnitt 11
Schlussvorschriften

§ 138 Verordnungsermächtigung

§ 139 Einschränkung von Grundrechten

§ 140 Übergangsvorschriften

Abschnitt 1

Aufgaben, allgemeine Befugnisse und Vorgaben

§ 1

Bundesnachrichtendienst

(1) Der Bundesnachrichtendienst ist der Auslandsnachrichtendienst der Bundesrepublik Deutschland.

(2) Er ist eine Bundesoberbehörde im Geschäftsbereich des Bundeskanzleramtes. Einer polizeilichen Dienststelle darf er nicht angegliedert werden.

§ 2

Aufgabe

(1) Aufgabe des Bundesnachrichtendienstes ist die nachrichtendienstliche Auslandsaufklärung. Die nachrichtendienstliche Auslandsaufklärung ist die Sammlung und Auswertung von erforderlichen Informationen zur Gewinnung von Erkenntnissen über das Ausland, die von außen- oder sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, mit dem Ziel der Früherkennung von Bedrohungen für besonders gewichtige Rechtsgüter. Zur nachrichtendienstlichen Auslandsaufklärung zählen auch die zur

Erfüllung dieser Aufgabe erforderlichen Tätigkeiten zum Schutz der Personen, die für den Bundesnachrichtendienst tätig sind, sowie der Einrichtungen, Gegenstände und geheimhaltungsbedürftigen Informationen des Bundesnachrichtendienstes. Bedrohungen im Sinne des Satzes 2 können im Einzelnen als erhebliche Bedrohungen nach § 3 oder Bedrohungen von herausgehobener Bedeutung nach § 4 zu qualifizieren sein.

(2) Besonders gewichtige Rechtsgüter sind insbesondere:

1. Bestand oder Sicherheit

   a) des Bundes oder eines Landes,

   b) von Einrichtungen internationaler Organisationen, sofern die Bundesrepublik Deutschland Mitglied dieser Organisationen ist, oder

   c) eines Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrags,

2. die Bündnis- und Verteidigungsfähigkeit der Bundesrepublik Deutschland,

3. die außenpolitische Handlungsfähigkeit der Bundesrepublik Deutschland,

4. die freiheitliche demokratische Grundordnung,

5. gewichtige Rechtsgüter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, sowie Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,

6. das Leben, die körperliche Unversehrtheit, Freiheit und sexuelle Selbstbestimmung einer Person.

§ 3

Erhebliche Bedrohungen

(1) Im Rahmen der nachrichtendienstlichen Auslandsaufklärung (§ 2 Absatz 1) ist eine Bedrohung als erheblich einzustufen, wenn sie geeignet ist, ein besonders gewichtiges Rechtsgut in besonderem Maße zu beeinträchtigen (erhebliche Bedrohung).

(2) Für die Qualifikation einer Bedrohung als erhebliche Bedrohung sind besonders zu berücksichtigen:

1. die in Absatz 3 genannten erheblichen Bedrohungsziele sowie

2. die in Absatz 4 genannten erheblichen Bedrohungsfelder.

(3) Erhebliche Bedrohungsziele sind:

1. die inländische oder europäische Wirtschaft und Wissenschaft im Falle ihrer erheblichen Beeinträchtigung,

2. die Versorgung der Bundesrepublik Deutschland, der Mitgliedstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrags mit wesentlichen Rohstoffen und Gütern, Energien sowie kritischen Technologien im Falle ihrer erheblichen Beeinträchtigung,

3. die Sicherheit von Infrastruktur im Weltraum, sofern sie erhebliche Auswirkungen auf die Bundesrepublik Deutschland haben kann.

(4) Erhebliche Bedrohungsfelder sind:

1. der Terrorismus oder Extremismus, der gewaltbereit oder auf die planvoll verborgen betriebene Durchsetzung politischer, religiöser oder ideologischer Ansichten ausgerichtet ist, oder die Unterstützung dieses Terrorismus oder Extremismus,

2. hybride Einflussnahmen, soweit sie erhebliche Auswirkungen auf die Bundesrepublik Deutschland haben können, insbesondere wenn sie durch fremde Mächte gesteuert werden,

3. die grenzüberschreitende Verbreitung von Kriegswaffen im Sinne des Gesetzes über die Kontrolle von Kriegswaffen sowie der unerlaubte Außenwirtschaftsverkehr mit Waren und technischen Unterstützungsleistungen in Fällen von erheblicher Bedeutung,

4. die organisierte Kriminalität, soweit diese auf die Begehung von Straftaten von erheblicher Bedeutung gerichtet ist,

5. aufkommende disruptive Technologien, soweit sie erhebliche Auswirkungen auf die Bundesrepublik Deutschland haben können, wehrtechnische Technologien und dazugehörige Programme sowie Technologien der künstlichen Intelligenz, sowie

6. krisenhafte Entwicklungen im Ausland, soweit sie erhebliche Auswirkungen auf die Bundesrepublik Deutschland haben können.

§ 4

Bedrohungen von herausgehobener Bedeutung

(1) Im Rahmen der nachrichtendienstlichen Auslandsaufklärung (§ 2 Absatz 1) ist eine Bedrohung als von herausgehobener Bedeutung einzustufen, die über die in § 3 Absatz 1 genannten Voraussetzungen einer erheblichen Bedrohung hinausgehend geeignet ist, im Einzelfall zusätzlich ein erhöhtes Gefährdungspotenzial zu entfalten (Bedrohung von herausgehobener Bedeutung). Ein erhöhtes Gefährdungspotenzial liegt vor, wenn

1. eine erhebliche Bedrohung ein gesteigertes Schadenspotential aufweist oder

2. sich die erhebliche Bedrohung in deutlichem Maße verdichtet hat.

(2) Für die Qualifikation einer erheblichen Bedrohung als Bedrohung von herausgehobener Bedeutung sind besonders zu berücksichtigen:

1. die in § 3 Absatz 3 genannten herausgehobenen Bedrohungsziele,

2. die in § 3 Absatz 4 genannten herausgehobenen Bedrohungsfelder sowie

3. die in Absatz 5 genannten herausgehobenen Bedrohungslagen.

(3) Herausgehobene Bedrohungsziele sind:

1. die Gesamtverteidigung der Bundesrepublik Deutschland oder verbündeter Staaten und die Einsätze und dauerhaften Stationierungen der Bundeswehr oder verbündeter Streitkräfte im Ausland,

2. die Funktionsfähigkeit

   a) staatlicher Einrichtungen der Bundesrepublik Deutschland, einschließlich des Bundesnachrichtendienstes und seiner Eigenbefähigung, sowie von Mitgliedstaaten von internationalen Organisationen, sofern die Bundesrepublik Deutschland Mitglied dieser Organisationen ist,

   b) von Einrichtungen internationaler Organisationen, sofern die Bundesrepublik Deutschland Mitglied dieser Organisationen ist, und

   c) der kritischen Infrastrukturen der Bundesrepublik Deutschland und von Mitgliedstaaten von internationalen Organisationen, sofern die Bundesrepublik Deutschland Mitglied dieser Organisationen ist.

(4) Herausgehobene Bedrohungsfelder sind:

1. die erhöhte Gefährdungslage von Personen im Ausland, wenn dadurch Belange der Bundesrepublik Deutschland in besonderer Weise berührt sind,

2. die durch sicherheitsgefährdende oder geheimdienstliche Tätigkeiten hervorgerufene Gefährdung von

   a) Personen, die für den Bundesnachrichtendienst tätig sind, oder

   b) Einrichtungen, geheimhaltungsbedürftigen Informationen oder Gegenständen des Bundesnachrichtendienstes,

3. terroristische, staatliche oder internationale kriminelle Angriffe auf die Vertraulichkeit, Integrität oder Verfügbarkeit von informationstechnischen Systemen, insbesondere mittels Schadprogrammen,

4. sicherheitsgefährdende oder geheimdienstliche Strukturen sowie sicherheitsgefährdende oder geheimdienstliche Tätigkeiten mit Auswirkungen auf die Bundesrepublik Deutschland oder auf Mitgliedstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrags.

(5) Herausgehobene Bedrohungslagen sind solche,

1. die nationale Bündnis- und Verteidigungsinteressen oder militärische Auseinandersetzungen betreffen, sofern sich diese auch auf die Bundesrepublik Deutschland, auf internationale Organisationen, vorausgesetzt, die Bundesrepublik Deutschland ist Mitglied dieser Organisationen, oder auf Mitgliedstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrags erheblich auswirken,

2. die zu einer wesentlichen Beeinträchtigung der allgemeinen Sicherheitslage, der wirtschaftlichen Struktur oder der grundlegenden gesellschaftlichen Strukturen der Bundesrepublik Deutschland führen können,

~~3.~~ die zu einer Gefährdung wesentlicher außen- oder sicherheitspolitischer Belange der Bundesrepublik Deutschland führen können, oder

4. die im Zusammenhang mit Organisationen stehen, welche zur Zielverfolgung Straftaten begehen, die gegen besonders gewichtige Rechtsgüter gerichtet sind und im Höchstmaß mit Freiheitsstrafe von mindestens fünf Jahren bedroht sind, wenn dadurch die außen- oder sicherheitspolitischen Interessen der Bundesrepublik Deutschland erheblich beeinträchtigt werden.

§ 5

Allgemeine Befugnisse

~~(1)~~ Der Bundesnachrichtendienst darf Informationen einschließlich personenbezogener Daten erheben, soweit dies zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist und nicht besondere Regelungen in diesem Gesetz entgegenstehen. Die Erhebung ist auch dann zulässig, wenn die betroffene Person eingewilligt hat.

~~(2)~~ Der Bundesnachrichtendienst darf personenbezogene Daten zur systematischen Zusammenführung zu einer Person erheben, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist.

~~(3)~~ Der Bundesnachrichtendienst darf personenbezogener Daten aus allgemein zugänglichen Quellen mittels einer Anwendung erheben, die biometrische Merkmale mit Daten abgleicht, auf die der Bundesnachrichtendienst zur nachrichtendienstlichen Auslandsaufklärung zugreifen darf. Der Abgleich darf auch durch eine öffentliche oder nichtöffentliche Stelle in einem Drittstaat erfolgen, wenn der Abgleich nicht durch den Bundesnachrichtendienst selbst, eine andere inländische Stelle oder eine Stelle eines Mitgliedstaates der Europäischen Union gleichermaßen erfolgen kann. Die im Rahmen des biometrischen Abgleichs erhobenen Daten sind nach Durchführung des Abgleichs zu löschen, wenn keine tatsächlichen Anhaltspunkte dafür vorliegen, dass die Daten im Einzelfall für die nachrichtendienstliche Auslandsaufklärung erforderlich sind. Der Unabhängige Kontrollrat hat die Einhaltung der Vorschriften über den Datenschutz bei der Erhebung durch biometrischen Abgleich mindestens alle zwei Jahre zu kontrollieren.

(4) Der Bundesnachrichtendienst darf zum Schutz seiner Einrichtungen und von Personen, die für den Bundesnachrichtendienst tätig sind, Legenden einsetzen sowie die hierfür erforderlichen Tarnmittel herstellen und nutzen. Die für die Herstellung der Papiere und Kennzeichen zuständigen Behörden sind verpflichtet, dem Bundesnachrichtendienst bei der Beschaffung und Herstellung dieser Tarnmittel Hilfe zu leisten.

§ 6

Allgemeine Vorgaben

(1) Erhebt der Bundesnachrichtendienst personenbezogene Daten aufgrund der in den Abschnitten 2, 3 und 8 geregelten Befugnisse, so hat er von mehreren geeigneten Maßnahmen der Datenerhebung diejenige zu wählen, die die betroffene Person voraussichtlich am wenigsten beeinträchtigt. In Individualrechte darf nur nach Maßgabe spezieller Befugnisse eingegriffen werden.

(2) Eine Maßnahme der Datenerhebung darf keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht. Eine Maßnahme ist unverzüglich zu beenden, wenn ihr Zweck erreicht ist oder sich ergibt, dass er nicht oder nicht auf diese Weise erreicht werden kann. Einer Maßnahme der Datenerhebung steht nicht entgegen, dass andere Personen von ihr unvermeidbar mit betroffen sind.

~~(3)~~ Sieht eine Maßnahme der Datenerhebung besondere Voraussetzungen für den Fall vor, dass sich die Person, gegen die sich die Maßnahme richtet, im Bundesgebiet aufhält oder eine Person mit deutscher Staatsangehörigkeit ist, so gelten diese besonderen Voraussetzungen nicht, soweit

1. tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffene Person hoheitliche Aufgaben einer fremden Macht wahrnimmt, und

2. zu erwarten ist, dass durch die jeweilige Maßnahme ausschließlich oder ganz überwiegend Erkenntnisse erlangt werden, die im Zusammenhang mit der Ausübung der hoheitlichen Aufgaben stehen.

(4) Wird eine Maßnahme der Datenerhebung gegen eine Person, die nicht die deutsche Staatsangehörigkeit besitzt, zu einem Zeitpunkt angeordnet, zu dem sich die Person nicht im Bundesgebiet aufhält, darf die Maßnahme unter den Voraussetzungen der Anordnung für längstens 72 Stunden im Bundesgebiet fortgeführt werden, wenn der Zweck der Maßnahme andernfalls vereitelt oder wesentlich erschwert würde.

Abschnitt 2

Datenerhebung unter Mitwirkung anderer Stellen

Unterabschnitt 1

Allgemeine Befugnisse und Vorgaben für die Datenerhebung unter Mitwirkung anderer Stellen

§ 7

Befugnis zur Datenerhebung unter Mitwirkung anderer Stellen

(1) Der Bundesnachrichtendienst darf andere Stellen um Übermittlung von Informationen einschließlich personenbezogener Daten ersuchen, soweit dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist. Das Ersuchen darf nur diejenigen personenbezogenen Daten enthalten, die für die Erteilung der Auskunft erforderlich sind. Schutzwürdige Interessen der betroffenen Person dürfen nur in unvermeidbarem Umfang beeinträchtigt werden.

(2) Eine ersuchte inländische Stelle darf die Informationen einschließlich personenbezogener Daten übermitteln, wenn nicht besondere gesetzliche Übermittlungsregelungen entgegenstehen.

§ 8

Mitteilungs- und Benachteiligungsverbot

(1) Einer ersuchten inländischen Stelle und ihren Beschäftigten ist verboten,

1. der betroffenen Person oder Dritten Informationen über das Ersuchen oder dessen Durchführung mitzuteilen, auch im Wege gesetzlicher Verdachtsmeldungen,

2. allein auf Grund eines Ersuchens einseitige Handlungen vorzunehmen, die für die betroffene Person nachteilig sind und die über die Erteilung der Auskunft hinausgehen, insbesondere bestehende Verträge oder Geschäftsverbindungen zu beenden, ihren Umfang zu beschränken oder ein Entgelt zu erheben oder zu erhöhen.

(2) In Ersuchen ist auf die Pflichten nach Absatz 1 und darauf hinzuweisen, dass das Ersuchen nicht die Aussage beinhaltet, dass sich die betroffene Person rechtswidrig verhalten hat oder ein darauf gerichteter Verdacht bestehen müsse.

§ 9

Umfang von Auskunftspflichten

~~(1)~~ Die Auskunftspflicht ist auf jeweils vorhandene Daten beschränkt. Soweit dies im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist, kann mit einem Auskunftsersuchen auch die Verpflichtung verbunden werden, zukünftig bei der auskunftspflichtigen Stelle anfallende personenbezogene Daten zur Erfüllung des Auskunftsersuchens zu speichern.

(2) Die Auskunftspflicht erstreckt sich auch auf Daten, die innerhalb von zwölf Monaten nach Übermittlung des Auskunftsersuchens anfallen, wenn der Bundesnachrichtendienst um entsprechende Auskunft ersucht.

Unterabschnitt 2

Datenerhebung unter Mitwirkung öffentlicher Stellen

§ 10

Übermittlung von Daten an den Bundesnachrichtendienst durch inländische öffentliche Stellen

(1) Inländische öffentliche Stellen dürfen dem Bundesnachrichtendienst, auch ohne ein vorheriges Ersuchen des Bundesnachrichtendienstes, Informationen einschließlich personenbezogener Daten wie Personaldaten übermitteln, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist, und besondere gesetzliche Übermittlungsregelungen nicht entgegenstehen.

(2) Für die nachfolgenden Stellen gilt Absatz 1 mit der Maßgabe, dass eine Übermittlung verpflichtend ist:

1. das Bundesamt für Verfassungsschutz und die Landesbehörden für Verfassungsschutz sowie das Bundesamt für den Militärischen Abschirmdienst,

2. das Bundesamt für Sicherheit in der Informationstechnik,

3. die Zentralstelle für Finanztransaktionsuntersuchungen,

4. Justizvollzugsbehörden, die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien, die Behörden des Zollfahndungsdienstes sowie andere Zolldienststellen, soweit diese Aufgaben nach dem Bundespolizeigesetz wahrnehmen,

5. das Bundesamt für Migration und Flüchtlinge und

6. Finanzbehörden.

Zur Durchführung ihrer Übermittlungspflicht dürfen die öffentlichen Stellen auch Daten aus allgemein zugänglichen Quellen verarbeiten. Sie dürfen dem Bundesnachrichtendienst in geeigneten Fällen die Möglichkeit für den automatisierten Abruf von Daten einrichten.

(3) Die Zuständigkeit und das Verfahren für die Entscheidung des Bundesamtes für Migration und Flüchtlinge zu Übermittlungen nach Absatz 2 Satz 1 Nummer 5 sind in einer Dienstvorschrift zu regeln, die der Zustimmung des Bundesministerium des Innern bedarf.

Nach Absatz 2 Satz 1 Nummer 5 übermittelte personenbezogene Daten dürfen vom Bundesnachrichtendienst nicht weiter übermittelt werden, wenn überwiegende schutzwürdige Belange Dritter entgegenstehen. Vor einer Übermittlung an eine Stelle des Herkunftsstaates ist das Bundesamt für Migration und Flüchtlinge zu beteiligen.

(4) Die Übermittlungspflicht nach Absatz 2 gilt nicht für

1. die in Absatz 2 Satz 1 Nummer 1 genannten Stellen, wenn überwiegenden Sicherheitsinteressen entgegenstehen, und

2. die in Absatz 2 Satz 1 Nummer 4 genannten Stellen, wenn überwiegende Gründe des Schutzes verdeckt eingesetzter Personen oder des Schutzes operativer Maßnahmen entgegenstehen.

§ 11

Verpflichtende Auskunftsersuchen gegenüber inländischen öffentlichen Stellen

(1) Soweit tatsächliche Anhaltspunkte dafür vorliegen, dass es zur nachrichtendienstlichen Auslandsaufklärung oder zum Schutz der von dem Auskunftsersuchen betroffenen Person erforderlich ist, darf der Bundesnachrichtendienst jede inländische öffentliche Stelle um die Übermittlung von vorliegenden und künftig anfallenden Informationen einschließlich personenbezogener Daten wie Personaldaten ersuchen. Die nach Satz 1 ersuchte Stelle hat auf das Ersuchen des Bundesnachrichtendienstes die Informationen einschließlich personenbezogener Daten wie Personaldaten, die ihr bekannt sind, zu übermitteln, wenn besondere gesetzliche Übermittlungsregelungen nicht entgegenstehen. § 10 Absatz 4 gilt entsprechend.

(2) Der Bundesnachrichtendienst darf amtliche Register einsehen, wenn die Voraussetzungen des Absatz 1 Satz 1 vorliegen und

1. durch die Übermittlung nach Absatz 1 Satz 2

   a) der Zweck des Ersuchens gefährdet wäre, oder

   b) die betroffene Person unverhältnismäßig beeinträchtigt würde, oder

2. die Einsichtnahme erforderlich ist zur Identifizierung von Personen, die in einem Zusammenhang mit dem Aufklärungsziel stehen, der Grund zu der Annahme gibt, dass dadurch Erkenntnisse über die erheblichen Bedrohungen gewonnen werden können.

Das Einsehen amtlicher Register hat der Bundesnachrichtendienst zu dokumentieren. Aus der Dokumentation muss der Zweck und die Veranlassung, die registerführende Stelle und die Fundstelle hervorgehen.

(3) Soweit dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen, werden auf Ersuchen des Bundesnachrichtendienstes folgende Personen und Gegenstände im polizeilichen Informationsverbund durch die jeweils zuständige Stelle zur verdeckten Kontrolle ausgeschrieben:

1. Personen, die für die zumindest erhebliche Bedrohung verantwortlich sind oder diese unterstützen, und

2. Personen und Gegenstände, die im Zusammenhang mit dem Aufklärungsziel stehen, der Grund zu der Annahme gibt, dass dadurch Erkenntnisse über die erheblichen

Bedrohungen gewonnen werden können, die nicht durch eine Ausschreibung nach Nummer 1 zu gewinnen sind.

Satz 1 gilt nach der Maßgabe unmittelbar geltender Rechtsakte der Europäischen Union auch für Datenverarbeitungssysteme der Europäischen Union. Ist die Ausschreibungsfrist abgelaufen oder die Maßnahme einzustellen, ist die Ausschreibung unverzüglich zu löschen. Der Bundesnachrichtendienst hat Ersuchen und Eingaben zu protokollieren.

(4) Verfügungsberechtigte öffentlicher Einrichtungen zur Videobeobachtung des öffentlich zugänglichen Raums haben auf Ersuchen des Bundesnachrichtendienstes,

1. eine Mitbenutzung der Einrichtung durch den Bundesnachrichtendienst zu ermöglichen und dem Bundesnachrichtendienst zu diesem Zweck den Zutritt zu den Räumlichkeiten der Einrichtung zu gewähren,

2. gespeicherte Bild- und Tonaufzeichnungen aus Videoüberwachungen an den Bundesnachrichtendienst zu übermitteln und

3. Daten der Videoüberwachung in Echtzeit an den Bundesnachrichtendienst auszuleiten.

Ein Ersuchen nach Satz 1 ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist. Ist das Ersuchen auf die Übermittlung gespeicherter Bild- und Tonaufzeichnungen aus Videoüberwachungen gerichtet, ist es abweichend von Satz 2 nur zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen. Die überlassenen Bild- und Tonaufzeichnungen sind unverzüglich zurückzugeben, zu löschen oder zu vernichten, soweit die Voraussetzungen in Satz 3 nicht mehr vorliegen oder die Daten zur Aufgabenerfüllung nicht mehr erforderlich sind.

Unterabschnitt 3

Datenerhebung unter Mitwirkung nichtöffentlicher Stellen

§ 12

Auskunftsersuchen gegenüber nichtöffentlichen Stellen

(1) Der Bundesnachrichtendienst darf die in Absatz 2 genannten nichtöffentlichen Stellen um Auskunft ersuchen zu Informationen über den angebotenen Dienst sowie zu Daten, welche die Stelle für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung des Nutzungsverhältnisses mit den Nutzern der angebotenen Dienste speichert (Bestandsdaten), soweit tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall erforderlich ist

1. zur nachrichtendienstlichen Auslandsaufklärung, oder

2. zum Schutz der von dem Auskunftsersuchen betroffenen Person.

(2) Um Auskunft dürfen ersucht werden:

1. Stellen, die öffentlich zugängliche Leistungen im Personen- oder Güterverkehr erbringen oder an der Erbringung mitwirken,

2. Kraftfahrzeughersteller oder, wenn dies nicht oder nicht ohne Gefährdung des Zwecks der Maßnahme möglich ist, von Kraftfahrzeugwerkstätten,

3. die verpflichteten Stellen nach § 2 Absatz 1 des Geldwäschegesetzes, wenn sie nicht durch Rechtsverordnung nach § 2 Absatz 2 des Geldwäschegesetzes vom Anwendungsbereich des Geldwäschegesetzes ausgenommen oder entsprechend § 30 Absatz 3 Satz 3 und 4 des Geldwäschegesetzes zur Verweigerung der Auskunft berechtigt sind,

4. Stellen, die öffentlich zugängliche Post- und Warenverkehrsdienste erbringen oder an der Erbringung mitwirken,

5. Stellen, die öffentlich zugängliche Telekommunikationsdienste erbringen oder an der Erbringung mitwirken,

6. Stellen, die öffentlich zugängliche digitale Dienste erbringen oder an der Erbringung mitwirken, und

7. Stellen, die öffentlich zugängliche technische Dienste nach § 2 Absatz 1 Nummer 9 des Zahlungsdiensteaufsichtsgesetzes erbringen oder an der Erbringung mitwirken.

Ein Auskunftsersuchen gegenüber einer der in Satz 1 Nummer 5 und 6 genannten Stellen ist unzulässig, soweit die Auskunft auf Ersuchen nach § 11 im automatisierten Auskunftsverfahren von der Bundesnetzagentur nach § 173 Absatz 4 des Telekommunikationsgesetzes erlangt werden kann.

(3) Bei Ersuchen nach Absatz 1 oder der Ankündigung eines solchen Ersuchens haben die in Absatz 2 Satz 1 Nummer 4 und 5 genannten Stellen sicherzustellen, dass die Geheimschutzmaßnahmen zum Schutz als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufter Informationen gemäß der nach § 35 Absatz 1 des Sicherheitsüberprüfungsgesetzes zu erlassenden allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz in der jeweils geltenden Fassung getroffen werden. Sie haben geeignetes Personal vorzuhalten, das zu einer einfachen Sicherheitsüberprüfung bereit ist.

(4) Der Bundesnachrichtendienst darf auch ersuchen, dass ihm von den in Absatz 2 Satz 1 Nummer 5 und 6 genannten Stellen Auskunft anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse, des genutzten Zahlungsmittels, der genutzten Kontakt- und Anmeldedaten, oder anderer Daten, die für eine Identifikation geeignet sind erteilt wird. Die Rechtsgrundlage und die tatsächlichen Anhaltspunkte, die das Auskunftsersuchen veranlassen, sind durch den Bundesnachrichtendienst zu dokumentieren.

(5) Der Bundesnachrichtendienst darf auch die in Absatz 2 Satz 1 Nummer 5 und 6 genannten Stellen um Auskunft ersuchen zu Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird. Ein Ersuchen nach Satz 1 ist nur dann zulässig, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(6) § 93 Absatz 9 der Abgabenordnung findet bei Ersuchen des Bundesnachrichtendienstes nach § 93 Absatz 8 der Abgabenordnung keine Anwendung.

§ 13

Qualifizierte Ersuchen gegenüber nicht öffentlichen Stellen

(1) Der Bundesnachrichtendienst darf die in § 12 Absatz 2 genannten Stellen um Auskunft zu Informationen einschließlich personenbezogener Daten, die nicht auf Bestandsdaten oder Sachinformationen zu den angebotenen Diensten beschränkt sind, ersuchen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist. Sind deutsche Staatsangehörige, sich im Bundesgebiet aufhaltende Personen oder inländische juristische Personen Betroffene des Auskunftsersuchens gilt dies nur, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen.

(2) Auskunftsersuchen nach Absatz 1 Satz 2 dürfen sich nur auf Personen beziehen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie

1. für eine erhebliche Bedrohung verantwortlich sind oder diese unterstützen,

2. Mitglieder eines abgrenzbaren Netzwerks sind, sofern zugleich tatsächliche Anhaltspunkte dafür vorliegen, dass das Netzwerk für die zumindest erheblliche Bedrohung verantwortlich ist oder von seinen Mitgliedern ausschließlich oder ganz überwiegend dazu genutzt wird, um die zumindest erhebliche Bedrohung zu unterstützen, oder

3. in Zusammenhang mit einer erheblichen Bedrohung stehen, der Grund zu der Annahme gibt, dass durch die Maßnahme Erkenntnisse über die erhebliche Bedrohungen gewonnen werden können, die nicht gleichermaßen durch eine Maßnahme gegen eine Person nach Nummer 1 zu gewinnen sind, insbesondere

   a) bei einer Auskunft nach § 12 Absatz 2 Satz 1 Nummer 1 bis 4 und 6, dass diese Personen die Leistung für eine Person nach Nummer 1 in Anspruch nehmen,

   b) bei einer Auskunft nach § 12 Absatz 2 Satz 1 Nummer 4 und 5, dass diese Personen für eine Person nach Nummer 1 bestimmte oder von ihr herrührende Mitteilungen entgegennehmen oder weitergeben, oder

   c) bei einer Auskunft nach § 12 Absatz 2 Satz 1 Nummer 5, dass eine Person nach Nummer 1 oder Buchstabe b den Anschluss dieser Personen benutzt.

Bei Auskunftsersuchen gegenüber einem in § 12 Absatz 2 Nummer 5 genannten Dienstleister genügt die räumlich und zeitlich hinreichende Bezeichnung der Daten, sofern anderenfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre. Auskunftsersuchen nach Absatz 1 Satz 2 dürfen sich auch auf Personen beziehen, deren Einsatzfähigkeit als nachrichtendienstliche Verbindungen nach § 23 geprüft wird.

(3) Ein Auskunftsersuchen nach Absatz 1 Satz 1 gegenüber den in § 12 Absatz 2 Satz 1 Nummer 1 genannten Dienstleistern, die öffentlich zugängliche Leistungen im Güterverkehr erbringen, sowie den in § 12 Absatz 2 Satz 1 Nummer 4 genannten Dienstleistern, die öffentlich zugängliche Post- und Warenverkehrsdienste erbringen, darf auch auf Auskunft zu den vorliegenden Daten ohne konkreten Bezug zu einer Person gerichtet sein, wenn und soweit tatsächliche Anhaltspunkte dafür vorliegen, dass die Auskunft erforderlich ist, um grenzüberschreitende Transportwege und Beschaffungsrouten aufzuklären und Informationen zu zumindest erheblichen Bedrohungen zu erlangen. Dies gilt auch in den Fällen, in denen das Auskunftsersuchen zu den in Absatz 1 Satz 2 genannten betroffenen Personen erfolgt.

(4) Richtet sich ein Auskunftsersuchen nach Absatz 1 gegen eine der in § 12 Absatz 2 Satz 1 Nummer 4 genannten Stellen und dient es der Durchführung einer Maßnahme nach § 28, so hat die Stelle

1. Auskunft über die näheren Umstände des Postverkehrs zu erteilen,

2. Sendungen, die ihr zum Einsammeln, Weiterleiten oder Ausliefern anvertraut sind, auszuhändigen und

3. dem Bundesnachrichtendienst auf Verlangen die zur Vorbereitung einer Anordnung erforderlichen Auskünfte zu Postfächern zu erteilen, ohne dass es hierzu einer gesonderten Anordnung bedarf.

(5) Richtet sich ein Auskunftsersuchen nach Absatz 1 gegen eine der in § 12 Absatz 2 Satz 1 Nummer 5 genannten Stellen und dient es der Durchführung einer Maßnahme nach § 32, § 35 oder §§ 37 und 38, so hat die Stelle

1. Auskunft über die näheren Umstände der durchgeführten Telekommunikation zu erteilen,

2. Sendungen, die ihr zur Übermittlung auf dem Telekommunikationsweg anvertraut sind, auszuleiten,

3. die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen, auch durch Zugangsgewährung zu seinen Einrichtungen während seiner üblichen Geschäftszeiten, sowie

4. die Einbringung von technischen Mitteln zur Durchführung einer Maßnahme nach §§ 37 und 38 durch Unterstützung bei der Umleitung von Telekommunikation durch die berechtigte Stelle zu ermöglichen

   a) durch Mitteilung der zur Erbringung in den umgeleiteten Datenstrom erforderlichen Informationen über die Strukturen der von ihm betriebenen Telekommunikationsnetze und Telekommunikationsanlagen sowie die von ihm erbrachten Telekommunikationsdienste;

   b) durch sonstige Unterstützung bei der Umleitung einschließlich der Gewährung des Zugangs zu seinen Einrichtungen während seiner üblichen Geschäftszeiten sowie der Ermöglichung der Aufstellung und des Betriebs von Geräten für die Durchführung der Maßnahme.

(6) Bei Ersuchen nach Absatz 1 oder der Ankündigung eines solchen Ersuchens haben die in § 12 Absatz 2 Satz 1 Nummer 4 und 5 genannten Stellen unverzüglich die Personen, die mit der Durchführung der Maßnahme betraut werden sollen,

1. auszuwählen,

2. einer einfachen Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz unterziehen zu lassen und

3. über Mitteilungsverbote nach § 8 sowie die Strafbarkeit eines Verstoßes nach § 136 zu belehren; die Belehrung ist zu dokumentieren.

Mit der Durchführung eines Ersuchens nach Absatz 1 dürfen nur Personen betraut werden, die nach Maßgabe des Satzes 1 Nummer 2 und 3 überprüft und belehrt worden sind. Der Bundesnachrichtendienst kann Ausnahmen von Satz 2 zulassen. Der Bundesnachrichtendienst kann anordnen, dass Sicherheitsüberprüfungen bereits als organisatorische

Vorkehrung zur künftigen unverzüglichen Umsetzung von Überwachungsmaßnahmen durchzuführen sind.

§ 14

Besondere Auskunftsersuchen bei informationstechnischen Angriffen

(1) Der Bundesnachrichtendienst darf, wenn dies aufgrund tatsächlicher Anhaltspunkte zur Aufklärung eines möglichen Angriffs im Sinne des § 4 Absatz 4 Nummer 3 erforderlich ist, Anbieter, die öffentlich zugänglich informationstechnische Systeme Dritten zur Nutzung überlassen, ersuchen, Auskunft über technische Informationen zur Aufklärung der vom Angreifer zum Angriff genutzten Infrastruktur und Technik sowie zum Vorgehen und zu den Angriffszielen zu erteilen. Das Auskunftsersuchen kann sich insbesondere beziehen auf

1. den Verkehrsfluss zu bestimmten Kennungen, für die tatsächliche Anhaltspunkte bestehen, dass der Angreifer sie für den Angriff nutzt (maliziöse Kennungen), und

2. Schadprogramme oder sonstige Angriffswerkzeuge und deren Einsatz, einschließlich Steuerungs- oder Protokolldateien, und Spuren, die technisch mit dem Angriff verbunden sind, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass das informationstechnische System für die Angriffe genutzt wurde.

Sind in dem informationstechnischen System des Verpflichteten Daten gespeichert, die durch den Angriff beschafft worden sind, hat der Verpflichtete dem Bundesnachrichtendienst auch hierzu Auskunft zu geben.

(2) Wenn dem Verpflichteten eine Auskunft nach Absatz 1 Satz 2 Nummer 2 technisch nicht möglich oder nicht zumutbar ist, kann der Bundesnachrichtendienst stattdessen vom Verpflichteten die Auskunft durch Herausgabe einer Kopie der Teile des informationstechnischen Systems verlangen, deren Auswertung zum Aufspüren der in Absatz 1 Satz 2 Nummer 2 bezeichneten Informationen erforderlich ist.

(3) Der Bundesnachrichtendienst prüft die erhobenen Daten unverzüglich darauf, ob sie für die Aufklärung des Angriffs erforderlich sind und löscht nicht erforderliche Daten unverzüglich. Bei Kopien nach Absatz 2 prüft der Bundesnachrichtendienst unverzüglich, ob neben den in Absatz 1 Satz 2 Nummer 2 bezeichneten Informationen noch weitere Daten erhoben worden sind, und löscht diese weiteren Daten unverzüglich.

(4) Stellt der Bundesnachrichtendienst bei Maßnahmen nach Absatz 1 Angriffswerkzeuge oder Daten, die der Angreifer durch den Angriff beschafft hat, fest, so darf der nach Absatz 1 Verpflichtete diese nach Herstellung einer Sicherungskopie löschen. Eine vom Verpflichteten hergestellte Sicherungskopie von Daten, die der Angreifer durch den Angriff beschafft hat, ist dem Bundesnachrichtendienst herauszugeben.

§ 15

Ersuchen gegenüber privaten Einrichtungen der Videoüberwachung

(1) Der Bundesnachrichtendienst darf Verfügungsberechtigte privater Einrichtungen der Videoüberwachung des öffentlich zugänglichen Raums ersuchen,

1. eine Mitbenutzung der Einrichtung durch den Bundesnachrichtendienst zu ermöglichen und dem Bundesnachrichtendienst zu diesem Zweck den Zutritt zu den Räumlichkeiten der Einrichtung zu gewähren,

2. gespeicherte Bild- und Tonaufzeichnungen aus Videoüberwachungen an den Bundesnachrichtendienst zu übermitteln sowie

3. Daten der Videoüberwachung in Echtzeit an den Bundesnachrichtendienst auszuleiten.

(2) Ein Ersuchen nach Absatz 1 ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen. Überlassene Bild- und Tonaufzeichnungen sind unverzüglich zurückzugeben, zu löschen oder zu vernichten, soweit die Voraussetzungen in Satz 1 nicht mehr vorliegen oder die Daten zur Aufgabenerfüllung nicht mehr erforderlich sind.

(3) Führt das Ersuchen zu einer dem § 27 Absatz 1 Nummer 2 in Verbindung mit Absatz 2 Nummer 2 vergleichbaren längerfristigen optischen und akustischen Überwachung einer Person, so gelten abweichend von Absatz 2 Satz 1 die in § 27 Absatz 2 Nummer 2 genannten Voraussetzungen.

§ 16

Pflichten bei Ersuchen an nicht öffentliche Stellen

(1) Zur Auskunft nach § 12 Absatz 1, § 13 Absatz 1 und 3, § 14 Absatz 1 und 2 sowie zur Auskunft und Mitwirkung nach § 13 Absatz 4 und 5 ist verpflichtet, wer in Deutschland

1. eine Niederlassung hat oder

2. den Dienst oder die Leistung erbringt oder an der Erbringung mitwirkt.

(2) Zur Mitwirkung oder Übermittlung nach § 15 ist verpflichtet, wer in Deutschland eine Videoüberwachung des öffentlich zugänglichen Raums betreibt. Bei einem Auskunftsersuchen nach § 15 Absatz 1 Nummer 3 beschränkt sich die Verpflichtung auf den Einsatz der bei dem Verpflichteten vorhandenen technischen Mittel.

(3) Der Bundesnachrichtendienst teilt den nach den Absätzen 1 und 2 verpflichteten Stellen das Ersuchen schriftlich mit, soweit dies erforderlich ist, um dem Verpflichteten die Erfüllung seiner Verpflichtung zu ermöglichen. In Ersuchen sind die Informationen einschließlich der personenbezogenen Daten, zu denen Auskunft ersucht wird, anzugeben. Die Stellen nach den Absätzen 1 und 2 haben dem Ersuchen unverzüglich und vollständig zu entsprechen.

(4) Die in den Absätzen 1 und 2 genannten Stellen erhalten für die Erfüllung ihrer Verpflichtungen eine Entschädigung, deren Umfang sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes bemisst. Der Bundesnachrichtendienst kann mit den Verpflichteten besondere Entschädigungsvereinbarungen treffen, deren Höhe sich an den nachgewiesenen tatsächlichen Kosten orientiert, falls die Höhe der Entschädigung nach Satz 1 nichtangemessen ist. Die Vorschriften der Verjährung in § 2 Absatz 1 und Absatz 4 des Justizvergütungs- und Entschädigungsgesetzes finden entsprechende Anwendung.

§ 17

Anordnungen

(1) Auskunftsersuchen nach § 13 Absatz 1 Satz 2, die sich gegen eine der in § 12 Absatz 2 Nummer 4 und 5 genannten Stellen richten, sowie nach § 14 Absatz 2 bedürfen der Anordnung durch die Behördenleitung des Bundesnachrichtendienstes oder einer von ihr bestimmten Vertretung. Dies gilt nicht, wenn es sich um Auskunftsersuchen nach § 13 Absatz 4 oder 5 handelt, die der Durchführung von Maßnahmen dienen, die bereits von der Behördenleitung des Bundesnachrichtendienst oder einer von ihr bestimmten Vertretung angeordnet wurden.

(2) In der Anordnung sind anzugeben:

1. das Aufklärungsthema, im Falle eines Auskunftsersuchens zu einer Person die Person, soweit möglich mit Namen und Anschrift,

2. Art, Umfang und Dauer des Auskunftsersuchens,

3. die Befristung der Anordnung nach Absatz 3 und

4. eine Begründung.

(3) Eine Anordnung zur Auskunft über zukünftig anfallende Daten ist auf höchstens zwölf Monate zu befristen. Verlängerungen der Anordnung sind zulässig, sofern die Voraussetzungen fortbestehen.

(4) Die Anordnung eines Auskunftsverlangens nach Absatz 1 kann den Zusatz enthalten, dass sich das Auskunftsverlangen auch auf andere als die in der Anordnung genannten Personen beziehen kann, wenn tatsächliche Anhaltspunkte dafür vorliegen,

1. dass bei dem in der Anordnung bestimmten Aufklärungsziel mit weiteren Beteiligten zu rechnen ist, und

2. die Voraussetzungen des jeweiligen Auskunftsverlangens auch in Bezug auf die nicht in der Anordnung genannten Personen vorliegen werden.

(5) Die Anordnung nach Absatz 1 sowie deren Verlängerungen sind durch den Bundesnachrichtendienst zu dokumentieren.

Abschnitt 3

Einsatz nachrichtendienstlicher Mittel

Unterabschnitt 1

Allgemeine Befugnis und Vorgaben für den Einsatz nachrichtendienstlicher Mittel

§ 18

Einsatz nachrichtendienstlicher Mittel

(1) Der Bundesnachrichtendienst darf zur heimlichen Beschaffung von Informationen einschließlich personenbezogener Daten Methoden, Gegenstände und Instrumente (nachrichtendienstliche Mittel) einsetzen, wenn

1. tatsächliche Anhaltspunkte dafür vorliegen, dass der Einsatz eines bestimmten nachrichtendienstlichen Mittels im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist,

2. das Bundeskanzleramt den Bundesnachrichtendienst zur Aufklärung beauftragt hat, und

3. die in den Unterabschnitten 2 und 3 enthaltenen Befugnisse für den Einsatz bestimmter nachrichtendienstlicher Mittel keine abweichenden Regelungen treffen.

Zu den nachrichtendienstlichen Mitteln zählen insbesondere der Einsatz nachrichtendienstlicher Verbindungen oder technischer Mittel sowie die Inbesitznahme von Sachen zu deren Auswertung. Eine durch den Bundesnachrichtendienst in Besitz genommene Sache ist dem Eigentümer oder dem rechtmäßigen Inhaber der tatsächlichen Gewalt nach Abschluss der heimlichen Auswertung zurückzugeben, wenn keine überwiegenden Sicherheitsinteressen einer Rückgabe entgegenstehen. Handelt es sich bei der in Besitz genommenen Sache um einen informationstechnischen Speicher, so richtet sich die Auswertung nach § 54.

(2) Unter den Voraussetzungen des Einsatzes eines nachrichtendienstlichen Mittels darf der Bundesnachrichtendienst zu dessen Vorbereitung und Durchführung Gebäude und Räume, die keine Wohnungen sind, auch ohne Wissen des Inhabers betreten. Eine Wohnung darf der Bundesnachrichtendienst zur Vorbereitung und Durchführung eines nachrichtendienstlichen Mittels nur betreten, wenn tatsächliche Anhaltspunkten dafür bestehen, dass dies im Einzelfall erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen. Im Falle einer im Bundesgebiet befindlichen Wohnung gilt dies nur

1. bei einer konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut und

2. auf Grund einer besonderen Anordnung durch die Behördenleitung des Bundesnachrichtendienstes oder einer von ihr bestimmten Vertretung.

Eine technische Datenerhebung aus Wohnungen ist nur nach § 29 oder § 113 zulässig.

(3) Eine konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut ist ein Sachverhalt, bei dem sich der zum Schaden führende Kausalverlauf zwar noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, aber bereits tatsächliche Anhaltspunkte im Einzelfall auf die Entstehung einer konkreten Gefahr für ein besonders gewichtiges Rechtsgut hinweisen.

§ 19

Besonderer Einsatz nachrichtendienstlicher Mittel

(1) Ist der Einsatz eines nachrichtendienstlichen Mittels zur Erhebung personenbezogener Daten, welches nicht in der Dienstvorschrift nach § 95 Absatz 1 enthalten ist, seiner Art nach insbesondere unter Berücksichtigung der Ausnutzung dauerhafter persönlicher Vertrauensbeziehungen, einer weitgehenden Erfassung der Persönlichkeit oder des Anfallens höchstprivater Informationen vergleichbar gewichtig wie die in den Unterabschnitten 2 und 3 enthaltenen Befugnisse für den Einsatz eingriffsintensiver nachrichtendienstlicher Mittel, so darf er nur zur Erprobung erfolgen. Die erlangten personenbezogenen Daten dürfen nur weiterverarbeitet werden zur Aufklärung

1. einer zumindest konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut oder

2. einer Bedrohung von herausgehobener Bedeutung.

Eine Erprobung ist höchstens vier Jahre zulässig und kann darüber hinaus nicht verlängert werden.

(2) Wird ein nachrichtendienstliches Mittel nach § 18 Absatz 1 ausnahmsweise so eingesetzt, dass es unter Berücksichtigung der Ausnutzung dauerhafter persönlicher Vertrauensbeziehungen, einer weitgehenden Erfassung der Persönlichkeit oder des Anfallens höchstprivater Informationen vergleichbar gewichtig ist wie die in Unterabschnitt 2 und 3 genannten Befugnisse, deren Eingriffsgewicht tatsächliche Anhaltspunkte für eine

1. erhebliche Bedrohung voraussetzen, so darf es nur eingesetzt werden, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme im Einzelfall erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen, oder

2. Bedrohung von herausgehobener Bedeutung voraussetzen, so darf es nur eingesetzt werden, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme im Einzelfall erforderlich ist, um Informationen zu Bedrohungen von herausgehobener Bedeutung zu erlangen.

§ 20

Einsatz nachrichtendienstlicher Mittel gegen eine Person

(1) Der Einsatz von nachrichtendienstlichen Mitteln zur Erhebung von personenbezogenen Daten ist gegen eine Person gerichtet, wenn er mit dem Ziel einer systematischen Sammlung von Informationen zu dieser Person erfolgt.

(2) Der Einsatz nachrichtendienstlicher Mittel nach § 18 Absatz 1 und Unterabschnitt 2 darf sich nur gegen eine Person richten, wenn tatsächliche Anhaltspunkte vorliegen, dass diese Person in einem Zusammenhang mit dem Aufklärungsziel steht, der Grund zu der Annahme gibt, dass durch die Maßnahme Erkenntnisse über das Aufklärungsziel gewonnen werden können. Der Einsatz nachrichtendienstlicher Mittel zur Erhebung von personenbezogenen Daten gegen eine andere Person ist nur zulässig, soweit die Erkenntnisse durch eine Inanspruchnahme von Personen nach Satz 1 nicht erlangt werden kann.

(3) Abweichend von Absatz 2 darf sich der Einsatz nachrichtendienstlicher Mittel nach Unterabschnitt 2, deren Eingriffsgewicht das Vorliegen einer zumindest erheblichen Bedrohung voraussetzt, gegen deutsche Staatsangehörige oder sich im Bundesgebiet

aufhaltende Personen nur dann richten, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass sie

1. für eine erhebliche Bedrohung verantwortlich sind oder diese unterstützen,

2. Mitglieder eines abgrenzbaren Netzwerks sind, sofern zugleich tatsächliche Anhaltspunkte dafür vorliegen, dass das Netzwerk für die zumindest erhebliche Bedrohung verantwortlich ist oder von seinen Mitgliedern ausschließlich oder ganz überwiegend dazu genutzt wird, die zumindest erhebliche Bedrohung zu unterstützen, oder

3. in Zusammenhang mit einer zumindest erheblichen Bedrohung stehen, der Grund zu der Annahme gibt, dass durch die Maßnahme Erkenntnisse über die zumindest erhebliche Bedrohung gewonnen werden können, die nicht gleichermaßen durch eine Maßnahme gegen eine Person nach Nummer 1 zu gewinnen sind, insbesondere dass diese Personen für eine Person nach Nummer 1 bestimmte oder von ihr herrührende Mitteilungen entgegennehmen oder weitergeben.

(4) Die Absätze 2 und 3 finden keine Anwendung, bei der Prüfung von Personen in Bezug auf ihren Einsatz als nachrichtendienstliche Verbindungen nach § 23.

§ 21

Schutz des Kernbereichs privater Lebensgestaltung

(1) Der Einsatz nachrichtendienstlicher Mittel zur Erlangung von kernbereichsrelevanten Informationen ist unzulässig. Der Einsatz ist auch dann unzulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass durch den Einsatz allein kernbereichsrelevante Informationen gewonnen werden würden. Bei der Planung des Einsatzes nachrichtendienstlicher Mittel zur Erhebung von personenbezogenen Daten ist darauf hinzuwirken, dass die Erlangung kernbereichsrelevanter Informationen vermieden wird.

(2) Erlangt der Bundesnachrichtendienst durch den Einsatz nachrichtendienstlicher Mittel kernbereichsrelevante Informationen, so sind die entsprechenden Daten unverzüglich zu löschen. Die Löschung ist zu protokollieren. Bestehen Zweifel, ob durch den Einsatz eines nachrichtendienstlichen Mittels kernbereichsrelevante Informationen erlangt worden sind, entscheidet hierüber ein Bediensteter des behördlichen Datenschutzes mit der Befähigung zum Richteramt. Die Daten sind ihm in Fällen des Satzes 3 unverzüglich vorzulegen. Die Daten, bei denen Zweifel an der Kernbereichsrelevanz bestehen, dürfen nur mit der Zustimmung des behördlichen Datenschutzes genutzt werden.

(3) Der Einsatz eines nachrichtendienstlichen Mittels ist zu unterbrechen, wenn für den Bundesnachrichtendienst erkennbar wird, dass durch ihn nicht nur am Rande kernbereichsrelevante Informationen erlangt werden. Wird das nachrichtendienstliche Mittel in einer Weise eingesetzt, dass bei einer Unterbrechung eine Gefährdung von Leib, Leben oder Freiheit einer Person oder der weiteren Einsetzbarkeit des nachrichtendienstlichen Mittels droht, so hat eine Unterbrechung erst dann zu erfolgen, sobald dies ohne Gefährdung möglich ist. Ist für den Bundesnachrichtendienst zu erwarten, dass bei einer Fortsetzung eines unterbrochenen Einsatzes nicht nur am Rande kernbereichsrelevante Informationen erhoben werden, so hat er diesen Einsatz abzubrechen. Beim Einsatz technischer Mittel, die eine Aufzeichnung ermöglichen, darf die Fortsetzung nur durch Anfertigung einer Aufzeichnung erfolgen. Auf die in den Satz 4 genannten Daten findet Absatz 2 Satz 3 bis 5 Anwendung. Die Unterbrechung und die Fortsetzung des Einsatzes des nachrichtendienstlichen Mittels sind unter Angabe der Gründe zu dokumentieren.

(4) Beim Einsatz einer nachrichtendienstlichen Verbindung oder bei der Nutzung einer Legende nach § 25 darf keine intime Beziehung oder vergleichbar engste persönliche Bindung gezielt zum Zweck der Informationsgewinnung begründet oder fortgeführt werden.

(5) Im Rahmen der Durchführung der technischen Aufklärung nach Unterabschnitt 3 hat der Bundesnachrichtendienst, soweit ihm technisch möglich, sicherzustellen, dass kernbereichsrelevante Informationen nicht erhoben werden. Personenbezogene Daten, die durch Maßnahmen nach § 37 Absatz 2 oder 3 oder § 38 erlangt wurden und bei denen tatsächliche Anhaltspunkte dafür bestehen, dass sie den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen oder dem Unabhängigen Kontrollrat zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Tatsächliche Anhaltspunkte im Sinne des Satzes 2 liegen insbesondere dann vor, wenn Daten in einem unmittelbaren Zusammenhang mit solchen Daten stehen, die als kernbereichsrelevant identifiziert wurden.

§ 22

Schutz von Vertraulichkeitsbeziehungen

(1) Die Erhebung von personenbezogenen Daten zum Zweck der gezielten Erlangung von Daten aus einer Vertraulichkeitsbeziehung ist unzulässig. Daten entstammen einer Vertraulichkeitsbeziehung, wenn

1. sie Geistlichen in ihrer Eigenschaft als Seelsorger oder anderen Personen, die als Seelsorger tätig sind, in dieser Eigenschaft anvertraut worden oder bekanntgeworden sind,

2. sie Rechtsanwältinnen oder Rechtsanwälten sowie Verteidigerinnen oder Verteidigern in dieser Eigenschaft anvertraut worden oder bekanntgeworden sind,

3. sie Journalistinnen oder Journalisten in dieser Eigenschaft anvertraut worden oder bekanntgeworden sind oder

4. sie Mitgliedern des Deutschen Bundestages, der Bundesversammlung, des Europäischen Parlaments aus der Bundesrepublik Deutschland oder eines Landtages in ihrer Eigenschaft als Mitglieder dieser Organe anvertraut worden sind oder die vorgenannten Personen die Daten in ihrer Eigenschaft als Mitglieder dieser Organe anderen Personen anvertraut haben.

Daten entstammen auch dann einer Vertraulichkeitsbeziehung, wenn sie einer Person anvertraut oder bekannt geworden sind, die an einer Tätigkeit der in Absatz 1 Satz 2 genannten Berufsgruppen im Rahmen eines Vertragsverhältnisses einschließlich der gemeinschaftlichen Berufsausübung, einer berufsvorbereitenden Tätigkeit oder einer sonstigen Hilfstätigkeit mitwirken.

(2) Abweichend von Absatz 1 Satz 1 ist die Datenerhebung zulässig, wenn Tatsachen die Annahme rechtfertigen, dass

1. die in Absatz 1 Satz 2 und 3 genannten Personen

   a) für eine zumindest erhebliche Bedrohung verantwortlich sind oder diese unterstützen,

   b) Mitglieder eines abgrenzbaren Netzwerks sind, sofern zugleich tatsächliche Anhaltspunkte dafür vorliegen, dass das Netzwerk für eine zumindest erhebliche Bedrohung verantwortlich ist oder von seinen Mitgliedern ausschließlich oder ganz

überwiegend dazu genutzt wird, eine zumindest erhebliche Bedrohung zu unterstützen, oder

c) in Zusammenhang mit einer zumindest erheblichen Bedrohung stehen, der Grund zu der Annahme gibt, dass durch die Maßnahme Erkenntnisse über diese Bedrohung gewonnen werden können, die nicht gleichermaßen durch eine Maßnahme gegen eine Person nach Buchstaben a und b zu gewinnen sind; dies kann insbesondere der Fall sein, wenn diese Personen für eine Person nach Buchstaben a und b bestimmte oder von ihr herrührende Mitteilungen entgegennehmen oder weitergeben, oder

2. die Datenerhebung notwendig ist zur Abwendung einer erheblichen Gefahr für ein besonders gewichtiges Rechtsgut im Sinne des § 2 Absatz 2.

(3) Sofern die Weiterverarbeitung der bei einer in Absatz 1 Satz 2 und 3 genannten Person erhobenen personenbezogenen Daten ergibt, dass diese aus einer Vertraulichkeitsbeziehung stammen, dürfen die Daten nur weiterverarbeitet oder übermittelt werden, wenn die Voraussetzungen des Absatzes 2 vorliegen. Anderenfalls sind die Daten unverzüglich zu löschen. § 21 Absatz 2 findet entsprechende Anwendung.

(4) Die Entscheidung über die Zugehörigkeit einer Person zu dem in Absatz 1 Satz 2 und 3 genannten Personenkreis ist zu dokumentieren.

§ 23

Vorgaben für den Einsatz nachrichtendienstlicher Verbindungen

(1) Der Bundesnachrichtendienst arbeitet zur Aufgabenerfüllung mit Personen zusammen, die nicht Bedienstete des Bundesnachrichtendienstes sind und deren Zusammenarbeit mit dem Bundesnachrichtendienst Dritten verborgen bleiben soll (nachrichtendienstliche Verbindungen).

(2) Als nachrichtendienstliche Verbindungen dürfen deutsche Staatsangehörige oder sich im Bundesgebiet aufhaltende Personen nicht geführt werden, wenn sie

1. nicht voll geschäftsfähig, insbesondere minderjährig sind,

2. von den Geld- oder Sachzuwendungen für die Tätigkeit als nachrichtendienstliche Verbindung auf Dauer als alleinige Lebensgrundlage abhängen würden,

3. an einem Aussteigerprogramm teilnehmen

4. Mitglied des Europäischen Parlaments aus der Bundesrepublik Deutschland, Mitglied des Deutschen Bundestages, eines Landesparlaments der Bundesrepublik Deutschland oder Bedienstete eines solchen Mitglieds sind oder

5. im Bundeszentralregister mit einer Verurteilung wegen eines Verbrechens oder zu einer Freiheitsstrafe, deren Vollstreckung nicht zur Bewährung ausgesetzt worden ist, eingetragen sind.

(3) Wenn die Aufgabenerfüllung des Bundesnachrichtendienstes auf andere Weise aussichtslos oder wesentlich erschwert wäre, können durch die Behördenleitung oder einer von ihr bestimmten Vertretung folgende Ausnahmen angeordnet werden

1. von Absatz 2 Nummer 1 bei Personen, die mindestens 16 Jahre alt sind, wenn bei der Führung der jugendlichen Person Belange der Fürsorge besonders berücksichtigt werden,

2. von Absatz 2 Nummer 2 bis 4 sowie

3. von Absatz 2 Nummer 5 unter der Voraussetzung, dass die Verurteilung nicht als Täter eines Totschlags (§§ 212, 213 des Strafgesetzbuchs) oder einer allein mit lebenslanger Haft bedrohten Straftat erfolgt ist.

Im Falle einer Ausnahme nach Satz 1 Nummer 2 oder 3 ist die Maßnahme nach höchstens sechs Monaten zu beenden, wenn durch die Maßnahme keine Informationen zu zumindest erheblichen Bedrohungen erlangt wurden.

(4) Nachrichtendienstliche Verbindungen dürfen weder zur Gründung von Vereinigungen im Sinne der §§ 129, 129a und 129b des Strafgesetzbuchs noch zur steuernden Einflussnahme auf diese eingesetzt werden. Im Übrigen ist die Tätigkeit einer nachrichtendienstlichen Verbindung nicht rechtswidrig, wenn die Tätigkeit

1. nicht in Individualrechte eingreift,

2. zur Gewinnung und Sicherung der Information oder Informationszugänge unumgänglich ist und

3. nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts steht.

Erfolgt die Tätigkeit einer nachrichtendienstlichen Verbindung im Ausland, so gilt Satz 2 mit der Maßgabe, dass die Tätigkeit abweichend von Satz 2 Nummer 1 nicht in Leib, Leben, Freiheit oder die sexuelle Selbstbestimmung einer Person eingreifen darf. Sofern zureichende Anhaltspunkte dafür bestehen, dass eine nachrichtendienstliche Verbindung bei ihrem Einsatz rechtswidrig einen Straftatbestand von erheblicher Bedeutung verwirklicht hat, soll der Einsatz unverzüglich beendet und die Strafverfolgungsbehörde unterrichtet werden.

(5) Hat ein Strafverfahren ein Vergehen zum Gegenstand, das eine nachrichtendienstliche Verbindung im Einsatz begangen haben soll, so kann die Staatsanwaltschaft von der Verfolgung absehen, wenn

1. die Maßnahme zur nachrichtendienstlichen Auslandsaufklärung erfolgte und

2. die Tat zur Gewinnung und Sicherung der Information oder Informationszugänge unumgänglich war.

Dabei ist das Verhältnis der Bedeutung der Aufklärung des Sachverhalts zur Schwere der begangenen Straftat und der Schuld des Täters zu berücksichtigen. Ein Absehen von der Verfolgung ist ausgeschlossen, wenn eine höhere Strafe als eine Freiheitsstrafe von einem Jahr zu erwarten ist. Ein Absehen von der Verfolgung ist darüber hinaus stets ausgeschlossen, wenn zu erwarten ist, dass die Strafe nicht zur Bewährung ausgesetzt werden würde. Bei Vergehen, die mit einer im Mindestmaß erhöhten Strafe bedroht sind und bei denen die durch die Tat verursachten Folgen nicht gering sind, bedarf die Einstellung des Verfahrens der Zustimmung des für die Eröffnung des Hauptverfahrens zuständigen Gerichts. Ist die Klage bereits erhoben, so kann das Gericht in jeder Lage des Verfahrens unter den Voraussetzungen des Satz 1 mit Zustimmung der Staatsanwaltschaft und des Angeschuldigten das Verfahren einstellen.

(6) Beim Einsatz einer nachrichtendienstlichen Verbindung hat der Bundesnachrichtendienst darauf hinzuwirken, dass die nachrichtendienstliche Verbindung keine kernbereichsrelevanten Informationen erhebt und weitergibt. Der Bundesnachrichtendienst muss

vor der Weiterverarbeitung der Informationen, die die nachrichtendienstliche Verbindung weitergibt, prüfen, ob diese kernbereichsrelevante Informationen enthalten. Wird dem Bundesnachrichtendienst bekannt, dass die nachrichtendienstliche Verbindung kernbereichsrelevante Informationen gewonnen hat, hat es diesen Umstand auch unabhängig von der Weitergabe von Inhalten zu dokumentieren.

(7) Bei der Verpflichtung von nachrichtendienstlichen Verbindungen ist § 1 Absatz 3 des Verpflichtungsgesetzes mit der Maßgabe anzuwenden, dass auch von der Unterzeichnung der Niederschrift durch die verpflichtete Person abgesehen werden kann, wenn dies im Interesse der inneren oder äußeren Sicherheit der Bundesrepublik Deutschland geboten ist.

Unterabschnitt 2

Besondere Befugnisse zum Einsatz nachrichtendienstlicher Mittel

§ 24

Einsatz nachrichtendienstlicher Verbindungen gegen eine Person

(1) Der Einsatz einer nachrichtendienstlichen Verbindung gegen eine Person ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme im Einzelfall

1. zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist, falls der Einsatz länger als sechs Monate andauert oder

2. erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen, falls der Einsatz gegen eine Person gerichtet ist, zu der die nachrichtendienstliche Verbindung eine besondere persönliche Vertrauensbeziehung unterhält.

(2) Der Einsatz einer nachrichtendienstlichen Verbindung gegen deutsche Staatsangehörige oder sich im Bundesgebiet aufhaltende Personen ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme im Einzelfall erforderlich ist,

1. um Informationen zu zumindest erheblichen Bedrohungen zu erlangen, falls der Einsatz länger als sechs Monate andauert oder

2. um Informationen zu Bedrohungen von herausgehobener Bedeutung zu erlangen, falls der Einsatz gegen eine Person gerichtet ist, zu der die nachrichtendienstliche Verbindung eine besondere persönliche Vertrauensbeziehung unterhält.

§ 25

Nutzung einer Legende auf vertiefter Vertrauensbasis

(1) Der Bundesnachrichtendienst darf eine Legende einsetzen, um zum Zweck der Informationsgewinnung eine vertiefte Vertrauensbasis zu einer Person auszunutzen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist.

(2) Der Einsatz einer Legende zum Zweck der Informationsgewinnung nach Absatz 1 gegen deutsche Staatsangehörige oder sich im Bundesgebiet aufhaltende Personen ist nur

zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme im Einzelfall erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen.

§ 26

Einsatz technischer Mittel zur längerfristigen Standortfeststellung

(1) Der Bundesnachrichtendienst darf technische Mittel zur längerfristigen Standortfeststellung einer Person einsetzen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme

1. im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist, falls die Maßnahme erfolgt

   a) über einen Zeitraum von

      aa) sieben Tagen oder länger im durchgehenden Einsatz,

      bb) an 14 oder mehr einzelnen Tagen innerhalb des Zeitraums von 30 Tagen im täglich durchgehenden Einsatz oder

   b) in einer Weise, die ein dem Buchstabe a Doppelbuchstabe aa oder bb in der Persönlichkeitsrelevanz gleichwertiges Bewegungsprofil ergibt, oder

2. im Einzelfall erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen, falls die Maßnahme erfolgt

   a) über einen Zeitraum von

      aa) 30 Tagen oder länger im durchgehenden Einsatz,

      bb) an fünf oder mehr Wochen innerhalb eines Zeitraums von 60 Tagen im wöchentlich durchgehenden Einsatz oder

   b) in einer Weise, die ein dem Buchstabe a Doppelbuchstabe aa oder bb in der Persönlichkeitsrelevanz gleichwertiges Bewegungsprofil ergibt.

(2) Gegen deutsche Staatsangehörige oder sich im Bundesgebiet aufhaltende Personen ist eine Maßnahme nach Absatz 1 nur zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme im Einzelfall erforderlich ist, um Informationen

1. zu zumindest erheblichen Bedrohungen zu erlangen, falls es sich um eine Maßnahme nach Absatz 1 Nummer 1 handelt, oder

2. zu Bedrohungen von herausgehobener Bedeutung zu erlangen, falls es sich um eine Maßnahme nach Absatz 1 Nummer 2 handelt.

(3) Ein Einsatz technischer Mittel zur längerfristigen Standortfeststellung ist durchgehend, wenn er ermöglicht, die Bewegung der Person über den Zeitraum zusammenhängend zu überwachen.

(4) Eine Maßnahme der Standortfeststellung ist, wenn sie mit einem der in Unterabschnitt 3 genannten nachrichtendienstlichen Mittel erfolgt, nur nach Maßgabe der dort genannten Befugnisse zulässig.

§ 27

Längerfristige optische und akustische Überwachung

(1) Der Bundesnachrichtendienst darf längerfristige optische und akustische Überwachungen gegen Personen, auch unter Einsatz observationsunterstützender technischer Mittel, durchführen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme

1. im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist, falls die Maßnahme erfolgt

   a) durchgehend 48 Stunden oder länger oder

   b) an sieben oder mehr Tagen innerhalb eines Zeitraums von 30 Tagen oder

2. im Einzelfall erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen, falls die Maßnahme über einen Zeitraum von durchgehend sieben Tagen oder länger erfolgt.

(2) Gegen deutsche Staatsangehörige oder sich im Bundesgebiet aufhaltende Personen ist eine Maßnahme nach Absatz 1 nur zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme im Einzelfall erforderlich ist, um Informationen

1. zu zumindest erheblichen Bedrohungen zu erlangen, falls es sich um eine Maßnahme nach Absatz 1 Nummer 1 handelt, oder

2. zu Bedrohungen von herausgehobener Bedeutung zu erlangen, falls es sich um eine Maßnahme nach Absatz 1 Nummer 2 handelt.

(3) Der Bundesnachrichtendienst darf mit technischen Mitteln zur optischen und akustischen Überwachung das Verhalten von Personen im nichtöffentlichen Raum aufzeichnen, wenn im Einzelfall tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme

1. zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist,

2. erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen, falls die Maßnahme auf die Überwachung von deutschen Staatsangehörigen oder sich im Bundesgebiet aufhaltenden Personen zielt.

Ist bei der Aufzeichnung mit der Erfassung von höchstprivaten Informationen zu rechnen, so ist die Maßnahme abweichend von Satz 1 nur zulässig, wenn im Einzelfall tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen oder, falls die Maßnahme auf die Überwachung von deutschen Staatsangehörigen oder sich im Bundesgebiet aufhaltenden Personen zielt, zu Bedrohungen von herausgehobener Bedeutung zu erlangen.

(4) Die Anforderungen des Absatz 2 und des Absatz 3 Satz 1 Nummer 2 gelten nicht für Maßnahmen zum Schutz eingesetzter Personen oder bei der Prüfung von Personen in Bezug auf ihren Einsatz als nachrichtendienstliche Verbindungen nach § 23.

(5) Eine technische Datenerhebung aus Wohnungen ist nur nach § 29 oder § 113 zulässig.

§ 28

Maßnahmen bei Post- und Warensendungen

(1) Der Bundesnachrichtendienst darf die dem Brief- oder Postgeheimnis unterliegenden Sendungen überwachen, insbesondere Sendungen öffnen und einsehen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme im Einzelfall erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen. Ist die Überwachung auf die Erlangung von Informationen zu Umständen der Verkehre beschränkt, ist sie auch zulässig, wenn tatsächliche Anhaltspunkte vorliegen, dass die Maßnahme im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist.

(2) Der Bundesnachrichtendienst darf die dem Brief- oder Postgeheimnis unterliegenden Sendungen von deutschen Staatsangehörigen, inländischen juristischen Personen sowie sich im Bundesgebiet aufhaltenden Personen oder an diese Personen nur öffnen und einsehen, wenn

1. tatsächliche Anhaltspunkte vorliegen, dass die Maßnahme im Einzelfall erforderlich ist, um Informationen zu Bedrohungen von herausgehobener Bedeutung zu erlangen und

2. die Erlangung der Informationen auf andere Weise, mit Ausnahme von Maßnahmen nach § 29 und § 37 Absatz 3, aussichtslos oder wesentlich erschwert wäre.

Ist die Maßnahme auf die Erlangung von Informationen zu Umständen der Verkehre einer der in Satz 1 genannten Personen beschränkt, ist sie zulässig, wenn tatsächliche Anhaltspunkte vorliegen, dass die Maßnahme im Einzelfall erforderlich ist, um Informationen zu erheblichen Bedrohungen zu erlangen. Abgeordnetenpost von Mitgliedern des Deutschen Bundestages und der Parlamente der Länder sowie von Mitgliedern der Bundesversammlung und des Europäischen Parlaments aus der Bundesrepublik Deutschland darf nicht in eine Maßnahme einbezogen werden, die sich gegen einen Dritten richtet.

(3) Der Bundesnachrichtendienst darf zur Informationsgewinnung unter den Voraussetzungen der Absätze 1 bis 2 Sendungen, die dem Brief- oder Postgeheimnis unterliegen, bearbeiten, insbesondere der Sendung andere Gegenstände hinzufügen oder in der Sendung enthaltene Gegenstände manipulieren. Eine über die Informationsgewinnung hinausgehende Veränderung des Inhalts einer Sendung, die dem Brief- oder Postgeheimnis unterliegt, ist nur zulässig, wenn

1. Tatsachen vorliegen, die die Annahme rechtfertigen, dass eine unmittelbar bevorstehende Gefahr für eines der in § 2 Absatz 2 oder in § 4 Absatz 1, auch in Verbindung mit Absatz 2 des Außenwirtschaftsgesetzes genannten Rechtsgüter besteht,

2. die Gefahr durch eine andere Behörde mit Ausnahme eines anderen Nachrichtendienstes mittels einer gleich geeigneten Maßnahme nicht oder nicht rechtzeitig abgewehrt werden kann und

3. die Maßnahme in einer solchen Art und Weise durchgeführt wird, dass die für die betroffene Person zu erwartenden Nachteile in einem angemessenen Verhältnis zu dem Ziel der Maßnahme stehen.

(4) Auf die mittels einer Maßnahme nach Absatz 2 erhobenen Daten finden die § 64 Absatz 2 Satz 1 Nummer 1, § 65 Absatz 2, § 66 Absatz 3 und § 67 entsprechende Anwendung.

§ 29

Wohnraumüberwachung

(1) Der Bundesnachrichtendienst darf mit technischen Mitteln personenbezogene Daten aus einer Wohnung erheben, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme im Einzelfall erforderlich ist, um Informationen zu Bedrohungen von herausgehobener Bedeutung zu erlangen.

(2) Bei im Bundesgebiet liegenden Wohnungen und Wohnungen von deutschen Staatsangehörigen im Ausland ist eine Maßnahme nach Absatz 1 nur zulässig, wenn

1. dies im Einzelfall zur Abwehr einer dringenden Gefahr für besonders gewichtige Rechtsgüter erforderlich ist,

2. die Erforschung des Sachverhalts durch den Bundesnachrichtendienst mit anderen Mitteln aussichtslos oder wesentlich erschwert wäre,

3. geeignete polizeiliche Hilfe für das bedrohte Rechtsgut ansonsten nicht rechtzeitig erlangt werden kann und

4. auf Grund tatsächlicher Anhaltspunkte, insbesondere zu der Art der zu überwachenden Wohnräume und dem Verhältnis der zu überwachenden Personen untereinander, anzunehmen ist, dass durch die Überwachung kernbereichsrelevante Informationen nicht oder nur am Rande erfasst werden.

(3) Die Maßnahme nach Absatz 2 darf sich abweichend von § 20 nur gegen eine Person richten, zu der tatsächliche Anhaltspunkte dafür vorliegen, dass sie für die Gefahr verantwortlich ist. In die Überwachung einbezogen werden dürfen nur

1. die Wohnung dieser Person,

2. eine andere Wohnung, wenn hinreichende tatsächliche Anhaltspunkte dafür vorliegen, dass diese Person sich dort zur Zeit der Maßnahme aufhält und die Maßnahme Erkenntnisse zur Gefahrenabwehr erbringen wird, die nicht nach Nummer 1 zu gewinnen sind.

(4) Aufzeichnungen, die durch Maßnahmen nach Absatz 2 erhoben und nicht unmittelbar nach der Erhebung ohne inhaltliche Kenntnisnahme gelöscht worden sind, sind unverzüglich dem Unabhängigen Kontrollrat vorzulegen. Der Unabhängige Kontrollrat entscheidet über die Zulässigkeit der Weiterverarbeitung und Übermittlung. Die Weiterverarbeitung und Übermittlung ist zulässig, wenn die Erkenntnisse im Rahmen einer durch den Unabhängigen Kontrollrat als rechtmäßig festgestellten Anordnung erhoben worden sind und soweit keine Informationen aus dem Kernbereich privater Lebensgestaltung enthalten sind.

(5) Vor Feststellung der Rechtmäßigkeit der Maßnahme nach § 97 Absatz 6 Satz 1 sowie zur Zulässigkeit der Nutzung von Aufzeichnungen nach Absatz 4 darf der Bundesnachrichtendienst die nach Absatz 2 erhobenen Daten nur weiterverarbeiten, soweit dies bei Gefahr im Verzug zur Gefahrenabwehr nach Absatz 2 Nummer 1 unerlässlich ist.

(6) Der Bundesnachrichtendienst prüft unverzüglich nach der Erhebung und sodann regelmäßig in Abständen von höchstens zwei Jahren, ob die mit einer Maßnahme nach Absatz 2 erhobenen personenbezogenen Daten für die Abwehr einer dringenden Gefahr für besonders gewichtige Rechtsgüter erforderlich sind. Soweit die personenbezogenen Daten für diese Zwecke nicht mehr erforderlich sind, hat der Bundesnachrichtendienst sie unverzüglich zu löschen. Die Löschung ist zu protokollieren. Die Löschung der erhobenen personenbezogenen Daten unterbleibt, solange und soweit diese Daten für eine Mitteilung

nach § 100 oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Maßnahme von Bedeutung sein können. In diesem Fall ist die Verarbeitung der erhobenen personenbezogenen Daten einzuschränken; sie dürfen nur zu den genannten Zwecken verwendet werden.

(7) Die Daten aus einer Maßnahme der Wohnraumüberwachung nach Absatz 2 sind zu kennzeichnen. Die Behördenleitung oder eine von ihr bestimmte Vertretung kann anordnen, dass bei der Übermittlung auf die Kennzeichnung verzichtet wird, wenn dies unerlässlich ist, um die Geheimhaltung einer Maßnahme nicht zu gefährden, und der Unabhängige Kontrollrat zugestimmt hat. Bei Gefahr im Verzug kann die Übermittlung bereits vor der Zustimmung erfolgen. Wird die Zustimmung versagt, ist die Kennzeichnung durch den Übermittlungsempfänger unverzüglich nachzuholen. Der Empfänger gekennzeichneter Daten prüft unverzüglich, ob die Daten zu löschen sind. Er trifft angemessene organisatorische Vorkehrungen, dass künftig zu löschende Daten gelöscht werden. Der Bundesnachrichtendienst hat den Übermittlungsempfänger von diesen Pflichten zu unterrichten.

Unterabschnitt 3

Besondere Befugnisse der technischen Aufklärung

§ 30

Begriffsbestimmungen der technischen Aufklärung

Es bezeichnen die Begriffe:

1. „Eignungsprüfung“ die Prüfung der Eignung von Telekommunikationsnetzen oder die Bestimmung von geeigneten Suchbegriffen;

2. „Einsichtnahme“ die Abfrage und Bewertung von personenbezogenen Daten aus der strategischen Aufklärung, um diese für die inhaltliche Auswertung verfügbar zu machen;

3. „kommunikationsbezogene Inhaltsdaten“ die personenbezogenen Daten, die den Inhalt einer laufenden interpersonellen Kommunikation zwischen zwei oder mehr Teilnehmerinnen und Teilnehmern ausmachen;

4. „kommunikationsbezogene Metadaten“ die personenbezogenen Daten, die im Rahmen einer laufenden interpersonellen Kommunikation zwischen zwei oder mehr Teilnehmerinnen und Teilnehmern anfallen, ohne kommunikationsbezogene Inhaltsdaten der jeweiligen Übertragung zu sein;

5. „Kommunikationsdaten“ alle kommunikationsbezogenen Inhalts- und Metadaten;

6. „qualifizierter Inlandsbezug“ ein besonderer Bezug zum Inland, der daraus folgt, dass unter den Teilnehmerinnen und Teilnehmern der Kommunikation mindestens eine Person ist, bei der es sich handelt um:

   a) eine Person mit deutscher Staatsangehörigkeit, sofern es sich nicht um eine der in § 6 Absatz 3 genannten Personen handelt,

   b) eine inländische juristische Person, sofern es sich nicht um eine juristische Person handelt, bei der tatsächliche Anhaltspunkte dafür bestehen, dass sie von einer mit

nachrichtendienstlichen Aufgaben betrauten ausländischen öffentlichen Stelle gesteuert wird und in deren Interesse tätig ist, sowie

c) eine sich im Bundesgebiet aufhaltende Person ausländischer Staatsangehörigkeit, sofern

aa) es sich nicht um eine der in § 6 Absatz 3 genannten Personen handelt oder

bb) der Aufenthalt nicht auf den in § 6 Absatz 4 bestimmten Zeitraum begrenzt bleibt;

7. „reine Inlandskommunikation“ eine interpersonelle Kommunikation bei der sowohl bei Absender als auch bei Empfänger ein qualifizierter Inlandsbezug vorliegt,

8. „selektierte Kommunikationsdaten“ solche Kommunikationsdaten, die durch den Einsatz von Suchbegriffen im Wege der Einsichtnahme gefiltert wurden,

9. „strategische Aufklärung“ die Erhebung von personenbezogenen Daten, die in einem Telekommunikationsnetz übertragen werden;

10. „strategische Aufklärungsmaßnahmen“ die Maßnahmen, durch welche die strategische Aufklärung durchgeführt wird und welche die strategische Aufklärung hinsichtlich ihrer Erkenntnisziele und Dauer näher konkretisieren;

11. „Telekommunikationsnetz“ die Gesamtheit von Übertragungssystemen, ungeachtet dessen, ob sie auf einer permanenten Infrastruktur oder zentralen Verwaltungskapazität basieren, und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitigen Ressourcen, einschließlich der nicht aktiven Netzbestandteile, die die Übertragung von Signalen über Kabel, Funk, optische und andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetzen, festen, leitungs- und paketvermittelten Netzen, einschließlich des Internets, und mobilen Netzen, Stromleitungssystemen, soweit sie zur Signalübertragung genutzt werden, Netzen für Hör- und Fernsehfunk sowie Kabelfernsehnetzen, unabhängig von der Art der übertragenen Information;

12. „Telekommunikationsüberwachung“ die durch den Bundesnachrichtendienst veranlasste Ausleitung personenbezogener Daten anhand von Anschlusskennungen durch Anbieter von Telekommunikationsdiensten.

§ 31

Vorgaben für die strategische Aufklärung

(1) Die Durchführung der strategischen Aufklärung ist nur im Rahmen von strategischen Aufklärungsmaßnahmen zulässig.

(2) Der Bundesnachrichtendienst darf die durch die strategische Aufklärung erhobenen Kommunikationsdaten nur weiterverarbeiten und übermitteln, nachdem und soweit eine Einsichtnahme nach § 33 Absatz 1 und 2 oder § 34 Absatz 1 und 2 erfolgt ist. Dies gilt nicht

1. im Falle der Übermittlung an die Bundeswehr nach § 80 Absatz 2 und

2. im Falle einer Kooperation nach den §§ 43 bis 44, wenn danach eine vorherige Einsichtnahme entbehrlich ist.

Im Übrigen darf abweichend von Satz 1 der Bundesnachrichtendienst die durch die strategische Aufklärung erhobenen Kommunikationsdaten weiterverarbeiten, wenn dies ausschließlich zur Vorbereitung der späteren Einsichtnahme, insbesondere zur Erkennung von personenbezogenen Daten, welche nicht zur nachrichtendienstlichen Auslandsaufklärung erforderlich sind, geschieht.

(3) Eine unbeschränkte strategische Aufklärung ist unzulässig. Die strategische Aufklärung durch den Bundesnachrichtendienst ist auf das für die wirksame Auslandsaufklärung notwendige Maß zu begrenzen, insbesondere durch Beschränkung der Erhebung

1. auf diejenigen Bestandteile von Telekommunikationsnetzen oder, wenn anderenfalls der Zweck der Maßnahme gefährdet wäre, auf diejenigen Telekommunikationsnetze, bei denen tatsächliche Anhaltspunkte dafür bestehen, dass sie Daten enthalten, die für die nachrichtendienstliche Auslandsaufklärung in besonderem Maße erforderlich sind, und

2. auf nicht mehr als 15 Prozent des Datenvolumens, welches in allen Telekommunikationsnetzen übertragen werden kann.

Satz 2 Nummer 1 gilt nicht bei der Prüfung der Eignung von Telekommunikationsnetzen im Rahmen der Eignungsprüfung.

(4) Eine strategische Aufklärung zum Zweck der Erzielung von Wettbewerbsvorteilen ist unzulässig.

(5) Die strategische Aufklärung darf auch in der Weise erfolgen, dass die Erhebung durch ein technisches Mittel erfolgt, welches vom Bundesnachrichtendienst gemeinsam mit einer anderen öffentlichen Stelle betrieben wird. Erfolgt die Datenerhebung durch ein technisches Mittel auf dem Gebiet der Bundesrepublik Deutschland, so ist soweit technisch möglich sicherzustellen, dass eine Erhebung von Kommunikationsdaten mit qualifiziertem Inlandsbezug durch eine ausländische öffentliche Stelle nicht erfolgt.

(6) Stellt der Bundesnachrichtendienst während einer strategischen Aufklärungsmaßnahme fest, dass Tatsachen vorliegen, die die Annahme rechtfertigen, dass eine unmittelbar bevorstehende Gefahr für ein besonders gewichtiges Rechtsgut besteht, so darf der Bundesnachrichtendienst, um diese Gefahr abzuwehren,

1. Daten verändern oder löschen,

2. Datenverkehre, von denen die Gefahr ausgeht, unterbinden oder auf eine vom Bundesnachrichtendienst vorgegebene Zieladresse umleiten, und

3. in den Fällen des § 32 Absatz 2 den Betrieb informationstechnischer Systeme einschränken oder unterbinden.

Dies gilt nur, wenn die Gefahr durch eine andere Behörde mit Ausnahme eines anderen Nachrichtendienstes mittels einer gleich geeigneten Maßnahme nicht oder nicht rechtzeitig abgewehrt werden kann und die Maßnahme in einer solchen Art und Weise durchgeführt wird, dass die für die betroffene Person zu erwartenden Nachteile in einem angemessenen Verhältnis zu dem Ziel der Maßnahme stehen.

§ 32

Erhebung von Daten im Rahmen von strategischen Aufklärungsmaßnahmen

(1) Der Bundesnachrichtendienst darf im Rahmen von strategischen Aufklärungsmaßnahmen personenbezogene Daten erheben, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist.

(2) Eine strategische Aufklärungsmaßnahme darf auch in der Weise durchgeführt werden, dass sich der Bundesnachrichtendienst Zugang zu informationstechnischen Systemen eines Anbieters von Telekommunikationsdiensten oder von digitalen Diensten auch ohne dessen Wissen zur Durchführung der strategischen Aufklärung verschafft und personenbezogene Daten, die dieser Anbieter anlässlich der Erbringung seiner Dienste verarbeitet, aus laufenden Übertragungen erhebt. Gegenüber einem Anbieter von Telekommunikationsdiensten oder von digitalen Diensten, bei dem es sich um eine inländische juristische Person handelt, ist eine solche Maßnahme nur zulässig, wenn

1. ein ausländisches Unternehmen einen beherrschenden Einfluss über den Anbieter ausübt,

2. der Anbieter einem Auskunftsersuchen nach § 13 Absatz 5 nicht nachgekommen ist, oder

3. tatsächliche Anhaltspunkte dafür bestehen, dass der Zweck eines Auskunftsersuchens durch die Offenlegung des Ersuchens gegenüber dem Verpflichteten gefährdet wäre.

Dabei darf der Bundesnachrichtendienst auch personenbezogene Daten erheben, die der Anbieter während der Verarbeitung der laufenden Übertragung in seinen informationstechnischen Systemen speichert, sofern diese innerhalb des Anordnungszeitraums der strategischen Aufklärungsmaßnahme erhoben werden und vor ihrer Erhebung durch den Bundesnachrichtendienst nicht älter als 72 Stunden sind. Verschafft sich der Bundesnachrichtendienst nach Satz 1 Zugang, so darf er auch Bestandsdaten des Anbieters erheben, die dieser anlässlich der Erbringung seines Dienstes verarbeitet. Die in § 39 Absatz 3 genannten technischen Vorgaben gelten entsprechend.

(3) Die Erhebung von reiner Inlandskommunikation ist unzulässig. Soweit technisch möglich, ist dafür zu sorgen, dass solche Daten automatisiert herausgefiltert und gelöscht werden. Die Filtermethoden werden kontinuierlich fortentwickelt und sind auf dem jeweiligen Stand der Technik zu halten. Wird im Rahmen der Einsichtnahme erkannt, dass Daten entgegen Satz 1 erhoben wurden, sind diese unverzüglich zu löschen. Abweichend von Satz 1 ist eine Erhebung reiner Inlandskommunikation ausnahmsweise zulässig, wenn

1. tatsächliche Anhaltspunkte vorliegen, dass es sich bei den Übertragungen um Angriffe im Sinne von § 4 Absatz 4 Nummer 3 handelt,

2. die Erhebung dem Schutz der betroffenen Person dient, die betroffene Person in die Weiterverarbeitung eingewilligt hat oder, falls eine Einwilligung nicht oder nicht rechtzeitig eingeholt werden kann, die Weiterverarbeitung dem mutmaßlichen Willen der betroffenen Person entspricht,

3. tatsächliche Anhaltspunkte dafür vorliegen, dass die Erhebung erforderlich ist zur Abwehr einer erheblichen Gefahr für ein besonders gewichtiges Rechtsgut, oder

4. es sich bei den Daten nicht um kommunikationsbezogene Inhaltsdaten handelt und diejenigen Daten, die eine Identifizierung von Absender und Empfänger ermöglichen, bei Erhebung automatisiert unkenntlich gemacht wurden, wobei die Unkenntlichmachung auch dergestalt erfolgen kann, dass die Eindeutigkeit der Daten erhalten bleibt,

wenn eine rückwirkende Identifizierung der Person unmöglich oder nur mit unvertretbar hohem Aufwand möglich ist.

Eine Einsichtnahme in die Daten richtet sich nach § 33. Die nach Satz 5 Nummer 1 erhobenen Daten dürfen nach Einsichtnahme nur zur Aufklärung eines Angriffs im Sinne von § 4 Absatz 4 Nummer 3 sowie im Rahmen der in § 31 Absatz 6 genannten Maßnahmen weiterverarbeitet werden. Die nach Satz 5 Nummer 2 bis 3 erhobenen Daten dürfen nach Einsichtnahme nur für die dort genannten Zwecke weiterverarbeitet werden.

§ 33

Einsichtnahme in Kommunikationsdaten im Rahmen von strategischen Aufklärungsmaßnahmen

(1) Der Bundesnachrichtendienst darf im Rahmen von strategischen Aufklärungsmaßnahmen in kommunikationsbezogene Metadaten Einsicht nehmen, wenn dies zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist.

(2) Der Bundesnachrichtendienst darf im Rahmen von strategischen Aufklärungsmaßnahmen in kommunikationsbezogene Inhaltsdaten nur Einsicht nehmen, wenn

1. tatsächliche Anhaltspunkte dafür vorliegen, dass die Einsichtnahme erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen,

2. die Einsichtnahme dem Schutz der betroffenen Person dient, die betroffene Person in die Erhebung oder Einsichtnahme eingewilligt hat oder, falls eine Einwilligung nicht oder nicht rechtzeitig eingeholt werden kann, die Einsichtnahme dem mutmaßlichen Willen der betroffenen Person entspricht, oder

3. tatsächliche Anhaltspunkte dafür vorliegen, dass die Einsichtnahme erforderlich ist zur Abwehr einer erheblichen Gefahr für ein besonders gewichtiges Rechtsgut.

(3) Der Bundesnachrichtendienst darf die Einsichtnahme in kommunikationsbezogene Inhaltsdaten nach Absatz 2 Nummer 1 und 2 nur anhand von Suchbegriffen durchführen. Diese müssen für die jeweilige strategische Aufklärungsmaßnahme bestimmt, geeignet und erforderlich sein und ihre Verwendung muss im Einklang mit den außen- oder sicherheitspolitischen Interessen der Bundesrepublik Deutschland stehen.

(4) Der Bundesnachrichtendienst darf abweichend von den Absätzen 1 und 2 in Kommunikationsdaten, die im Rahmen der strategischen Aufklärung erhoben wurden, auch zur Eignungsprüfung Einsicht nehmen. In diesem Fall darf er die Kommunikationsdaten nur für die Zwecke der Eignungsprüfung weiterverarbeiten.

(5) Die individualisierende Überwachung der gesamten Telekommunikation einer Person im Rahmen einer strategischen Aufklärungsmaßnahme, welche dazu führt, dass die Aufklärungsmaßnahme in Sicherheit und Wirkung einer Telekommunikationsüberwachung nach § 35 annähernd vergleichbar ist, ist nur unter den dortigen Voraussetzungen zulässig.

§ 34

Besondere Vorgaben für die Einsichtnahme in Kommunikationsdaten mit qualifiziertem Inlandsbezug

(1) Der Bundesnachrichtendienst darf in kommunikationsbezogene Metadaten mit qualifiziertem Inlandsbezug nur Einsicht nehmen, wenn die Voraussetzungen des § 33 Absatz 2 vorliegen.

(2) Der Bundesnachrichtendienst darf in kommunikationsbezogene Inhaltsdaten mit qualifiziertem Inlandsbezug nur Einsicht nehmen, wenn die Voraussetzungen des § 33 Absatz 2 vorliegen. § 33 Absatz 3 findet mit der Maßgabe Anwendung, dass keine Suchbegriffe verwendet werden dürfen, die Personen mit qualifiziertem Inlandsbezug zugeordnet sind. Die Verwendung von Suchbegriffen, die Personen mit qualifiziertem Inlandsbezug zugeordnet sind, ist abweichend von Satz 2 ausnahmsweise zulässig, wenn

1. tatsächliche Anhaltspunkte dafür bestehen, dass die Verwendung der Suchbegriffe erforderlich ist, um Angriffe im Sinne von § 4 Absatz 4 Nummer 3 aufzuklären,

2. dies dem Schutz der betroffenen Person dient, die betroffene Person in die Einsichtnahme eingewilligt hat oder, falls eine Einwilligung nicht oder nicht rechtzeitig eingeholt werden kann, die Einsichtnahme dem mutmaßlichen Willen der betroffenen Person entspricht, oder

3. tatsächliche Anhaltspunkte dafür vorliegen, dass die Verwendung der Suchbegriffe erforderlich ist zur Abwehr einer erheblichen Gefahr für ein besonders gewichtiges Rechtsgut.

§ 35

Telekommunikationsüberwachung

(1) Der Bundesnachrichtendienst darf mittels Telekommunikationsüberwachung personenbezogene Daten erheben, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist. Die Erhebung von kommunikationsbezogenen Inhaltsdaten ist nur zulässig, wenn tatsächliche Anhaltspunkte vorliegen, dass die Maßnahme im Einzelfall erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen.

(2) Richtet sich die Maßnahme gegen Personen mit qualifiziertem Inlandsbezug, so darf der Bundesnachrichtendienst personenbezogene Daten nur dann erheben, wenn im Einzelfall tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen. Die Erhebung von kommunikationsbezogenen Inhaltsdaten ist nur zulässig, wenn im Einzelfall tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme erforderlich ist, um Informationen zu Bedrohungen von herausgehobener Bedeutung zu erlangen.

(3) Die Telekommunikationsüberwachung darf auch in der Weise erfolgen, dass die von der Telekommunikationsüberwachung betroffenen Anschlusskennungen als Suchbegriffe im Rahmen einer strategischen Aufklärungsmaßnahme verwendet werden.

(4) Maßnahmen nach Absatz 1 Satz 2 und nach Absatz 2 dürfen sich nur gegen Personen richten, hinsichtlich derer tatsächliche Anhaltspunkte dafür vorliegen, dass

1. sie für die erhebliche Bedrohung oder, im Falle des Absatzes 2 Satz 2, für die Bedrohung von herausgehobener Bedeutung verantwortlich sind oder diese unterstützen,

2. sie Mitglieder eines abgrenzbaren Netzwerks sind, sofern zugleich tatsächliche Anhaltspunkte dafür vorliegen, dass das Netzwerk für die zumindest erhebliche Bedrohung oder, im Falle des Absatzes 2 Satz 2, für die Bedrohung von herausgehobener Bedeutung verantwortlich ist, oder von seinen Mitgliedern ausschließlich oder ganz überwiegend dazu genutzt wird, um die zumindest erhebliche Bedrohung oder, im Falle des Absatzes 2 Satz 2, um die Bedrohung von herausgehobener Bedeutung zu unterstützen, oder

3. sie in Zusammenhang mit einer erheblichen Bedrohung oder, im Falle des Absatzes 2 Satz 2, mit einer Bedrohung von herausgehobener Bedeutung stehen, der Grund zu der Annahme gibt, dass durch die Maßnahme Erkenntnisse über die jeweilige Bedrohungen gewonnen werden können, die nicht gleichermaßen durch eine Maßnahme gegen eine Person nach Nummer 1 zu gewinnen sind, insbesondere

   a) dass diese Personen für eine Person nach Nummer 1 bestimmte oder von ihr herrührende Informationen entgegennehmen oder weitergeben,

   b) dass eine Person nach Nummer 1 oder Buchstabe a den Anschluss dieser Person benutzt.

§ 36

Erhebung technischer Spuren aus informationstechnischen Systemen bei informationstechnischen Angriffen

(1) Soweit im Rahmen von besonderen Auskunftsersuchen bei informationstechnischen Angriffen nach § 14 Absatz 1 die dort genannten Informationen nicht oder nicht ohne Gefährdung des Zwecks der Maßnahme durch Auskunft bei dem Anbieter erlangt werden können, darf der Bundesnachrichtendienst diese Informationen auch durch den Zugriff auf das informationstechnische System erheben. Können die Informationen nach § 14 Absatz 1 Satz 2 Nummer 2 nicht ohne Gefährdung des Zwecks der Maßnahme aufgespürt werden, ist die Erstellung einer Kopie der Teile des informationstechnischen Systems, deren Auswertung zum Aufspüren der Informationen erforderlich ist, zulässig. Kopien nach Satz 2 dürfen nicht fortlaufend erhoben werden.

(2) Stellt der Bundesnachrichtendienst Angriffswerkzeuge oder Daten, die bei einem informationstechnischen Angriff beschafft wurden, fest, darf er sie im informationstechnischen System nach Herstellung einer Sicherungskopie löschen oder deren Verwendbarkeit einschränken, wenn eine entsprechende Maßnahme durch eine andere Behörde mit Ausnahme eines anderen Nachrichtendienstes mittels einer gleich geeigneten Maßnahme nicht oder nicht rechtzeitig erfolgen kann. Ist die Herstellung einer Sicherungskopie nicht ohne Gefährdung des Zwecks der Maßnahme möglich, hat der Bundesnachrichtendienst die Löschung der Daten oder die Einschränkung der Verwendbarkeit zu dokumentieren.

§ 37

Erhebung von Daten aus informationstechnischen Systemen

(1) Der Bundesnachrichtendienst darf auf informationstechnische Systeme, die aufgrund ihrer technischen Funktionalität allein oder durch technische Vernetzung Daten derart vorhalten können, dass bei einem Zugriff auf das jeweilige System Umfang, Vielfalt und Qualität der Daten einen Einblick in wesentliche Teile der Lebensgestaltung einer Person oder ein aussagekräftiges Bild der Persönlichkeit ermöglichen, zugreifen und dort verarbeitete personenbezogene Daten erheben, wenn tatsächliche Anhaltspunkte dafür vorliegen,

dass dies erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen.

(2) Richtet sich die Maßnahme gegen ein informationstechnisches System im Sinne des Absatzes 1, welches als eigenes privat genutzt wird, so ist die Maßnahme nur zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass durch sie Informationen zu Bedrohungen von herausgehobener Bedeutung erlangt werden können.

(3) Eine Maßnahme nach Absatz 2 gegen eine Person mit deutscher Staatsangehörigkeit ist nur zulässig, wenn

1. bestimmte Tatsachen die Annahme rechtfertigen, dass eine zumindest konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut vorliegt, und

2. die Maßnahme nicht oder nicht rechtzeitig durch eine andere Behörde mit Ausnahme eines anderen Nachrichtendienstes mittels einer gleich geeigneten Maßnahme durchgeführt werden kann.

Gegen eine sich im Bundesgebiet aufhaltenden Person ist eine Maßnahme nach Absatz 2 nur zulässig, wenn die Voraussetzungen des Satzes 1 sowie tatsächliche Anhaltspunkte dafür vorliegen, dass die konkretisierte Gefahr in einem unmittelbaren Zusammenhang mit einer grenzüberschreitenden Tätigkeit steht.

(4) Wird bei der Durchführung einer Maßnahme erkennbar, dass es sich bei dem betroffenen informationstechnischen System

1. nicht um einfaches, sondern um ein informationstechnisches System im Sinne des Absatzes 1 handelt,

2. nicht um ein informationstechnisches System im Sinne des Absatzes 1, sondern um ein informationstechnisches System im Sinne des Absatzes 2 oder 3 handelt, oder

3. nicht um ein informationstechnisches System im Sinne des Absatzes 2, sondern um ein informationstechnisches System im Sinne des Absatzes 3 handelt,

darf die Maßnahme nur fortgeführt werden, wenn die dort genannten Voraussetzungen vorliegen.

§ 38

Abgegrenzte Erhebung von Daten aus informationstechnischen Systemen

(1) Zielt die Maßnahme nach § 37 Absatz 2 oder 3 nur auf die abgegrenzte Erhebung von personenbezogenen Daten, so ist sie zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass durch sie Informationen zu zumindest erheblichen Bedrohungen erlangt werden können. Eine abgegrenzte Erhebung liegt vor, wenn die Maßnahme auf Erkenntnisse aus bestimmten abgegrenzten Teilen der Datenverarbeitung in einem informationstechnischen System und zudem nur auf bestimmte Arten von Daten zielt. Durch eine Mehrzahl von Zugriffen dürfen nicht die Voraussetzungen des § 37 Absatz 2 und 3 umgangen werden.

(2) Eine abgegrenzte Erhebung nach Absatz 1 darf nur bei tatsächlichen Anhaltspunkten dafür erfolgen, dass die Maßnahme im Einzelfall erforderlich ist, um Informationen zu Bedrohungen von herausgehobener Bedeutung zu erlangen, wenn sie

1. gegen deutsche Staatsangehörige oder sich im Bundesgebiet aufhaltende Personen gerichtet ist und

2. auf die Erfassung zielt von,

   a) personenbezogenen Daten, die den Inhalt einer interpersonellen Kommunikation zwischen zwei oder mehr Teilnehmerinnen und Teilnehmern ausmachen, oder

   b) Daten, die vergleichbar gewichtige Einblicke in die Lebensführung ermöglichen.

Daten im Sinne des Satzes 1 Nummer 2 Buchstabe b sind insbesondere umfassende bildliche Dokumentationen.

(3) Bei Maßnahmen nach den Absätzen 1 und 2 ist technisch sicherzustellen, dass nur diejenigen Arten von Daten aus denjenigen abgegrenzten Teilen der Datenverarbeitung des informationstechnischen Systems erhoben werden, auf die die Maßnahme zielt. Ist dies in Ausnahmefällen nicht möglich, sind darüber hinausgehende Daten unverzüglich zu löschen.

(4) § 37 Absatz 4 gilt entsprechend.

§ 39

Vorgaben für die Erhebung von Daten aus informationstechnischen Systemen

(1) Eine Maßnahme nach § 37 Absatz 2 oder 3 sowie § 38 Absatz 2 darf nur durchgeführt werden, wenn anderenfalls die Erlangung der Informationen aussichtslos oder wesentlich erschwert wäre. Die Maßnahme darf sich nur gegen Personen richten, hinsichtlich derer tatsächliche Anhaltspunkte dafür vorliegen, dass

1. sie für die Bedrohung oder, im Falle des § 37 Absatz 3, für die konkretisierte Gefahr verantwortlich sind oder diese unterstützen,

2. sie Mitglieder eines abgrenzbaren Netzwerks sind, sofern zugleich tatsächliche Anhaltspunkte dafür vorliegen, dass das Netzwerk für die zumindest erhebliche Bedrohung oder, im Falle des § 37 Absatz 3, für die konkretisierte Gefahr verantwortlich ist oder von seinen Mitgliedern ausschließlich oder ganz überwiegend dazu genutzt wird, die zumindest erhebliche Bedrohung oder, im Falle des § 37 Absatz 3, die konkretisierte Gefahr zu unterstützen, oder

3. in Zusammenhang mit einer Bedrohung oder, im Falle des § 37 Absatz 3, mit einer konkretisierten Gefahr stehen, der Grund zu der Annahme gibt, dass durch die Maßnahme Erkenntnisse über die Bedrohung oder Gefahr gewonnen werden können, die nicht gleichermaßen nach Nummer 1 zu gewinnen sind, insbesondere

   a) dass diese Personen für eine Person nach Nummer 1 bestimmte oder von ihr herrührende Informationen entgegennehmen oder weitergeben,

   b) dass eine Person nach Nummer 1 oder Buchstabe a deren informationstechnisches System benutzt.

(2) Eine Maßnahme nach den §§ 36 und 37 Absatz 1 bis 3 sowie § 38 darf auch durchgeführt werden, wenn andere Personen oder Informationssysteme unvermeidbar betroffen werden. Sie darf unter Abwägung aller vorliegenden Informationen keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht.

(3) Wird eine Maßnahme nach den §§ 36 bis 38 mit technischen Mitteln durchgeführt, ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenverarbeitung unerlässlich sind, und

2. die die Integrität des informationstechnischen Systems beeinträchtigenden vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch und ohne Gefährdung des Zwecks der Maßnahme möglich, rückgängig gemacht werden, falls keine tatsächlichen Anhaltspunkte im Einzelfall dafür vorliegen, dass die Veränderung in absehbarer Zeit erneut zur Durchführung einer nachrichtendienstlichen Maßnahme erforderlich ist.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(4) Stellt der Bundesnachrichtendienst während einer Maßnahme nach §§ 36 bis 38 fest, dass Tatsachen vorliegen, die die Annahme rechtfertigen, dass eine unmittelbar bevorstehende Gefahr für ein besonders gewichtiges Rechtsgut besteht, so darf der Bundesnachrichtendienst, um diese Gefahr abzuwehren,

1. Daten verändern oder löschen,

2. Datenverkehre umleiten oder unterbinden und

3. den Betrieb des informationstechnischen Systems, von dem die Gefahr ausgeht, einschränken oder unterbinden.

Dies gilt nur, wenn die Gefahr durch eine andere Behörde mit Ausnahme eines anderen Nachrichtendienstes mittels einer gleich geeigneten Maßnahme nicht oder nicht rechtzeitig abgewehrt werden kann und die Maßnahme in einer solchen Art und Weise durchgeführt wird, dass die für die betroffene Person zu erwartenden Nachteile in einem angemessenen Verhältnis zu dem Ziel der Maßnahme stehen.

(5) Die Erhebung von Daten aus informationstechnischen Systemen darf auch gemeinsam mit einer anderen öffentlichen Stelle erfolgen.

§ 40

Datenerhebung durch eine ausländische öffentliche Stelle

(1) Der Bundesnachrichtendienst darf ausländische öffentliche Stellen um die Durchführung technischer Maßnahmen nach diesem Unterabschnitt ersuchen, sofern die Voraussetzungen der jeweiligen Maßnahme vorliegen.

(2) Der Bundesnachrichtendienst darf die von der ausländischen öffentlichen Stelle nach Absatz 1 erhobenen personenbezogenen Daten verarbeiten. Die in diesem Unterabschnitt und in Abschnitt 5 geregelten Vorschriften zur Datenverarbeitung finden entsprechende Anwendung.

(3) Soweit die ausländische öffentliche Stelle Suchbegriffe des Bundesnachrichtendienstes verwendet, müssen diese die in § 33 Absatz 3 oder § 43 Absatz 1 Nummer 2 geregelten Voraussetzungen für die Verwendung von Suchbegriffen erfüllen.

(4) Soweit der Bundesnachrichtendienst die ausländische öffentliche Stelle um eine Erhebung von Daten aus informationstechnischen Systemen oder aus einer Maßnahme der Telekommunikationsüberwachung ersucht, muss die Behördenleitung oder ihre Stellvertretung dem Ersuchen zustimmen. Eine Zustimmung darf nur erfolgen, wenn die Voraussetzungen der jeweiligen Maßnahme vorliegen.

§ 41

Kooperation mit ausländischen öffentlichen Stellen bei der technischen Aufklärung

(1) Soweit der Bundesnachrichtendienst bei der technischen Aufklärung mit ausländischen öffentlichen Stellen, die nachrichtendienstliche Aufgaben wahrnehmen, kooperiert, dürfen dabei auch personenbezogene Daten mittels der in diesem Unterabschnitt geregelten Befugnisse erhoben und an den Kooperationspartner automatisiert übermittelt werden.

(2) Eine Erstreckung der Kooperation auf Kommunikationsdaten mit qualifiziertem Inlandsbezug ist unzulässig. § 32 Absatz 3 gilt entsprechend.

(3) Die strategische Aufklärung und die Telekommunikationsüberwachung auf dem Gebiet der Bundesrepublik Deutschland dürfen bei einer Kooperation nur durch den Bundesnachrichtendienst durchgeführt werden.

(4) Eine Kooperation mit den in Absatz 1 genannten ausländischen öffentlichen Stellen ist zulässig, um

1. frühzeitig zumindest erhebliche Bedrohungen erkennen zu können oder

2. die Aufgabenerfüllung durch den Bundesnachrichtendienst sicherzustellen, die ohne eine solche Kooperation wesentlich erschwert oder unmöglich wäre.

(5) Die Verantwortung für die Zulässigkeit der Kooperation trägt der Bundesnachrichtendienst. Sofern Anhaltspunkte dafür vorliegen, dass der Kooperationspartner die abgegebenen Zusicherungen oder Absprachen nicht einhält, hat der Bundesnachrichtendienst auf deren Einhaltung hinzuwirken und erforderlichenfalls die Kooperation zu beenden.

(6) Der Bundesnachrichtendienst hat unter Nutzung der Ergebnisse und Erfahrungen seiner Arbeit etwaige Hinweise auf besonders schutzbedürftige Personen nach § 22 Absatz 1 zu sammeln und Suchbegriffe, die diesen Personen zuzuordnen sind, zusammenzuführen, um dem besonderen Schutzbedürfnis dieser Personen im Rahmen von Kooperationen Rechnung tragen zu können. Die Datenbanken und Filterverfahren, die dem Zweck nach Satz 1 dienen, sind kontinuierlich zu aktualisieren und fortzuentwickeln.

§ 42

Absichtserklärung für Kooperationen mit ausländischen öffentlichen Stellen bei der technischen Aufklärung

(1) Einzelheiten der Kooperation sind vor dem Beginn zwischen dem Bundesnachrichtendienst und der ausländischen öffentlichen Stelle in einer Absichtserklärung schriftlich niederzulegen. In die Absichtserklärung sind insbesondere aufzunehmen:

1. der Zweck der Kooperation,

2. die Dauer der Kooperation,

3. eine Zusicherung der ausländischen öffentlichen Stelle, dass

   a) die bei der Kooperation erhobenen und übermittelten Daten nur zu dem Zweck verwendet werden, zu dem sie erhoben und übermittelt wurden, und eine Weitergabe an Dritte nur mit Zustimmung des Bundesnachrichtendienstes erfolgt,

   b) Kommunikationsdaten mit qualifiziertem Inlandsbezug, die unbeabsichtigt entgegen § 41 Absatz 2 erhoben oder übermittelt wurden und von der ausländischen öffentlichen Stelle bei der Datenauswertung als solche erkannt werden, unverzüglich gelöscht werden,

   c) Daten von schutzwürdigen Personen nach § 22 Absatz 1 die unbeabsichtigt erhoben oder übermittelt wurden und von der ausländischen öffentlichen Stelle bei der Datenauswertung als solche erkannt werden, unverzüglich gelöscht werden, es sei denn, der Bundesnachrichtendienst kommt zu dem Schluss, dass ein Fall des § 22 Absatz 2 vorliegt,

   d) Daten betreffend den Kernbereich privater Lebensgestaltung, die unbeabsichtigt erhoben oder übermittelt wurden und von der ausländischen öffentlichen Stelle bei der Datenauswertung als solche erkannt werden, unverzüglich gelöscht werden,

   e) die Verwendung der Daten mit grundlegenden rechtsstaatlichen Prinzipien vereinbar ist und die Daten insbesondere weder zu politischer Verfolgung noch zu unmenschlicher oder erniedrigender Bestrafung oder Behandlung oder zur Unterdrückung Oppositioneller oder bestimmter Bevölkerungsgruppen eingesetzt werden,

   f) sich die ausländische öffentliche Stelle bereit erklärt, auf Ersuchen des Bundesnachrichtendienstes Auskunft über die Verwendung der Daten zu erteilen,

   g) einer Löschungsaufforderung des Bundesnachrichtendienstes Folge geleistet wird und

   h) im Falle einer Datenübermittlung nach § 44 die kommunikationsbezogene Metadaten nicht länger als zwölf Monate bevorratend gespeichert werden.

(2) Der Zweck der Kooperation muss gerichtet sein auf die Gewinnung von Informationen

1. zur Gesamtverteidigung der Bundesrepublik Deutschland oder verbündeter Staaten oder zu Einsätzen und dauerhaften Stationierungen der Bundeswehr oder verbündeter Streitkräfte im Ausland sowie der Streitkräfte des Kooperationspartners,

2. zur Gefährdungs- oder Sicherheitslage von Personen,

3. zur Aufklärung sicherheitsgefährdender oder geheimdienstlicher Strukturen sowie sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten mit Auswirkungen auf die Bundesrepublik Deutschland oder Mitgliedstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrags oder auf den Kooperationspartner,

4. zu Terrorismus oder Extremismus, der gewaltbereit oder auf die planvoll verborgen betriebene Durchsetzung politischer, religiöser oder ideologischer Ansichten ausgerichtet ist, oder deren Unterstützung,

5. die grenzüberschreitende Verbreitung von Kriegswaffen im Sinne des Gesetzes über die Kontrolle von Kriegswaffen sowie der unerlaubte Außenwirtschaftsverkehr mit Waren und technischen Unterstützungsleistungen in Fällen von erheblicher Bedeutung,

6. zu terroristischen, staatlichen oder internationalen kriminellen Angriffen auf die Vertraulichkeit, Integrität oder Verfügbarkeit von informationstechnischen Systemen, insbesondere mittels Schadprogrammen,

7. zur organisierten Kriminalität, soweit diese auf die Begehung von Straftaten von erheblicher Bedeutung gerichtet ist,

8. zu krisenhaften Entwicklungen im Ausland und zu deren Auswirkungen,

9. zu politischen, wirtschaftlichen oder militärischen Vorgängen im Ausland, die von erheblicher außen- oder sicherheitspolitischer Bedeutung sind,

10. zur Herstellung oder zum Erhalt wesentlicher Fähigkeiten des Bundesnachrichtendienstes oder des Kooperationspartners oder

11. zu vergleichbaren Fällen.

(3) Für einzelne Kooperationszwecke nach Absatz 2 sind Erkenntnisziel und Dauer schriftlich festzulegen. Die Erkenntnisziele dürfen den außen- oder sicherheitspolitischen Interessen der Bundesrepublik Deutschland nicht entgegenstehen.

(4) Die Absichtserklärung bedarf der Zustimmung des Bundeskanzleramtes.

(5) Ist der Abschluss einer Absichtserklärung aufgrund besonderer Eilbedürftigkeit nicht rechtzeitig möglich und würde ansonsten die Gewinnung der Informationen vereitelt oder wesentlich erschwert, so kann die Kooperation ohne den vorherigen Abschluss einer Absichtserklärung durchgeführt werden, sofern der Kooperationspartner die Einhaltung der in Absatz 1 genannten Vorgaben zusichert und der Zweck der Kooperation der Regelung des Absatzes 2 entspricht. Die besondere Eilbedürftigkeit ist zu begründen. Der Abschluss einer Absichtserklärung ist unverzüglich nachzuholen. Wird die Absichtserklärung nicht unverzüglich nachgeholt, wird der Kooperationspartner zur Löschung der erhobenen und übermittelten Daten aufgefordert.

§ 43

Übermittlung von selektierten Kommunikationsdaten im Rahmen von Kooperationen zur strategischen Aufklärung

(1) Die Übermittlung selektierter Kommunikationsdaten durch den Bundesnachrichtendienst im Rahmen einer Kooperation zur strategischen Aufklärung ist zulässig,

1. um die vereinbarten Kooperationszwecke zu erreichen und

2. wenn für die Selektierung nur solche Suchbegriffe verwendet werden, die zur Erreichung der vereinbarten Kooperationszwecke geeignet und erforderlich sind.

Für die Übermittlung von kommunikationsbezogenen Inhaltsdaten dürfen nur hinreichend bestimmte Suchbegriffe verwendet werden. Die Erhebung der personenbezogenen Daten und die Verwendung der Suchbegriffe müssen zudem in Einklang mit den außen- oder sicherheitspolitischen Interessen der Bundesrepublik Deutschland stehen.

(2) Im Rahmen der Kooperation dürfen selektierte personenbezogene Daten übermittelt werden, wenn eine automatisierte Prüfung die Zulässigkeit der hierfür verwendeten Suchbegriffe ergibt. Dies ist der Fall, wenn

1. die Ausrichtung der verwendeten Suchbegriffe an den Kooperationszielen und -inhalten hinreichend plausibel ist und

2. keine tatsächlichen Anhaltspunkte dafür vorliegen, dass

   a) durch die Verwendung der Suchbegriffe ausschließlich oder überwiegend Informationen aus dem Kernbereich privater Lebensgestaltung erlangt werden oder

   b) Suchbegriffe einer besonders schutzbedürftigen Person nach § 22 Absatz 1 verwendet werden.

(3) Im Rahmen der Kooperation dürfen die anhand der Suchbegriffe zur Übermittlung vorgesehenen Daten an den Kooperationspartner automatisiert übermittelt werden, wenn die folgenden bei einer automatisierten Prüfung erkannten Daten von der Übermittlung ausgenommen werden:

1. Kommunikationsdaten mit qualifiziertem Inlandsbezug oder Daten, deren Übermittlung nationalen Interessen der Bundesrepublik Deutschland entgegenstehen würde,

2. Daten, die zum Kernbereich privater Lebensgestaltung gehören, und

3. Daten, die einer besonders schutzbedürftigen Person nach § 22 Absatz 1 zugeordnet werden können.

(4) Die Übermittlung der Daten ist zu protokollieren.

(5) Das ordnungsgemäße Funktionieren der automatisierten Prüfung nach den Absätzen 2 und 3 ist durch den Bundesnachrichtendienst stichprobenartig zu überprüfen. Die Prüfung erfolgt unter Aufsicht einer Bediensteten oder eines Bediensteten des Bundesnachrichtendienstes, die oder der die Befähigung zum Richteramt hat. Sofern nachträglich erkannt wird, dass Daten entgegen diesen Vorgaben an den Kooperationspartner übermittelt wurden, wird der Kooperationspartner zur Löschung der Daten aufgefordert. Der Bundesnachrichtendienst unterrichtet das Bundeskanzleramt in Abständen von höchstens sechs Monaten über die Durchführung der Prüfung nach Satz 1.

§ 44

Übermittlung unselektierter kommunikationsbezogener Metadaten im Rahmen von Kooperationen bei der strategischen Aufklärung

(1) Die automatisierte Übermittlung von unselektierten kommunikationsbezogenen Metadaten im Rahmen einer Kooperation durch den Bundesnachrichtendienst ist nur zulässig, wenn ein qualifizierter Aufklärungsbedarf vorhanden ist. § 43 Absatz 3 Nummer 1 und 3 und Absatz 4 und 5 findet entsprechende Anwendung.

(2) Ein qualifizierter Aufklärungsbedarf kann mittels einer Anordnung festgestellt werden, wenn Tatsachen vorliegen, die die Annahme rechtfertigen, dass die automatisierte Übermittlung

1. erforderlich ist zur Aufklärung einer zumindest erheblichen Bedrohung und

2. erforderlich ist, um die Handlungsfähigkeit der Bundesrepublik Deutschland oder des Kooperationspartners sicherzustellen.

§ 45

Übermittlung personenbezogener Daten im Rahmen von Kooperationen zur Telekommunikationsüberwachung oder der Erhebung gespeicherter Daten aus informationstechnischen Systemen

(1) Die Übermittlung personenbezogener Daten durch den Bundesnachrichtendienst bei Kooperationen im Rahmen von Maßnahmen der Telekommunikationsüberwachung nach § 35 oder der Erhebung gespeicherter Daten aus informationstechnischen Systemen nach den §§ 37 und 38 ist zulässig, um die vereinbarten Kooperationszwecke zu erreichen.

(2) Der Bundesnachrichtendienst darf den Kooperationspartnern die erhobenen personenbezogenen Daten automatisiert übermitteln. Für Daten, die mit einer Maßnahme nach § 37 Absatz 3 erhoben wurden, ist eine automatisierte Übermittlung nur zulässig, wenn die Voraussetzungen für die Maßnahme auch zum Zeitpunkt der Übermittlung vorliegen. Für Daten, die mit Maßnahmen der Telekommunikationsüberwachung erhoben wurden, gilt § 43 entsprechend.

Unterabschnitt 4

Anordnungen

§ 46

Anordnung des Einsatzes nachrichtendienstlicher Mittel

(1) Eine Anordnung durch die Behördenleitung des Bundesnachrichtendienstes oder durch eine von ihr bestimmte Vertretung ist erforderlich,

1. wenn der Einsatz eines der in den Unterabschnitten 1 und 2 genannten nachrichtendienstlichen Mittel voraussetzt, dass tatsächliche Anhaltspunkte dafür bestehen, dass der Einsatz erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen,

2. bei dem Einsatz von nachrichtendienstlichen Mitteln nach § 19 Absatz 1 oder 2 oder

3. bei Maßnahmen nach § 18 Absatz 2 und § 29 Absatz 2.

(2) In der Anordnung sind anzugeben:

1. das Aufklärungsthema sowie im Fall einer gegen eine Person gerichteten Maßnahme die Person, soweit möglich mit Name und Anschrift,

2. Art, Umfang und Dauer der Maßnahme,

3. die Befristung der Anordnung nach Absatz 3,

4. bei Maßnahmen der Wohnraumüberwachung nach § 29 Absatz 2 die zu überwachende Wohnung oder die zu überwachenden Wohnräume sowie

5. eine Begründung.

(3) Die Anordnung für den Einsatz nachrichtendienstlicher Mittel ist zu befristen

1. bei Maßnahmen nach §§ 24 und 25 auf höchstens ein Jahr,

2. bei anderen als den in Nummer 1 genannten Maßnahmen, die nur zulässig sind, wenn tatsächliche Anhaltspunkte dafür bestehen, dass sie erforderlich sind, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen, auf höchstens sechs Monate,

3. bei Maßnahmen, die nur zulässig sind, wenn tatsächliche Anhaltspunkte dafür bestehen, dass sie erforderlich sind, um Informationen zu Bedrohungen von herausgehobener Bedeutung zu erlangen, auf höchstens drei Monate und

4. bei Maßnahmen der Wohnraumüberwachung nach § 29 Absatz 2 auf höchstens einen Monat.

Verlängerungen der Anordnungen sind zulässig, sofern die Voraussetzungen für die Anordnungen fortbestehen.

(4) Die Maßnahme ist vor Ablauf der in Absatz 3 genannten Frist einzustellen, wenn

1. die Voraussetzungen für die Maßnahme nicht mehr vorliegen,

2. der Zweck der Maßnahme erreicht ist oder

3. sich zeigt, dass der Zweck der Maßnahme nicht erreicht werden kann.

(5) Die Anordnung einer gegen eine Person gerichteten Maßnahme kann den Zusatz enthalten, dass sich die Maßnahme auch gegen andere als die in der Anordnung genannten Personen richten kann, wenn tatsächliche Anhaltspunkte vorliegen,

1. dass bei dem in der Anordnung bestimmten Aufklärungsziel mit weiteren Beteiligten zu rechnen ist und

2. die Voraussetzungen der jeweiligen Maßnahme auch in Bezug auf die nicht in der Anordnung genannten Personen vorliegen werden.

(6) Die Anordnung nach Absatz 1 sowie die Durchführung der Maßnahme sind zu dokumentieren.

§ 47

Anordnungen im Zusammenhang mit strategischen Aufklärungsmaßnahmen

(1) Strategische Aufklärungsmaßnahmen bedürfen der Anordnung durch die Behördenleitung des Bundesnachrichtendienstes oder durch eine von ihr bestimmte Vertretung.

(2) In der Anordnung nach Absatz 1 sind anzugeben

1. zur Erhebung von personenbezogenen Daten im Rahmen der jeweiligen strategischen Aufklärungsmaßnahme:

   a) das Aufklärungsthema und

   b) dessen geografischer Fokus, soweit es sich nicht um ein Aufklärungsthema handelt, bei dem tatsächliche Anhaltspunkte dafür bestehen, dass eine geografische Fokussierung nicht möglich ist,

2. zur Einsichtnahme in personenbezogene Daten im Rahmen der jeweiligen strategischen Aufklärungsmaßnahme:

a) die jeweilige erhebliche Bedrohung oder die jeweiligen erheblichen Bedrohungen, zu deren Früherkennung durch Einsichtnahme Informationen gewonnen werden sollen,

b) ob im Rahmen der Maßnahme auch in Kommunikationsdaten mit qualifiziertem Inlandsbezug Einsicht genommen werden soll, und

c) ob und in welchem Ausmaß im Rahmen der Verarbeitung von Daten auch solche Suchbegriffe Verwendung finden sollen, die sich auf bestimmbare Personen beziehen,

3. eine Befristung der Anordnung nach Absatz 3 und

4. eine Begründung.

Die Nennung von Suchbegriffen ist nicht erforderlich.

(3) Die Anordnung nach Absatz 1 ist auf höchstens 36 Monate zu befristen. Verlängerungen der Anordnung sind zulässig, sofern die Voraussetzungen der Anordnung fortbestehen.

(4) Die Einsichtnahme anhand von Suchbegriffen, die Einrichtungen der Europäischen Union oder öffentlichen Stellen der Mitgliedstaaten der Europäischen Union zugeordnet sind, bedarf der gesonderten Anordnung durch die Behördenleitung oder durch eine von ihr bestimmte Vertretung. Gleiches gilt für die Verwendung von Suchbegriffen zum Zweck der Einsichtnahme in Kommunikation aus Vertraulichkeitsbeziehungen nach § 22 Absatz 1.

(5) In einer Anordnung nach Absatz 4 sind anzugeben:

1. die strategische Aufklärungsmaßnahme, in deren Rahmen die Einsichtnahme anhand der Suchbegriffe gemäß Absatz 4 erfolgt,

2. die Person oder Personengruppe, soweit möglich mit Namen und Anschrift, der die Suchbegriffe zuzuordnen sind,

3. eine Befristung der Anordnung nach Absatz 3 Satz 1 und

4. eine Begründung.

Die Nennung von Suchbegriffen ist nicht erforderlich. Verlängerungen der Anordnung sind zulässig, soweit die Voraussetzungen der Anordnung fortbestehen.

(6) Der qualifizierte Aufklärungsbedarf nach § 44 bedarf der Feststellung mittels einer gesonderten Anordnung durch die Behördenleitung oder durch eine von ihr bestimmte Vertretung.

(7) Der Bundesnachrichtendienst unterrichtet das Bundeskanzleramt in regelmäßigen Abständen über Anordnungen nach den Absätzen 1 und 4. Die Anordnungen sowie die Durchführung der Maßnahme sind zu dokumentieren.

§ 48

Anordnung sonstiger besonderer Befugnisse der technischen Aufklärung

(1) Maßnahmen nach § 35 Absatz 2, § 36 Absatz 1, § 37 Absatz 2 oder 3 sowie § 38 bedürfen der Anordnung durch die Behördenleitung oder durch eine von ihr bestimmte Vertretung.

(2) In der Anordnung nach Absatz 1 sind anzugeben:

1. das Aufklärungsziel sowie im Fall einer gegen eine Person gerichteten Maßnahme die Person, soweit möglich mit Namen und Anschrift, gegen die sich die Maßnahme richtet und ob es sich um eine Person mit qualifiziertem Inlandsbezug handelt,

2. die Befristung der Anordnung nach Absatz 3,

3. in den Fällen des § 35 Absatz 4 Nummer 2 Buchstabe b die Rufnummer oder eine andere Kennung eines zu überwachenden Anschlusses,

4. bei Maßnahmen nach § 36 Absatz 1 eine möglichst genaue Bezeichnung des informationstechnischen Systems, aus dem Angriffsspuren erhoben werden sollen,

5. bei Maßnahmen nach § 37 Absatz 2 oder 3 sowie § 38 eine Beschreibung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll, sowie

6. eine Begründung.

(3) Die Anordnung ist auf höchstens zwölf Monate, in den Fällen des § 37 Absatz 3 auf höchstens sechs Monate, zu befristen. Verlängerungen der Anordnungen sind zulässig, sofern die Voraussetzungen der Anordnungen fortbestehen.

(4) Die Anordnung einer gegen eine Person gerichteten Maßnahme kann den Zusatz enthalten, dass sich die Maßnahme auch gegen andere als die in der Anordnung genannten Personen richten kann, wenn tatsächliche Anhaltspunkte dafür vorliegen,

1. dass bei dem in der Anordnung bestimmten Aufklärungsziel mit weiteren Beteiligten zu rechnen ist, und

2. dass die Voraussetzungen der jeweiligen Maßnahme auch in Bezug auf die nicht in der Anordnung genannten Personen vorliegen werden.

Handelt es sich um eine Maßnahme nach § 35 Absatz 4 Nummer 2 Buchstabe b, so kann die Anordnung auch den Zusatz erhalten, dass sich die Maßnahme gegen andere als die in der Anordnung genannten Rufnummern oder Anschlüsse richten kann, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass weitere Rufnummern oder Anschlüsse von Beteiligten oder Nachrichtenmittlern genutzt werden.

(5) Sind zur Durchführung von Maßnahmen nach §§ 36 bis 38 vorbereitende Maßnahmen erforderlich, die in die Integrität eines informationstechnischen Systems eingreifen, sind diese ohne die Erhebung personenbezogener Daten bereits vor Anordnung zulässig, wenn ansonsten der Erfolg der Maßnahme gefährdet wäre.

(6) Die Anordnung nach Absatz 1 sowie die Durchführung der Maßnahme sind zu dokumentieren.

Abschnitt 4

Erweiterte nachrichtendienstliche Maßnahmen

§ 49

Spezifische Gefährdungslage

(1) Im Falle einer spezifischen Gefährdungslage, die der Bundesnachrichtendienst infolge seiner nachrichtendienstlichen Auslandsaufklärung feststellt, obliegt ihm im Rahmen dieses Abschnittes auch ein aktives Einwirken mit dem Ziel einer Abwendung oder Einschränkung dieser Gefährdung (erweiterte nachrichtendienstliche Maßnahmen). Die Zuständigkeit nach Satz 1 besteht im Inland nur, wenn die rechtzeitige Abwendung oder Einschränkung der Gefährdung nur durch den Bundesnachrichtendienst erfolgen kann, insbesondere weil

1. nur er über die erforderlichen Fähigkeiten verfügt oder

2. eine Weitergabe der für die Abwendung oder Einschränkung der Gefährdung erforderlichen Informationen an eine andere Stelle aus Gründen der Geheimhaltung nicht möglich ist.

(2) Eine spezifische Gefährdungslage liegt vor, wenn tatsächliche Anhaltspunkte dafür bestehen, dass besonders gewichtige Rechtsgüter nach § 2 Absatz 2 Nummer 1 bis 5

1. durch eine bestimmte fremde Macht,

2. anhaltend und planvoll sowie

3. in besonderem Maße

gefährdet werden.

(3) Der Bundesnachrichtendienst prüft spätestens sechs Monate nach der ersten Feststellung einer spezifischen Gefährdungslage und sodann in regelmäßigen Abständen von höchstens sechs Monaten, ob eine spezifische Gefährdungslage weiterhin andauert.

§ 50

Grundanordnung

(1) Erweiterte nachrichtendienstliche Maßnahmen dürfen nur auf der Grundlage einer Grundanordnung durchgeführt werden, die das Ziel sowie Art und Umfang der Maßnahmen begrenzt.

(2) Eine Grundanordnung erfolgt durch die Behördenleitung des Bundesnachrichtendienstes oder ihre Vertretung.

(3) In der Grundordnung sind anzugeben:

1. die spezifische Gefährdungslage,

2. Art und Umfang, in denen erweiterte nachrichtendienstliche Maßnahmen erfolgen sollen,

3. eine Befristung nach Absatz 4 und

4. eine Begründung zu den Nummern 1 bis 3.

(4) Die Grundanordnung ist auf höchstens zwölf Monate zu befristen. Sie endet vor Ablauf der Frist, wenn der Bundesnachrichtendienst feststellt, dass die spezifische Gefährdungslage nicht länger vorliegt. Verlängerungen der Grundanordnung sind zulässig, sofern ihre Voraussetzungen fortbestehen.

(5) Die Grundanordnung ist zu dokumentieren.

§ 51

Befugnis für erweiterte nachrichtendienstliche Maßnahmen

(1) Der Bundesnachrichtendienst darf im Rahmen einer Grundanordnung nach § 50 die zur Abwendung oder Einschränkung einer Gefährdung im Einzelfall erforderlichen erweiterten nachrichtendienstlichen Maßnahmen durchführen.

(2) Erweiterte nachrichtendienstliche Maßnahmen sind grundsätzlich außerhalb des Hoheitsgebietes der Bundesrepublik Deutschland durchzuführen. Eine Durchführung im Inland ist nur zulässig, wenn eine Durchführung außerhalb des Hoheitsgebietes der Bundesrepublik Deutschland nicht möglich oder nicht ebenso effektiv ist.

(3) Erweiterte nachrichtendienstliche Maßnahmen sind gegen die fremde Macht zu richten, welche für die spezifische Gefährdungslage verantwortlich ist. Sie dürfen sich nicht gezielt gegen Leib und Leben von Personen richten.

(4) Erweiterte nachrichtendienstliche Maßnahmen müssen in einer solchen Art und Weise durchgeführt werden, dass die zu erwartenden Schäden in einem angemessenen Verhältnis zu dem Ziel der Maßnahme stehen.

(5) Auf Ersuchen des Bundesnachrichtendienst dürfen Dritte bei der Durchführung von erweiterten nachrichtendienstlichen Maßnahmen nach Absatz 1 Hilfe leisten. § 8 gilt entsprechend. Zur Hilfe verpflichtet sind

1. öffentliche Stellen,

2. Anbieter öffentlich zugänglicher Telekommunikationsdienste und Betreiber einer Telekommunikationsanlage, mit der solche Dienste erbracht werden,

3. geschäftsmäßige Anbieter von digitalen Diensten.

Die Verpflichtung gilt nicht, wenn ein Ausnahmegrund entsprechend § 5 Absatz 3 des Verwaltungsverfahrensgesetzes vorliegt. Für eine Hilfeleistung nichtöffentlicher Stellen hat der Bundesnachrichtendienst eine angemessene Entschädigung zu leisten, deren Höhe sich an den nachgewiesenen tatsächlichen Kosten orientiert.

(6) Die Durchführung von erweiterten nachrichtendienstlichen Maßnahmen ist zu dokumentieren.

Abschnitt 5

Weiterverarbeitung personenbezogener Daten

Unterabschnitt 1

Allgemeine Weiterverarbeitungsvorschriften

§ 52

Allgemeine Befugnis zur Weiterverarbeitung

(1) Der Bundesnachrichtendienst darf personenbezogene Daten über die erstmalige Speicherung hinaus nur weiterverarbeiten, wenn

1. tatsächliche Anhaltspunkte dafür bestehen, dass dies zur nachrichtendienstlichen Auslandsaufklärung oder zum Schutz der betroffenen Person erforderlich ist, und

2. dieses Gesetz keine abweichenden Bestimmungen enthält.

Eine Weiterverarbeitung von personenbezogenen Daten, die mit einer Maßnahme nach § 29 Absatz 2 oder mit einer Maßnahme nach § 37 Absatz 3 erhoben wurden, ist nur zulässig, wenn die Voraussetzungen für die Maßnahmen auch zum Zeitpunkt der Weiterverarbeitung vorliegen.

(2) Der Bundesnachrichtendienst darf personenbezogene Daten auch weiterverarbeiten, wenn

1. es sich um Daten aus allgemein zugänglichen Quellen handelt oder

2. die betroffene Person eingewilligt hat.

(3) Der Bundesnachrichtendienst darf personenbezogene Daten zu einer Person in Personendatensätzen speichern. Personendatensätze sind Sammlungen personenbezogener Daten, die anhand bestimmter Merkmale, die zu den jeweiligen Personen hinterlegt werden, in einer Personendatenbank automatisiert ausgewertet werden können. Eine Personendatenbank ist die strukturierte Sammlung von personenbezogenen Daten nach bestimmten, durch den Bundesnachrichtendienst festgelegten Merkmalen, die der nachrichtendienstlichen Auslandsaufklärung dienen, indem Personen automatisiert anhand zuvor definierter Merkmale auffindbar gemacht werden. Der Bundesnachrichtendienst prüft in Abständen von höchstens fünf Jahren die Notwendigkeit der Weiterführung oder einer Änderung einer Personendatenbank.

(4) Die Weiterverarbeitung nach den Absätzen 1 und 2 darf auch automatisiert erfolgen. Dies schließt die Nutzung von Anwendungen ein, welche für ihre Funktion selbstlernende Systeme verwenden und anpassungsfähig auf einen autonomen Betrieb ausgelegt sind (KI-Anwendungen). Diskriminierende Algorithmen dürfen bei der Verwendung von KI-Anwendungen weder herausgebildet noch genutzt werden. Das ordnungsgemäße Funktionieren einer KI-Anwendung ist durch den Bundesnachrichtendienst stichprobenartig zu überprüfen. Die Prüfung erfolgt unter Aufsicht einer Bediensteten oder eines Bediensteten des Bundesnachrichtendienstes, die oder der die Befähigung zum Richteramt hat.

(5) Eine kommerzielle Beschaffung von KI-Anwendungen einer öffentlichen oder nichtöffentlichen Stelle in einem Drittstaat ist nur zulässig, wenn keine gleich geeignete KI-

Anwendung des Bundesnachrichtendienstes selbst, einer anderen inländischen Stelle oder einer Stelle eines Mitgliedstaates der Europäischen Union verfügbar ist.

§ 53

Besondere Befugnis zum Abruf von Auswertungsprodukten mit qualifiziertem Eingriffsgewicht

(1) Der Bundesnachrichtendienst darf Auswertungsprodukte mit qualifiziertem Eingriffsgewicht nur abrufen

1. nach Maßgabe der Absätze 3 bis 5 oder

2. zum Schutz der betroffenen Person, soweit die betroffene Person in den Abruf eingewilligt hat oder, falls eine Einwilligung nicht oder nicht rechtzeitig eingeholt werden kann, der Abruf dem mutmaßlichen Willen der betroffenen Person entspricht.

(2) Auswertungsprodukte mit qualifiziertem Eingriffsgewicht sind solche, die

1. mittels einer automatisierten Auswertung einschließlich unter Verwendung einer KI-Anwendung erstellt wurden,

2. über einen einfachen Datenabgleich hinausgehen und

3. durch Verknüpfung gespeicherter personenbezogener Daten neue Erkenntnisse über die Beziehung einer Person mit deutscher Staatsangehörigkeit oder einer sich im Bundesgebiet aufhaltenden Person zu anderen Personen oder Objekten oder über ihre Persönlichkeit gewinnen lassen.

(3) Der Abruf eines Auswertungsproduktes mit qualifiziertem Eingriffsgewicht, welches weder erheblich noch herausgehoben im Sinne der Absätze 4 und 5 ist, ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist.

(4) Der Abruf eines Auswertungsproduktes mit erheblichem Eingriffsgewicht ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies zur Aufklärung einer zumindest erheblichen Bedrohung erforderlich ist. Auswertungsprodukte mit erheblichem Eingriffsgewicht sind

1. Bewegungsprofile, welche unter Berücksichtigung von zusammenhängendem Zeitraum, zeitlichen Abständen und geodätischer Genauigkeit in der Persönlichkeitsrelevanz gleichwertig zu einer der in § 26 Absatz 2 Nummer 1 in Verbindung mit § 26 Absatz 1 Nummer 1 genannten Maßnahmen der längerfristigen Standortfeststellung sind,

2. solche, die zur Gewinnung von tatsächlichen Anhaltspunkten erstellt werden, dass eine Person, bei der individuell kein Anlass für eine Prüfung bestand, in einem Zusammenhang mit einer zumindest erheblichen Bedrohung steht, der Grund zu der Annahme gibt, dass durch die Aufklärung der Person auch Erkenntnisse über die Bedrohung gewonnen werden können,

3. Verhaltens- und Persönlichkeitsprofile für die umfassende Bewertung des individuellen Bedrohungspotenzials einer Person oder

4. personenbezogene Vorhersagen oder Empfehlungen.

(5) Der Abruf eines Auswertungsproduktes mit herausgehobenen Eingriffsgewicht ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies aufgrund einer Bedrohung von herausgehobener Bedeutung erforderlich ist. Auswertungsprodukte mit herausgehobenem Eingriffsgewicht sind

1. Bewegungsprofile, welche unter Berücksichtigung von zusammenhängendem Zeitraum, zeitlichen Abständen und geodätischer Genauigkeit in der Persönlichkeitsrelevanz gleichwertig zu einer der in § 26 Absatz 2 Nummer 2 in Verbindung mit § 26 Absatz 1 Nummer 2 genannten Maßnahmen der längerfristigen Standortfeststellung sind, oder

2. solche, die zur Gewinnung neuer höchstprivater Erkenntnisse über eine Person erstellt werden.

(6) Ein Auswertungsprodukt mit qualifiziertem Eingriffsgewicht, welches mit dem Ziel einer systematischen Sammlung von Informationen zu einer Person erstellt wurde, darf nur nach Maßgabe des § 20 abgerufen werden.

(7) Eine ausschließlich auf einem Auswertungsprodukt mit qualifiziertem Eingriffsgewicht beruhende automatisierte Veranlassung ist nur bei Auskunftsersuchen gegenüber öffentlichen Stellen nach § 11 zulässig. Abweichend von Satz 1 ist auch eine automatisierte Veranlassung eines Einsatzes von Maßnahmen nach den Abschnitten 3 und 4 zulässig, wenn

1. die Veranlassung mittels einer automatisierten Entscheidung im Einzelfall zur Abwehr eines Angriffs nach § 4 Absatz 4 Nummer 3 erforderlich ist,

2. die Maßnahme beschränkt ist auf

   a) das Verändern oder Löschen von Daten oder

   b) das Umleiten oder Unterbinden von Datenverkehren und

3. der Angriff ohne automatisierte Veranlassung nicht oder nicht rechtzeitig abgewehrt werden kann.

(8) Ein Abruf ist mit Zeitpunkt und abrufender Stelle zu protokollieren. Ist eine Protokollierung nicht möglich, trifft der Bundesnachrichtendienst geeignete technische oder organisatorische Maßnahmen, um eine datenschutzrechtliche Kontrolle zu ermöglichen.

(9) Der Unabhängige Kontrollrat hat die Einhaltung der Vorschriften über den Datenschutz bei der Weiterverarbeitung von Auswertungsprodukten mit qualifiziertem Eingriffsgewicht mindestens alle zwei Jahre zu kontrollieren. Stellt der Unabhängige Kontrollrat bei dieser Kontrolle fest, dass Auswertungsprodukte, die mittels einer automatisierten Auswertung erstellt wurden, dem Eingriffsgewicht der in den Absätzen 3 bis 5 genannten Auswertungsprodukte mit qualifiziertem Eingriffsgewicht nach den Folgen der Auswertung und der gewonnenen Persönlichkeitserkenntnis, insbesondere zu Verhalten, das nicht der Bedrohung dient, gleichkommen, so darf der Bundesnachrichtendienst diese Auswertungsprodukte nur unter den in den Absätzen 3 bis 5 genannten Voraussetzungen abrufen.

§ 54

Weiterverarbeitung von personenbezogenen Daten aus informationstechnischen Speichern

(1) Der Bundesnachrichtendienst darf informationstechnische Speicher, die sich in seinem Besitz befinden und zu denen er sich mit nachrichtendienstlichen Mitteln Zugang verschafft hat oder die er von einer ausländischen öffentlichen Stelle erhalten hat, auslesen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall erforderlich ist, um Informationen zur nachrichtendienstlichen Auslandsaufklärung zu erlangen.

(2) Ergibt sich aus den Umständen der Erlangung des informationstechnischen Speichers oder bei der Weiterverarbeitung der Daten, dass es sich um einen Speicher aus einem privat genutzten informationstechnischen System handelt, dürfen die Daten nur weiterverarbeitet oder übermittelt werden, wenn tatsächliche Anhaltspunkte vorliegen, dass die Maßnahme im Einzelfall erforderlich ist, um Informationen zu erlangen

1. zur Aufklärung von zumindest erheblichen Bedrohungen, oder

2. zur Aufklärung von Bedrohungen von herausgehobener Bedeutung, soweit das informationstechnische System von einer Person mit deutscher Staatsangehörigkeit oder einer sich im Bundesgebiet aufhaltenden Person genutzt wurde.

(3) § 21 Absatz 1 bis 3 findet entsprechende Anwendung.

§ 55

Datensätze zu minderjährigen Personen

(1) Der Bundesnachrichtendienst löscht einen Personendatensatz zu einer minderjährigen Person,

1. die das 16. Lebensjahr noch nicht vollendet hat, spätestens zwei Jahre nach seiner Anlage,

2. die das 16. Lebensjahr vollendet hat, spätestens fünf Jahre nach seiner Anlage.

(2) Fallen nach der Anlage des Personendatensatzes weitere Informationen zu der minderjährigen Person an, die zur nachrichtendienstlichen Auslandsaufklärung erforderlich sind, ist für die Frist des Absatzes 1 auf diesen Zeitpunkt abzustellen.

§ 56

Prüf- und Löschpflichten

(1) Der Bundesnachrichtendienst hat personenbezogene Daten unverzüglich zu löschen, wenn

1. ihre Speicherung unzulässig war oder

2. die Daten

   a) alleine oder in ihrer Gesamtheit zur nachrichtendienstlichen Auslandsaufklärung oder zum Schutz der betroffenen Person nicht oder nicht länger erforderlich sind, und

b) nicht aus allgemein zugänglichen Quellen stammen.

(2) Der Bundesnachrichtendienst prüft in Abständen von höchstens 15 Jahren, ob von ihm gespeicherte personenbezogene Daten alleine oder in ihrer Gesamtheit zur nachrichtendienstlichen Auslandsaufklärung erforderlich sind, soweit

1. es sich nicht um Daten handelt, die erhoben wurden

   a) aus allgemein zugänglichen Quellen, oder

   b) zu sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten einer fremden Macht und

2. nicht besondere Regelungen in diesem Gesetz entgegenstehen.

(3) Die Löschung unterbleibt, wenn tatsächliche Anhaltspunkte vorliegen, dass durch die Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. In diesem Falle dürfen die personenbezogenen Daten nur mit Einwilligung der betroffenen Person weiterverarbeitet oder übermittelt werden.

(4) Die Löschung kann ferner unterbleiben, wenn die Trennung der zu löschenden personenbezogenen Daten von anderen Informationen, die zur Erfüllung der Aufgaben des Bundesnachrichtendienstes erforderlich sind, nicht oder nur mit übermäßigem Aufwand möglich ist oder dem Zweck der Weiterverarbeitung entgegensteht. In diesem Fall ist die Weiterverarbeitung dieser Daten einzuschränken.

(5) Die Löschung unterbleibt, solange und soweit die Daten für eine Mitteilung nach § 100 oder zu Kontrollzwecken des Unabhängigen Kontrollrates erforderlich sind. Dies gilt auch für die Daten, welche zur Dokumentation der Durchführung einer Maßnahme nach § 46 Absatz 6, § 47 Absatz 7 Satz 2 und § 48 Absatz 6 erstellt wurden. In diesem Fall dürfen die Daten nur zu diesen Zwecken weiterverarbeitet oder übermittelt werden. Nach Ablauf von sechs Monaten nach der Mitteilung sind die Daten zu löschen, wenn die betroffene Person kein Interesse an der weiteren Speicherung geltend gemacht hat.

(6) Die Löschung unterbleibt bei im Rahmen der Aufgabenerfüllung erstellten Produkten des Bundesnachrichtendienstes sowie bei den in diesen Produkten enthaltenen personenbezogenen Daten. Personenbezogene Daten, die in Unterlagen, insbesondere in Produkten, des Bundesnachrichtendienstes enthalten sind, sind zu löschen, wenn eine Anbietung nicht zu einer Übernahme durch das Bundesarchiv geführt hat.

§ 57

Protokolldaten

(1) Nach diesem Gesetz zu speichernde Protokolldaten dürfen nur verwendet werden für Zwecke

1. der Datenschutzkontrolle,

2. des Schutzes der Mitarbeiterinnen und Mitarbeiter des Bundesnachrichtendienstes, seiner Einrichtungen, seiner Gegenstände oder seiner nachrichtendienstlichen Verbindungen gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten,

3. der Datensicherung sowie

4. der Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage.

Die nach § 43 Absatz 4 erstellten Protokolldaten dürfen darüber hinaus zur Löschaufforderung an den Kooperationspartner nach § 43 Absatz 5 Satz 3 verwendet werden.

(2) Protokolldaten, die der Bundesnachrichtendienst nach diesem Gesetz zu erstellen hat, sind bis zum Ablauf des zweiten Kalenderjahres, das auf die Protokollierung folgt, aufzubewahren und nach Ablauf dieser Aufbewahrungsfrist unverzüglich zu löschen. Die Löschung der Protokolldaten kann unterbleiben, wenn

1. die Trennung der nicht erforderlichen personenbezogenen Daten von den Informationen, die zur Erfüllung der Aufgaben des Bundesnachrichtendienstes erforderlich sind, nicht oder nur mit übermäßigem Aufwand möglich ist, oder

2. es sich um Protokolldaten nach § 71 handelt.

(3) Abweichend von Absatz 2 darf der Bundesnachrichtendienst Protokolldaten, die zum Schutz seiner Mitarbeiterinnen und Mitarbeiter, seiner Einrichtungen, seiner Gegenstände oder seiner nachrichtendienstlichen Verbindungen gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten erstellt wurden, bis zum Ablauf des fünfzehnten Kalenderjahres, das auf die Protokollierung folgt, aufbewahren. Diese Protokolldaten dürfen nur zu dem in Satz 1 genannten Zweck, einschließlich hieran anknüpfender Maßnahmen, genutzt werden.

§ 58

Verwendungseinschränkung personenbezogener Daten

(1) Der Bundesnachrichtendienst hat personenbezogene Daten, deren Weiterverarbeitung oder Übermittlung nach diesem Gesetz eingeschränkt ist, entsprechend zu kennzeichnen und durch technische oder organisatorische Maßnahmen sicherzustellen, dass eine Weiterverarbeitung oder Übermittlung jenseits der jeweiligen Einschränkung nicht erfolgt.

(2) Eine Aufhebung der Einschränkung ist möglich, wenn ihre Voraussetzungen nachträglich entfallen. In diesem Fall ist die entsprechende Kennzeichnung zu entfernen.

§ 59

Berichtigungspflicht

Der Bundesnachrichtendienst hat gespeicherte personenbezogene Daten in Personendatenbanken zu berichtigen, wenn sie unrichtig sind.

§ 60

Weiterverarbeitung zu Forschungs- oder Entwicklungszwecken

(1) Der Bundesnachrichtendienst darf personenbezogene Daten zu Forschungs- oder Entwicklungszwecken weiterverarbeiten, soweit

1. tatsächliche Anhaltspunkte dafür bestehen, dass die Weiterverarbeitung für die jeweiligen Forschungs- oder Entwicklungszwecke erforderlich ist, und

2. Daten verwendet werden, die unkenntlich gemacht wurden, wobei die Unkenntlichmachung auch dergestalt erfolgen kann, dass die Eindeutigkeit der Daten erhalten bleiben

darf, wenn eine rückwirkende Identifizierung der Person unmöglich oder nur mit unvertretbar hohem Aufwand möglich ist.

Satz 1 Nummer 2 gilt nicht, wenn eine Unkenntlichmachung den jeweiligen Forschungs- oder Entwicklungszwecken widersprechen würde oder nur mit unverhältnismäßigem Aufwand möglich wäre.

(2) Der Bundesnachrichtendienst darf in personenbezogene Daten, die im Rahmen einer strategischen Aufklärungsmaßnahme erhoben wurden, abweichend von den §§ 33 und 34 auch Einsicht nehmen, um sie zu Forschungs- oder Entwicklungszwecken weiterzuverarbeiten.

(3) Erfolgt die Weiterverarbeitung zu dem Zweck, eine KI-Anwendung zu trainieren, hat der Bundesnachrichtendienst dafür Sorge zu tragen, dass diese KI-Anwendung ein angemessenes Niveau an Genauigkeit, Robustheit und Cybersicherheit erreicht.

(4) Soweit personenbezogene Daten zu Forschungs- oder Entwicklungszwecken weiterverarbeitet wurden, sind sie entsprechend zu kennzeichnen und spätestens fünfzehn Jahre nach ihrer Weiterverarbeitung zu löschen. Eine darüberhinausgehende Speicherung ist im Einzelfall möglich, soweit die Speicherung zur Erfüllung der jeweiligen Forschungs- oder Entwicklungszwecke weiterhin erforderlich ist.

(5) Eine Verwendung der zu Forschungs- oder Entwicklungszwecken weiterverarbeiteten personenbezogenen Daten für andere Zwecke ist unzulässig. Dies gilt nicht, wenn tatsächliche Anhaltspunkte für eine unmittelbar bevorstehende Gefahr für ein besonders gewichtiges Rechtsgut vorliegen.

§ 61

Errichtungsanordnungen für Personendatenbanken

(1) Der Bundesnachrichtendienst hat für von ihm betriebene Personendatenbanken Errichtungsanordnungen zu treffen.

(2) In der Errichtungsanordnung nach Absatz 1 ist für jede Personendatenbank festzulegen:

1. die Bezeichnung der Personendatenbank,
2. der Grund für die Errichtung der Personendatenbank,
3. die Voraussetzung der Weiterverarbeitung und Übermittlung,
4. die Anlieferung oder Eingabe,
5. die Zugangsberechtigung,
6. die Überprüfungsfristen,
7. die Speicherungsdauer und
8. die Protokollierung.

(3) Die Errichtungsanordnung bedarf der Zustimmung des Bundeskanzleramtes.

(4) Ist wegen der Dringlichkeit der Aufgabenerfüllung die vorherige Zustimmung des Bundeskanzleramtes und die Anhörung des Unabhängigen Kontrollrates nicht möglich, so

kann der Bundesnachrichtendienst eine Sofortanordnung treffen. Das Verfahren nach den Absätzen 1 bis 3 ist unverzüglich nachzuholen. Wird die Zustimmung des Bundeskanzleramtes nach Absatz 3 nicht erteilt, ist die Sofortanordnung aufzuheben.

(5) Wird die Notwendigkeit einer Errichtungsanordnung nach Absatz 1 erst nachträglich erkannt, so ist das Errichtungsanordnungsverfahren unverzüglich nachzuholen.

§ 62

Akten

(1) Der Bundesnachrichtendienst darf Personen- und Sachakten führen. Personen- und Sachakten werden jeweils von einem Organisationsbereich geführt. Akten oder Auszüge aus Akten dürfen auch in elektronischer Form geführt werden. Bei der Abfrage personenbezogener Daten sind der Zeitpunkt, die Angaben, die die Feststellung der abgefragten Daten ermöglichen, sowie Angaben zur Feststellung des Abfragenden zu protokollieren.

(2) Stellt der Bundesnachrichtendienst fest, dass in Akten gespeicherte personenbezogene Daten unrichtig sind oder wird ihre Richtigkeit von betroffenen Personen bestritten, so ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.

(3) Ist die Führung einer Akte für die Aufgabenerfüllung auch in eingeschränkter Form nicht mehr erforderlich, ist die Akte zu vernichten. Eine Vernichtung der Akte erfolgt nicht, wenn

1. tatsächliche Anhaltspunkte vorliegen, dass durch die Vernichtung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden, oder

2. die Akte nach den Vorschriften des Bundesarchivgesetzes dem Bundesarchiv zur Übernahme anzubieten ist und das Bundesarchiv die Archivwürdigkeit annimmt.

Im Fall von Satz 2 Nummer 1 ist die Verarbeitung der in der Akte gespeicherten personenbezogenen Daten einzuschränken. Die Daten dürfen nur für die Interessen, zu deren Schutz die Vernichtung unterbleibt, verarbeitet werden, oder wenn es zur Abwehr einer konkretisierten Gefahr für besonders gewichtige Rechtsgüter unerlässlich ist.

§ 63

Gemeinsame automatisierte Auswertung mit inländischen öffentlichen Stellen

(1) Der Bundesnachrichtendienst darf mit inländischen öffentlichen Stellen eine automatisierte Auswertung von personenbezogenen Daten, die die beteiligten Stellen in ihren Dateisystemen speichern, einrichten, wenn dies zur nachrichtendienstlichen Auslandsaufklärung für Aufgaben erforderlich ist, die dem Schutz besonders gewichtiger Rechtsgüter dienen und durch die beteiligten Stellen ohne operative Anschlussmaßnahmen zu Lasten der betroffenen Person wahrgenommen werden. In einer Vereinbarung der beteiligten Stellen festzulegen sind:

1. Struktur und Datenmodell der beteiligten Dateisysteme,

2. technische Anforderungen für eine gemeinsame Auswertbarkeit,

3. Zwecke und Voraussetzungen der Auswertung,

4. Verwendung der gewonnenen Informationen.

(2) Der Bundesnachrichtendienst darf für die Auswertung Daten bereitstellen. Die weiteren beteiligten Stellen dürfen Daten bereitstellen, soweit sie sie zur eigenen Auswertung für die Aufgabe nutzen dürfen. Soweit besondere Übermittlungsverbote entgegenstehen, dürfen Daten für die Auswertung nicht bereitgestellt werden. Die Auswertung ist nur zulässig, soweit sie im Einzelfall für den Einrichtungszweck erforderlich ist. Erkenntnisse der Auswertung dürfen nach Maßgabe der Voraussetzungen der §§ 81 bis 83 für die entsprechenden operativen Anschlussmaßnahmen zu Lasten der betroffenen Person genutzt werden. Im Übrigen dürfen Erkenntnisse der Auswertung nicht für operative Anschlussmaßnahmen zu Lasten der betroffenen Person genutzt werden.

(3) Betreibt der Bundesnachrichtendienst ein technisches Verbundsystem, in dem die beteiligten Stellen ihre Dateisysteme zur gemeinsamen Auswertung nach Absatz 1 führen, trifft es technische und organisatorische Maßnahmen entsprechend § 64 Absatz 3 des Bundesdatenschutzgesetzes. Gemeinsame technische Anforderungen für die Verbundteilnahme sind in der Vereinbarung nach Absatz 1 Satz 2 aufzunehmen.

Unterabschnitt 2

Besondere Weiterverarbeitungsvorschriften für Daten aus der technischen Aufklärung

§ 64

Besondere Kennzeichnungspflichten für Daten aus der technischen Aufklärung

(1) Personenbezogene Daten, die der Bundesnachrichtendienst mit einer Maßnahme nach § 37 Absatz 3 erhoben hat, sind unmittelbar nach der Erhebung mit dem Mittel der Datenerhebung zu kennzeichnen.

(2) Der Bundesnachrichtendienst hat, soweit dies technisch möglich ist, durch den Einsatz automatisierter Verfahren dafür zu sorgen, dass Kommunikationsdaten unmittelbar nach der Erhebung wie folgt gekennzeichnet werden:

1. als Kommunikationsdaten mit qualifiziertem Inlandsbezug oder

2. als Daten aus einer der in § 32 Absatz 3 Satz 5 Nummer 1 bis 3 genannten Übertragungen.

Die Verfahren sind kontinuierlich fortzuentwickeln und auf dem jeweiligen Stand der Technik zu halten. Wird der qualifizierte Inlandsbezug von Kommunikationsdaten erst im Rahmen der Einsichtnahme festgestellt oder wurden die Daten mit einer Maßnahme nach § 37 oder § 38 erhoben, so erfolgt die Kennzeichnung als Kommunikationsdaten mit qualifiziertem Inlandsbezug bei der über die erstmalige Speicherung hinausgehenden Weiterverarbeitung.

(3) Stellt der Bundesnachrichtendienst fest, dass es sich bei personenbezogenen Daten um solche aus einer Vertraulichkeitsbeziehung nach § 22 Absatz 1 handelt, so sind die Daten entsprechend zu kennzeichnen.

(4) Die Kennzeichnung entfällt

1. bei Übermittlungen oder

2. dann, wenn die personenbezogenen Daten unkenntlich gemacht wurden, wobei die Unkenntlichmachung auch dergestalt erfolgen kann, dass die Eindeutigkeit der Daten

erhalten bleiben darf, wenn eine rückwirkende Identifizierung der Person unmöglich oder nur mit unvertretbar hohem Aufwand möglich ist.

Abweichend von Satz 1 Nummer 1 bleibt die Kennzeichnung personenbezogener Daten, die der Bundesnachrichtendienst mit einer Maßnahme nach § 37 Absatz 3 erhoben hat, auch bei Übermittlung der Daten erhalten. Die Behördenleitung oder eine von ihr bestimmte Vertretung kann bei den Kennzeichnungen nach Absatz 1 anordnen, dass bei der Übermittlung auf diese Kennzeichnung verzichtet wird, wenn dies unerlässlich ist, um die Geheimhaltung einer Maßnahme nicht zu gefährden, und der Unabhängige Kontrollrat zugestimmt hat. Bei Gefahr im Verzug kann die Übermittlung bereits vor der Zustimmung erfolgen. Wird die Zustimmung versagt, ist die Kennzeichnung durch den Übermittlungsempfänger unverzüglich nachzuholen. Der Empfänger gekennzeichneter Daten prüft unverzüglich, ob die Daten zu löschen sind. Er trifft angemessene organisatorische Vorkehrungen, dass künftig zu löschende Daten gelöscht werden. Der Bundesnachrichtendienst hat den Übermittlungsempfänger von diesen Pflichten zu unterrichten.

§ 65

Besondere Prüfpflichten für Daten aus der technischen Aufklärung

~~(1)~~ Nimmt der Bundesnachrichtendienst Einsicht in kommunikationsbezogene Inhaltsdaten, die im Wege der strategischen Aufklärung erhoben wurden, und führt die Einsichtnahme zu einer Weiterverarbeitung, so sind die Daten spätestens sechs Jahre nach der Weiterverarbeitung erneut darauf hin zu prüfen, ob sie allein oder zusammen mit bereits vorliegenden Daten zur nachrichtendienstlichen Auslandsaufklärung erforderlich sind.

~~(2)~~ Erhebt der Bundesnachrichtendienst kommunikationsbezogene Inhaltsdaten mit einer Maßnahme der Telekommunikationsüberwachung nach § 35, so sind diese Daten unverzüglich daraufhin zu prüfen, ob sie allein oder zusammen mit bereits vorliegenden Daten zur nachrichtendienstlichen Auslandsaufklärung erforderlich sind. Die Prüfung ist spätestens sechs Jahre nach der ersten Prüfung erneut durchzuführen.

~~(3)~~ Handelt es sich bei den Daten nach den Absätzen 1 und 2 um kommunikationsbezogene Inhaltsdaten mit qualifiziertem Inlandsbezug, so ist die erneute Prüfung darauf, ob sie allein oder zusammen mit bereits vorliegenden Daten zur nachrichtendienstlichen Auslandsaufklärung erforderlich sind, bereits nach zwei Jahren durchzuführen.

(4) Die beim Auslesen technischer Spuren aus informationstechnischen Systemen bei informationstechnischen Angriffen nach § 36 erhobenen personenbezogene Daten sind unverzüglich darauf zu prüfen, ob sie für die Aufklärung des Angriffs im Sinne des § 4 Absatz 4 Nummer 3 erforderlich sind. Bei Kopien nach § 36 Absatz 1 Satz 2 prüft der Bundesnachrichtendienst unverzüglich, ob neben den in § 14 Absatz 1 Satz 2 Nummer 2 bezeichneten Informationen auch weitere personenbezogene Daten erhoben worden sind und löscht diese weiteren personenbezogenen Daten unverzüglich.

§ 66

Besondere Löschpflichten für Daten aus der technischen Aufklärung

(1) Die im Wege der strategischen Aufklärung erhobenen kommunikationsbezogenen Inhaltsdaten sind spätestens sechs Monate nach ihrer Erhebung zu löschen. Hat die Einsichtnahme in die Daten zu einer Weiterverarbeitung geführt, gelten unbeschadet des § 65 Absatz 1 und 3 die Vorschriften nach Unterabschnitt 1.

(2) Daten, die mittels einer Maßnahme der technischen Aufklärung erhoben wurden, sind spätestens fünfzehn Jahre nach ihrer Erhebung zu löschen, wenn

1. ihre Inhalte zum Zeitpunkt der Erhebung aus technischen Gründen nicht lesbar gemacht werden können oder

2. die Trennung der nicht erforderlichen Teile personenbezogener Daten von unlesbaren Teilen der Daten nur mit unverhältnismäßigem Aufwand möglich wäre oder den Zweck der Speicherung gefährden würde.

Eine über die Frist in Satz 1 hinausgehende Speicherung ist im Einzelfall möglich, soweit dies zur nachrichtendienstlichen Auslandsaufklärung weiterhin erforderlich ist. Handelt es sich bei den Daten im Sinne von Satz 1 Nummer 1 um kommunikationsbezogene Inhaltsdaten, die im Wege der strategischen Aufklärung erhoben und nachträglich lesbar gemacht worden, findet Absatz 1 entsprechende Anwendung. Die Frist beginnt in diesem Fall mit der Lesbarmachung der Daten.

(3) Kommunikationsbezogene Inhaltsdaten mit qualifiziertem Inlandsbezug sind unverzüglich zu löschen, wenn

1. die Einsichtnahme entgegen den Vorgaben des § 34 Absatz 2 zu einer Weiterverarbeitung geführt hat oder

2. bei der Überprüfung nach § 65 Absatz 3 eine Erforderlichkeit nicht festgestellt wird.

Die Löschung unterbleibt, soweit die Daten im Einzelfall für eine Mitteilung nach § 103 erforderlich sind, oder tatsächliche Anhaltspunkte dafür bestehen, dass die Daten für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Datenerhebung oder für Kontrollzwecke des Unabhängigen Kontrollrates erforderlich sind. In diesem Fall ist die Weiterverarbeitung der Daten einzuschränken; die Daten dürfen nur zu den in Satz 2 genannten Zwecken verwendet werden.

(4) Personenbezogene Daten, die mittels einer Maßnahme der technischen Aufklärung erhoben wurden, sind zu löschen

1. nach zwölf Monaten, wenn es sich um kommunikationsbezogene Metadaten handelt, die

   a) im Wege der strategischen Aufklärung erhoben wurden, sofern nicht die Einsichtnahme zu einer Weiterverarbeitung geführt hat, oder

   b) mittels einer Maßnahme der Telekommunikationsüberwachung nach § 35 erhoben wurden, oder

2. nach 36 Monaten, wenn es sich um personenbezogene Daten handelt, die durch eine Erhebung von Daten aus informationstechnischen Systemen nach § 37 oder eine abgegrenzte Erhebung von Daten aus informationstechnischen Systemen nach § 38 erhoben wurden.

Eine über die in Satz 1 Nummer 1 und 2 genannten Zeiträume hinausgehende Speicherung der Daten ist möglich, wenn dies im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist.

(5) Erkennt der Bundesnachrichtendienst bei der Durchführung einer Maßnahme nach den §§ 37 und 38 oder im Rahmen der Weiterverarbeitung dieser Daten, dass die Voraussetzungen der Maßnahme nicht vorlagen, sind diese unverzüglich zu löschen, es sei denn, die Voraussetzungen des § 37 Absatz 4 liegen vor. Absatz 3 Satz 2 und 3 findet Anwendung.

(6) Eine Löschung nach den Absätzen 3 bis 5 unterbleibt, solange dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zur Abwehr einer unmittelbar bevorstehenden Gefahr für ein besonders gewichtiges Rechtsgut erforderlich ist.

(7) Löschungen nach den Absätzen 1 bis 5 erfolgen unter Aufsicht einer Bediensteten oder eines Bediensteten, die oder der die Befähigung zum Richteramt hat.

§ 67

Besondere Protokollierungspflichten für Daten aus der technischen Aufklärung

Zu protokollieren sind:

1. die Einsichtnahme in und eine nach § 66 Absatz 3 erfolgte Löschung von kommunikationsbezogenen Inhaltsdaten mit qualifiziertem Inlandsbezug,

2. die Löschung von Daten nach § 66 Absatz 5 sowie

3. bei strategischen Aufklärungsmaßnahmen, die nach Maßgabe des § 32 Absatz 2 durchgeführt werden, und bei Eingriffen in informationstechnische Systeme nach § 37 Absatz 2 oder 3

   a) die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,

   b) die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen und

   c) die Angaben, die die Feststellung der erhobenen Daten ermöglichen.

Die Protokollierungspflichten nach § 21 Absatz 2 und § 22 Absatz 4 bleiben unbeschadet.

Abschnitt 6

Übermittlung von personenbezogenen Daten

Unterabschnitt 1

Politische Unterrichtung und Information der Öffentlichkeit

§ 68

Politische Unterrichtung

(1) Der Bundesnachrichtendienst unterrichtet zum Zweck der Information der Bundesregierung zur Wahrnehmung ihrer außen- oder sicherheitspolitischen Verantwortung unmittelbar das Bundeskanzleramt und die Bundesministerien sowie deren nachgeordnete Behörden im Rahmen ihrer Zuständigkeiten; hierbei ist auch die Weitergabe personenbezogener Daten zulässig. Soweit es für den in Satz 1 genannten Zweck der Information erforderlich ist, darf der Bundesnachrichtendienst auch das Bundespräsidialamt und die Landesregierungen sowie deren nachgeordnete Behörden unterrichten. Die empfangende Stelle darf die zur Verfügung gestellten personenbezogenen Daten nur zu dem in Satz 1

genannten Zweck der Information verarbeiten. Eine Weiterverarbeitung zu anderen Zwecken ist nur in den gesetzlich ausdrücklich genannten Fällen zulässig; § 70 Absatz 1 Satz 2 Nummer 1 findet entsprechende Anwendung.

(2) Der Bundesnachrichtendienst darf entsprechend Absatz 1 Satz 1 die Europäische Union sowie die Organisation des Nordatlantikvertrages zum Zweck der Wahrnehmung ihrer außen- oder sicherheitspolitischen Verantwortung unterrichten.

§ 69

Information der Öffentlichkeit

Der Bundesnachrichtendienst kann die Öffentlichkeit und Fachkreise über Erkenntnisse informieren, die er bei seiner Aufgabenwahrnehmung nach § 2 Absatz 1 oder bei der Aufarbeitung seiner Geschichte gewinnt. Bei der Information darf er auch personenbezogene Daten bekanntgeben, wenn

1. dies für die Information über Erkenntnisse nach Satz 1 erforderlich ist und

2. das Interesse der Allgemeinheit die schutzwürdigen Interessen der betroffenen Person überwiegt.

Unterabschnitt 2

Vorgaben zur Übermittlung von personenbezogenen Daten durch den Bundesnachrichtendienst

§ 70

Zweckbindung der übermittelten personenbezogenen Daten

(1) Die empfangende Stelle darf personenbezogene Daten nur zu den Zwecken weiterverarbeiten, zu denen sie ihr vom Bundesnachrichtendienst übermittelt worden sind. Eine Weiterverarbeitung zu anderen Zwecken durch die empfangende Stelle ist nur zulässig, wenn

1. der Bundesnachrichtendienst der Weiterverarbeitung zustimmt oder

2. es sich um Daten handelt, die nach § 79 übermittelt wurden.

Der Bundesnachrichtendienst darf einer über Satz 1 hinausgehenden Weiterverarbeitung nur zustimmen, wenn er die personenbezogenen Daten der empfangenden Stelle auch zu den anderen Zwecken hätte übermitteln dürfen.

(2) Die empfangende Stelle ist verpflichtet, dem Bundesnachrichtendienst auf Verlangen Auskunft über die Weiterverarbeitung der personenbezogenen Daten zu erteilen.

(3) Der Bundesnachrichtendienst hat die empfangende Stelle bei der Übermittlung von personenbezogenen Daten darauf hinzuweisen,

1. zu welchen Zwecken sie die personenbezogenen Daten verarbeiten darf und

2. dass sie dem Bundesnachrichtendienst auf Verlangen Auskunft über die Weiterverarbeitung erteilen muss.

(4) Voraussetzung für die Übermittlung von personenbezogenen Daten an ausländische Stellen und an über- oder zwischenstaatliche Stellen ist über die Absätze 1 und 3 hinaus, dass

1. die ausländische Stelle oder die über- oder zwischenstaatliche Stelle entsprechend Absatz 2 zur Auskunft verpflichtet wird und

2. die ausländische Stelle oder die über- oder zwischenstaatliche Stelle eine Zusicherung abgegeben hat, dass sie einer Löschungsaufforderung des Bundesnachrichtendienstes Folge leistet.

Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass die ausländische Stelle oder die über- oder zwischenstaatliche Stelle eine Zusicherung nach Satz 1 Nummer 2 nicht einhält, hat eine Übermittlung zu unterbleiben.

§ 71

Protokollierung der Übermittlung

Hat der Bundesnachrichtendienst einer anderen Stelle personenbezogene Daten übermittelt, so ist er verpflichtet, die folgenden Daten zu protokollieren:

1. die Stelle, an die die Daten übermittelt worden sind,

2. die Rechtsgrundlage für die Übermittlung und

3. den Zeitpunkt der Übermittlung.

§ 72

Verbundene personenbezogene Daten

(1) Sind mit personenbezogenen Daten, die übermittelt werden sollen, weitere personenbezogene Daten der betroffenen oder einer dritten Person so verbunden, dass eine Trennung der nicht erforderlichen personenbezogenen Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, so ist die Übermittlung auch dieser weiteren Daten zulässig, sofern nicht berechtigte Interessen der betroffenen oder der dritten Person an der Geheimhaltung offensichtlich überwiegen. Die Umstände, die zu einer Unmöglichkeit oder zu einem unverhältnismäßigen Aufwand einer Trennung führen, sind einzelfallbezogen zu dokumentieren.

(2) Die weiteren personenbezogenen Daten der betroffenen oder der dritten Person sind kenntlich zu machen. Die empfangende Stelle darf die übermittelten weiteren personenbezogenen Daten nicht weiterverarbeiten.

§ 73

Pflicht zur Übermittlung vervollständigter oder berichtigter Daten

(1) Erweisen sich personenbezogene Daten nach ihrer Übermittlung als unvollständig oder unrichtig, so hat der Bundesnachrichtendienst unverzüglich der empfangenden Stelle,

der er diese personenbezogenen Daten übermittelt hat, die vervollständigten oder berichtigten Daten zu übermitteln.

(2) Auf die Übermittlung der vervollständigten oder berichtigten Daten kann verzichtet werden, wenn die Vervollständigung oder Berichtigung für die Beurteilung eines Sachverhalts offensichtlich ohne Bedeutung ist und keine Auswirkungen auf andere Sachverhalte erkennbar sind.

§ 74

Verbot der Übermittlung

(1) Der Bundesnachrichtendienst darf personenbezogene Daten nicht übermitteln, wenn

1. für ihn erkennbar ist, dass unter Berücksichtigung der Art der Information und ihrer Erhebung die schutzwürdigen Interessen der betroffenen Person das Allgemeininteresse an der Übermittlung überwiegen,

2. der Übermittlung überwiegende Sicherheitsinteressen entgegenstehen oder

3. der Übermittlung besondere gesetzliche Regelungen zur Weiterverarbeitung der Daten entgegenstehen, wobei die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, unberührt bleibt.

(2) Ist die empfangende Stelle eine ausländische Stelle oder eine über- oder zwischenstaatliche Stelle, so überwiegen schutzwürdige Interessen der betroffenen Person das Allgemeininteresse an einer Übermittlung insbesondere dann, wenn tatsächliche Anhaltspunkte dafür bestehen, dass durch die Verwendung der Daten

1. in dem ausländischen Staat erhebliche Menschenrechtsverletzungen drohen würden oder

2. die Verletzung von elementaren rechtsstaatlichen Grundsätzen droht, etwa wenn die Daten verwendet würden, um eine Person

   a) politisch zu verfolgen oder

   b) unmenschlich oder erniedrigend zu bestrafen oder sonst unmenschlich oder erniedrigend zu behandeln.

In Zweifelsfällen hat der Bundesnachrichtendienst zu berücksichtigen, ob die empfangende Stelle einen angemessenen Schutz der übermittelten Daten zusichert und ob Anhaltspunkte dafür vorliegen, dass die Zusicherung nicht eingehalten wird.

(3) Ist die empfangende Stelle eine ausländische Stelle oder eine über- oder zwischenstaatliche Stelle, so stehen der Übermittlung überwiegende Interessen insbesondere entgegen, wenn durch die Übermittlung beeinträchtigt würden:

1. wesentliche Sicherheitsinteressen des Bundes oder eines Landes oder

2. wesentliche auswärtige Belange der Bundesrepublik Deutschland.

Bei der Prüfung, ob der Übermittlung überwiegende Interessen entgegenstehen, muss der Bundesnachrichtendienst insbesondere die Art der Information und ihre Erhebung sowie den bisherigen Umgang der ausländischen Stelle mit übermittelten Daten berücksichtigen.

§ 75

Schutz von minderjährigen Personen bei Übermittlungen

(1) Personenbezogene Daten einer minderjährigen Person darf der Bundesnachrichtendienst an inländische Stellen nur übermitteln, wenn

1. eine Weiterverarbeitung ausgeschlossen ist

   a) für eine die betroffene Person belastende operative Anschlussmaßnahme oder

   b) für Handlungen, die für die betroffene Person eine nachteilige rechtliche Wirkung entfalten oder sie in anderer Weise erheblich beeinträchtigen,

2. die Übermittlung nach den §§ 81 bis 83 erfolgt und die betroffene Person mindestens 14 Jahre alt ist oder

3. die Übermittlung nach § 82 erfolgt wegen einer konkretisierten Gefahr für

   a) Leib oder Leben einer Person,

   b) Einrichtungen der Bundesrepublik Deutschland, der Europäischen Union oder einer internationalen Organisation, der die Bundesrepublik Deutschland angehört oder

   c) Mitgliedstaaten der Europäischen Union oder des Nordatlantikvertrages.

(2) Personenbezogene Daten einer minderjährigen Person darf der Bundesnachrichtendienst an ausländische öffentliche Stellen nur übermitteln

1. an Staaten, die unmittelbar an die Bundesrepublik Deutschland angrenzen, oder Mitgliedstaaten oder Organe der Europäischen Union oder des Nordatlantikvertrages gemäß Absatz 1,

2. im Übrigen,

   a) wenn

      aa) die minderjährige Person weder deutscher Staatsangehörigkeit ist noch sich im Bundesgebiet aufhält und

      bb) ein besonderes nachrichtendienstliches Interesse an der minderjährigen Person im Einzelfall besteht, insbesondere aufgrund einer besonderen Bedeutung für die Herrschaftsstrukturen einer fremden Macht,

   b) wenn der dringende Tatverdacht einer besonders schweren Straftat besteht nach § 81 in Verbindung mit § 86 oder

   c) zur Abwehr einer konkretisierten Gefahr nach § 82 in Verbindung mit § 86, wobei die konkretisierte Gefahr für Leib oder Leben einer Person oder für Einrichtungen der Europäischen Union oder des Nordatlantikvertrages oder für Einrichtungen von deren Mitgliedstaaten bestehen muss, wenn die Person noch nicht 16 Jahre alt ist.

§ 76

Übermittlung im Interesse der betroffenen Person

~~(1)~~ Der Bundesnachrichtendienst darf personenbezogene Daten an andere Stellen übermitteln, wenn die betroffene Person eingewilligt hat oder offensichtlich ist, dass die Übermittlung im Interesse der betroffenen Person liegt. Er darf personenbezogene Daten insbesondere für Zwecke der Jugendhilfe übermitteln.

~~(2)~~ Eine Übermittlung kann auch automatisiert erfolgen.

§ 77

Vorgaben für die Übermittlung von personenbezogenen Daten aus besonderen Erhebungsarten

Der Bundesnachrichtendienst darf personenbezogene Daten,

1. die er durch eine Maßnahme nach § 29 Absatz 2 oder § 113 Absatz 2 erhoben hat, nur übermitteln,

   a) an inländische öffentliche Stellen zur Strafverfolgung, wenn bestimmte Tatsachen den Verdacht einer in § 100b Absatz 2 der Strafprozessordnung bezeichneten Straftat begründen, beschränkt auf Informationen aus akustischer Überwachung und soweit diese zur Verfolgung dieser Straftat erforderlich sind,

   b) an sonstige Stellen, soweit dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zur Abwehr einer dringenden Gefahr für ein besonders gewichtiges Rechtsgut im Sinne des § 2 Absatz 1 erforderlich ist;

2. die er durch eine Maßnahme nach § 37 Absatz 3 erhoben hat, nur übermitteln,

   a) an inländische öffentliche Stellen zur Strafverfolgung, wenn bestimmte Tatsachen den Verdacht einer in § 100b Absatz 2 der Strafprozessordnung bezeichneten Straftat begründen und soweit die Daten zur Verfolgung dieser Straftat erforderlich sind,

   b) an sonstige Stellen, soweit dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zur Abwehr einer konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut erforderlich ist.

§ 78

Einrichtung automatisierter Abrufverfahren

Zur Übermittlung an inländische öffentliche Stellen kann der Bundesnachrichtendienst in geeigneten Fällen automatisierte Abrufverfahren einrichten.

Unterabschnitt 3

Übermittlung von personenbezogenen Daten durch den Bundesnachrichtendienst

§ 79

Übermittlung an inländische Nachrichtendienste

(1) Der Bundesnachrichtendienst darf personenbezogene Daten an das Bundesamt für Verfassungsschutz, an die Verfassungsschutzbehörden der Länder und an das Bundesamt für den Militärischen Abschirmdienst übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung erforderlich ist

1. zur nachrichtendienstlichen Auslandsaufklärung oder

2. zur Erfüllung der Aufgaben der empfangenden Stelle.

(2) Eine automatisierte Übermittlung von personenbezogenen Daten nach Absatz 1 ist zulässig.

§ 80

Übermittlung an die Bundeswehr

(1) Der Bundesnachrichtendienst darf personenbezogene Daten an die Bundeswehr übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung erforderlich ist

1. für die Sicherstellung der Einsatzbereitschaft und den Schutz der Bundeswehr oder verbündeter Streitkräfte,

2. zur Landes- und Bündnisverteidigung, oder

3. zur Vorbereitung oder Durchführung von Auslandseinsätzen.

(2) Eine automatisierte Übermittlung von personenbezogenen Daten nach Absatz 1 ist zulässig.

§ 81

Übermittlung an inländische öffentliche Stellen zur Strafverfolgung

(1) Der Bundesnachrichtendienst darf personenbezogene Daten an eine inländische öffentliche Stelle zur Strafverfolgung übermitteln, wenn bestimmte Tatsachen den Verdacht einer besonders schweren Straftat begründen und soweit die Daten zur Verfolgung dieser Straftat erforderlich sind.

(2) Besonders schwere Straftaten im Sinne des Absatzes 1 sind Straftaten,

1. die im Höchstmaß mit Freiheitsstrafe von mehr als fünf Jahren bedroht sind und

2. die aus der Anlage 1 ersichtlichen Straftaten.

§ 82

Übermittlung an inländische öffentliche Stellen zur Gefahrenabwehr

Der Bundesnachrichtendienst darf personenbezogene Daten an inländische öffentliche Stellen übermitteln, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung im Einzelfall zur Abwehr einer zumindest konkretisierten Gefahr für ein besonders gewichtiges Rechtsguts erforderlich ist. Soweit die Übermittlung personenbezogener Daten durch den Bundesnachrichtendienst an inländische öffentliche Stellen in anderen Rechtsvorschriften vorgesehen ist, bleiben diese unberührt.

§ 83

Übermittlung an inländische öffentliche Stellen im Gefahrenvorfeld

(1) Der Bundesnachrichtendienst darf personenbezogene Daten an inländische öffentliche Stellen übermitteln, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung im Einzelfall zum Schutz eines besonders gewichtigen Rechtsguts erforderlich ist,

1. zur Bereitstellung von Hintergrundinformationen an die empfangenden Stellen zu Themen und Staaten in ihrem Zuständigkeitsbereich zur Erstellung eines eigenen Lagebildes,

2. für Aufgaben nach dem Staatsangehörigkeitsrecht,

3. für Aufgaben nach dem Aufenthaltsrecht oder zur Untersagung der Ausreise,

4. zur Verhinderung von strategischer Einflussnahme oder Ausspähung durch ausländische Mächte,

5. zur Aufklärung von Teilnehmerinnen und Teilnehmern am Außenwirtschaftsverkehr über Umstände, die für die Einhaltung von Beschränkungen des Außenwirtschaftsverkehrs von Bedeutung sind, einschließlich der Durchsetzung von im Bereich der Gemeinsamen Außen- und Sicherheitspolitik der Europäischen Union beschlossenen wirtschaftlichen Sanktionsmaßnahmen und

6. zum Schutz der Sicherheit in der Informationstechnik.

(2) Der Bundesnachrichtendienst darf personenbezogene Daten an eine inländische öffentliche Stelle zur Vorbereitung, Durchführung oder Überprüfung einer begünstigenden Maßnahme übermitteln, wenn dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zum Schutz besonders gewichtiger Rechtsgüter erforderlich ist.

§ 84

Übermittlung an inländische öffentliche Stellen ohne Möglichkeit operativer Anschlussmaßnahmen

(1) Der Bundesnachrichtendienst darf personenbezogene Daten an inländische öffentliche Stellen übermitteln, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist, insbesondere zur Vorbereitung und Durchführung eigener Maßnahmen des Bundesnachrichtendienstes.

(2) Der Bundesnachrichtendienst darf personenbezogene Daten an inländische öffentliche Stellen übermitteln, wenn dies auf Grund tatsächlicher Anhaltspunkte zum Schutz eines besonders gewichtigen Rechtsgutes für Aufgaben erforderlich ist, die die empfangende Stelle ohne operative Anschlussmaßnahmen zu Lasten der betroffenen Person wahrnimmt.

(3) Liegen die Voraussetzungen nach den §§ 81 und 82 nicht vor, darf die empfangende Stelle die übermittelten Daten nicht für operative Anschlussmaßnahmen zu Lasten der betroffenen Person nutzen.

(4) Der Bundesnachrichtendienst darf personenbezogene Daten an eine inländische öffentliche Stelle zum Zweck der Forschung und Entwicklung auch automatisiert übermitteln, soweit

1. tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung für die jeweiligen Forschungs- oder Entwicklungszwecke erforderlich ist, und

2. Daten verwendet werden, die unkenntlich gemacht wurden, wobei die Unkenntlichmachung auch dergestalt erfolgen kann, dass die Eindeutigkeit der Daten erhalten bleiben darf, wenn eine rückwirkende Identifizierung der Person unmöglich oder nur mit unvertretbar hohem Aufwand möglich ist.

Satz 1 Nummer 2 gilt nicht, wenn eine Unkenntlichmachung den jeweiligen Forschungs- oder Entwicklungszwecken widersprechen würde oder nur mit unverhältnismäßigem Aufwand möglich wäre.

§ 85

Übermittlung an inländische nichtöffentliche Stellen

(1) Der Bundesnachrichtendienst darf personenbezogene Daten an inländische nichtöffentliche Stellen übermitteln, wenn das mit der Übermittlung verfolgte Ziel nicht in gleicher Weise auch durch eine Übermittlung an eine zuständige öffentliche Stelle zu erreichen ist und tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung erforderlich ist

1. zur Abwehr einer zumindest konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut oder

2. zur Erreichung eines der folgenden Ziele

   a) Gewährleistung der Sicherheit von lebenswichtigen Gütern der Allgemeinheit,

   b) Schutz des Bestandes oder der Sicherheit des Bundes oder eines Landes oder für die Sicherheit eines Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages,

   c) Sicherstellung der Funktionsfähigkeit staatlicher Einrichtungen und kritischer Infrastrukturen der Bundesrepublik Deutschland oder der Mitgliedsstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrags,

   d) Schutz der freiheitlich demokratischen Grundordnung,

   e) Schutz der Sicherheit in der Informationstechnik,

f) Schutz der Wirtschaft gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten,

g) Schutz des Finanzsystems des Bundes vor Zufluss von inkriminierten Geldern in erheblicher Höhe,

h) wissenschaftliche Erforschung und Bewertung von Bedrohungen gegen besonders gewichtige Rechtsgüter.

Eine inländische nichtöffentliche Stelle, die personenbezogene Daten nach Satz 1 Nummer 2 erhalten hat, darf die Daten für Handlungen, die für die betroffene Person eine nachteilige rechtliche Wirkung entfalten oder diese Person in anderer Weise erheblich beeinträchtigen, nur verwenden, wenn dies im Einzelfall zum Schutz eines besonders gewichtigen Rechtsguts erforderlich ist und der Bundesnachrichtendienst der Verwendung zustimmt. Bei einer unmittelbar bevorstehenden Gefahr ist die vorherige Zustimmung des Bundesnachrichtendienstes entbehrlich. Die inländische nichtöffentliche Stelle hat den Bundesnachrichtendienst unverzüglich über ihre Handlungen und deren Anlass zu unterrichten.

(2) Abweichend von Absatz 1 darf der Bundesnachrichtendienst personenbezogene Daten auch zur eigenen Aufklärung einer Bedrohung für ein besonders gewichtiges Rechtsgut übermitteln, insbesondere zur Vorbereitung oder Konkretisierung eines Auskunftsersuchens.

(3) Der Bundesnachrichtendienst darf personenbezogene Daten an eine inländische nichtöffentliche Stelle zum Zweck der Forschung und Entwicklung auch automatisiert übermitteln, soweit

1. tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung für die jeweiligen Forschungs- oder Entwicklungszwecke erforderlich ist, und

2. Daten verwendet werden, die unkenntlich gemacht wurden, wobei die Unkenntlichmachung auch dergestalt erfolgen kann, dass die Eindeutigkeit der Daten erhalten bleiben darf, wenn eine rückwirkende Identifizierung der Person unmöglich oder nur mit unvertretbar hohem Aufwand möglich ist.

Nummer 2 gilt nicht, wenn eine Unkenntlichmachung den jeweiligen Forschungs- oder Entwicklungszwecken widersprechen würde oder nur mit unverhältnismäßigem Aufwand möglich wäre.

§ 86

Übermittlung an ausländische öffentliche Stellen oder an über- oder zwischenstaatliche Stellen

(1) Der Bundesnachrichtendienst darf personenbezogene Daten an ausländische öffentliche Stellen oder an über- oder zwischenstaatliche Stellen übermitteln, wenn bestimmte Tatsachen den Verdacht einer besonders schweren Straftat, deren Gewicht den Straftaten nach § 81 Absatz 2 entspricht, begründen und soweit die Daten zur Aufklärung dieser Straftat erforderlich sind. Eine Aufklärung im Sinne von Satz 1 umfasst nicht die Verwendung von personenbezogenen Daten im Rahmen eines Strafverfahrens. Die Regelungen des Gesetzes über die internationale Rechtshilfe in Strafsachen bleiben insoweit unberührt.

(2) Der Bundesnachrichtendienst darf personenbezogene Daten an ausländische öffentliche sowie über- oder zwischenstaatliche Stellen übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung

1. dem Schutz eines besonders gewichtigen Rechtsguts oder

2. der Sicherheit des Empfängerstaates oder eines Mitgliedstaates der über- oder zwischenstaatlichen Stelle

dient und eine zumindest konkretisierte Gefahr für das besonders gewichtige Rechtsgut oder für die Sicherheit des Empfängerstaates besteht.

(3) Eine Übermittlung an ausländische öffentliche Stellen sowie an über- oder zwischenstaatliche Stellen ist ferner zulässig, wenn dies dem Schutz eines besonders gewichtigen Rechtsguts oder der Sicherheit des Empfängerstaates oder eines Mitgliedstaates der über- oder zwischenstaatlichen Stelle dient und

1. eine Weiterverarbeitung für operative Anschlussmaßnahmen zu Lasten der betroffenen Person oder Dritter ausgeschlossen ist,

2. für die Vorbereitung und Durchführung eigener Maßnahmen des Bundesnachrichtendienstes erforderlich ist oder

3. für den Schutz der in § 2 Absatz 2 Nummer 1 Buchstabe b, c und Nummer 2 genannten besonders gewichtigen Rechtsgüter, einschließlich durch die Ermöglichung notwendiger Folgemaßnahmen, erforderlich ist.

(4) Der Bundesnachrichtendienst darf personenbezogene Daten an eine ausländische öffentliche Stelle oder an eine über- oder zwischenstaatliche Stelle zum Zweck der Forschung und Entwicklung automatisiert übermitteln, soweit

1. tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung für die jeweiligen Forschungs- oder Entwicklungszwecke erforderlich ist, und

2. Daten verwendet werden, die unkenntlich gemacht wurden, wobei die Unkenntlichmachung auch dergestalt erfolgen kann, dass die Eindeutigkeit der Daten erhalten bleiben darf, wenn eine rückwirkende Identifizierung der Person unmöglich oder nur mit unvertretbar hohem Aufwand möglich ist.

Satz 1 Nummer 2 gilt nicht, wenn eine Unkenntlichmachung den jeweiligen Forschungs- oder Entwicklungszwecken widersprechen würde oder nur mit unverhältnismäßigem Aufwand möglich wäre.

(5) Zum Ausschluss der Weiterverarbeitung für operative Anschlussmaßnahmen nach Absatz 3 Satz 1 Nummer 1 sowie der Weiterverarbeitung zu Zwecken, die über Forschungs- und Entwicklungszwecken hinausgehen, kann der Bundesnachrichtendienst eine Zusicherung der empfangenden Stelle einholen. § 70 Absatz 4 Satz 2 gilt entsprechend.

§ 87

Übermittlung an ausländische nichtöffentliche Stellen

(1) Der Bundesnachrichtendienst darf personenbezogene Daten an ausländische nichtöffentliche Stellen übermitteln, wenn das mit der Übermittlung verfolgte Ziel nicht in gleicher Weise auch durch eine Übermittlung an eine zuständige ausländische öffentliche Stelle zu erreichen ist und tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung zur Abwehr einer unmittelbar bevorstehenden Gefahr für besonders gewichtige Rechtsgüter erforderlich ist.

(2) Übermittlungen nach Absatz 1 bedürfen der vorherigen Zustimmung durch die Behördenleitung des Bundesnachrichtendienstes oder einer von ihr bestimmten Vertretung. Der Bundesnachrichtendienst unterrichtet das Bundeskanzleramt in regelmäßigen Abständen über Übermittlungen nach Absatz 1.

(3) Abweichend von Absatz 1 darf der Bundesnachrichtendienst personenbezogene Daten zur eigenen nachrichtendienstlichen Aufklärung übermitteln, insbesondere zur Vorbereitung oder Konkretisierung einer Anfrage.

§ 88

Übermittlung von sonstigen personenbezogenen Daten

(1) Der Bundesnachrichtendienst darf personenbezogene Daten, die er nicht durch einen biometrischen Abgleich nach § 5 Absatz 3, durch ein Auskunftsersuchen nach Abschnitt 2 oder durch ein nachrichtendienstliches Mittel nach Abschnitt 3 erhoben hat, an andere Stellen übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass dies erforderlich ist

1. zur nachrichtendienstlichen Auslandsaufklärung oder

2. zur Erfüllung der Aufgaben der empfangenden Stellen, wenn es sich bei ihnen um öffentliche Stellen handelt.

(2) Eine automatisierte Übermittlung ist zulässig.

Unterabschnitt 4

Gemeinsame Dateien

§ 89

Projektbezogene gemeinsame Dateien mit inländischen öffentlichen Stellen

(1) Soweit dies für die nachrichtdienstliche Auslandsaufklärung erforderlich ist, kann der Bundesnachrichtendienst für die Dauer einer befristeten projektbezogenen Zusammenarbeit mit inländischen öffentlichen Stellen eine gemeinsame Datei errichten und führen. Die projektbezogene Zusammenarbeit zielt nach Maßgabe der Aufgaben und Befugnisse der beteiligten Stellen auf den Austausch und die gemeinsame Auswertung von personenbezogenen Daten.

(2) Für die Eingabe personenbezogener Daten in die gemeinsame Datei gelten die für die jeweils eingebende öffentliche Stelle geltenden Übermittlungsvorschriften. Die Daten sind so zu kennzeichnen, dass die eingebende Stelle ersichtlich ist. Die Eingabe ist nur zulässig, wenn

1. technisch sichergestellt ist, dass nur diejenigen teilnehmenden Stellen Kenntnis von den jeweiligen Daten erhalten, denen die Daten auch hätten übermittelt werden dürfen, und

2. die Stelle, die die Daten eingegeben hat, die Daten auch in eigenen Dateien speichern darf.

(3) Personenbezogene Daten dürfen durch die an der projektbezogenen Zusammenarbeit beteiligten Stellen im Rahmen ihrer Aufgaben und Befugnisse weiterverarbeitet und übermittelt werden.

(4) Die Berichtigung, Verarbeitungseinschränkung und Löschung von personenbezogenen Daten richtet sich nach den für die eingebende Stelle jeweils geltenden Vorschriften. Die in die gemeinsame Datei eingegebenen personenbezogenen Daten sind spätestens zu löschen, wenn die zugehörigen Erkenntnisse nach den für die beteiligten Stellen jeweils geltenden Vorschriften zu löschen sind.

(5) Die Verantwortung im Sinne der allgemeinen Vorschriften des Datenschutzrechts trägt jede beteiligte Stelle nur für die von ihr eingegebenen Daten.

§ 90

Führung projektbezogener gemeinsamer Dateien mit inländischen öffentlichen Stellen durch den Bundesnachrichtendienst

(1) Eine durch den Bundesnachrichtendienst geführte projektbezogene gemeinsame Datei nach § 89 ist auf höchstens zwei Jahre zu befristen. Die Frist kann jeweils um weitere zwei Jahre verlängert werden, solange das Ziel der projektbezogenen Zusammenarbeit noch nicht erreicht worden ist und die gemeinsame Datei weiterhin für die Erreichung des Ziels erforderlich ist.

(2) Der Bundesnachrichtendienst hat für durch ihn geführte gemeinsame Dateien in einer Errichtungsanordnung die Angaben nach § 61 Absatz 2 sowie darüber hinaus Folgendes festzulegen:

1. die Rechtsgrundlage der gemeinsamen Datei,

2. die an der gemeinsamen Datei beteiligten Stellen,

3. die Arten der personenbezogenen Daten, die der Erschließung der gemeinsamen Datei dienen,

4. die Voraussetzungen, unter denen in der gemeinsamen Datei gespeicherte personenbezogene Daten an bestimmte Empfänger übermittelt werden dürfen, und welches Verfahren für die jeweilige Übermittlung gilt,

5. im Einvernehmen mit den an der projektbezogenen Zusammenarbeit beteiligten Stellen deren jeweilige Organisationseinheiten, die zur Eingabe und zum Aufruf befugt sind,

6. die umgehende Unterrichtung der eingebenden Stelle über Anhaltspunkte für die Unrichtigkeit eingegebener Daten durch die an der gemeinsamen Datei beteiligten Stellen sowie die Prüfung und erforderlichenfalls die unverzügliche Änderung, Berichtigung oder Löschung dieser Daten durch die eingebende Stelle,

7. die Möglichkeit der ergänzenden Eingabe weiterer Daten zu den bereits über eine Person gespeicherten Daten durch die an der gemeinsamen Datei beteiligten Stellen,

8. die Protokollierung des Zeitpunktes, der Angaben zur Feststellung des aufgerufenen Datensatzes sowie der für den Aufruf verantwortlichen beteiligten Stelle bei jedem Aufruf aus der gemeinsamen Datei für Zwecke der Datenschutzkontrolle einschließlich der Zweckbestimmung der Protokolldaten sowie deren Löschfrist und

9. die Zuständigkeit des Bundesnachrichtendienstes für Schadensersatzansprüche der betroffenen Personen nach § 83 des Bundesdatenschutzgesetzes.

(3) Die Errichtungsanordnung bedarf der Zustimmung des Bundeskanzleramtes. Die Errichtung und der Betrieb der gemeinsamen Datei durch den Bundesnachrichtendienst können vor Abschluss des Errichtungsanordnungsverfahrens nach Satz 1 erfolgen.

(4) An einer vom Bundesnachrichtendienst geführten gemeinsamen Datei können sich inländische öffentliche Stellen unbeschadet des § 89 Absatz 1 Satz 2 erst beteiligen, wenn

1. das Bundeskanzleramt der Errichtungsanordnung nach Absatz 3 Satz 1 zugestimmt hat und

2. die für die jeweiligen Stellen zuständigen obersten Bundes- oder Landesbehörden der Beteiligung zugestimmt haben.

(5) § 102 ist mit der Maßgabe anzuwenden, dass

1. der Bundesnachrichtendienst die Auskunft im Einvernehmen mit der Stelle erteilt, die die datenschutzrechtliche Verantwortung nach § 89 Absatz 5 trägt, und

2. die beteiligte Stelle die Zulässigkeit der Auskunftserteilung nach den für sie geltenden Bestimmungen prüft.

§ 91

Erweiterte Nutzung projektbezogener gemeinsamer Dateien mit inländischen öffentlichen Stellen

(1) Der Bundesnachrichtendienst darf zur Erfüllung seiner Aufgaben die in einer gemeinsamen Datei mit inländischen öffentlichen Stellen gespeicherten personenbezogenen Daten erweitert nutzen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall erforderlich ist, um Erkenntnisse zu zumindest erheblichen Bedrohungen zu erlangen. Eine erweiterte Nutzung von personenbezogenen Daten, die mit Maßnahmen nach § 29 Absatz 2 oder § 37 Absatz 3 erhoben wurden, ist nur zulässig, wenn die Voraussetzungen für die Durchführung der Maßnahmen auch bei der Weiterverarbeitung vorliegen.

(2) Eine erweiterte Nutzung ist das Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen, der Ausschluss von unbedeutenden Informationen und Erkenntnissen, die Zuordnung eingehender Informationen zu bekannten Sachverhalten sowie die statistische Auswertung der gespeicherten Daten auch im Wege einer automatisierten Anwendung zur Datenverarbeitung einschließlich selbstlernender Systeme. Hierzu darf der Bundesnachrichtendienst

1. Daten abfragen mittels

   a) phonetischer oder unvollständiger Daten,

   b) der Suche über eine Mehrzahl von Datenfeldern,

   c) der Verknüpfung von Personen, Personengruppen, Institutionen, Objekten, Sachen, Zusammenhängen, Mustern oder

   d) der zeitlichen Eingrenzung der Suchkriterien;

2. räumliche und sonstige Beziehungen zwischen Personen und Zusammenhänge zwischen Personen, Personengruppen, Institutionen, Objekten und Sachen darstellen sowie

3. die Suchkriterien gewichten.

§ 92

Gemeinsame Dateien mit der Bundeswehr

(1) Der Bundesnachrichtendienst kann zum Austausch und zur gemeinsamen Auswertung von Erkenntnissen gemeinsame Dateien mit der Bundeswehr errichten und führen oder sich an von der Bundeswehr errichteten und geführten Dateien beteiligen, soweit dies erforderlich ist,

1. für die Sicherstellung der Einsatzbereitschaft und den Schutz der Bundeswehr oder verbündeter Streitkräfte,

2. zur Landes- und Bündnisverteidigung, oder

~~3.~~ zur Vorbereitung oder Durchführung von Auslandseinsätzen.

(2) Für die Eingabe personenbezogener Daten in die gemeinsame Datei gelten die jeweiligen Übermittlungsvorschriften. Die Daten sind so zu kennzeichnen, dass die eingebende Stelle ersichtlich ist.

(3) Die Berichtigung, Verarbeitungseinschränkung und Löschung von personenbezogenen Daten richtet sich nach den für die eingebende Stelle jeweils geltenden Vorschriften. Die in die gemeinsamen Dateien eingegebenen personenbezogenen Daten sind spätestens zu löschen, wenn sie nach den für die eingebende Stellen jeweils geltenden Vorschriften zu löschen sind.

§ 93

Gemeinsame Dateien mit ausländischen öffentlichen Stellen

(1) Der Bundesnachrichtendienst kann für den Austausch und die gemeinsame Auswertung von personenbezogenen Daten mit ausländischen öffentlichen Stellen gemeinsame Dateien errichten und führen oder sich an diesen beteiligen, wenn

1. dies für die Aufklärung von zumindest erheblichen Bedrohungen erforderlich ist und

2. in dem Staat, dem die ausländische öffentliche Stelle angehört, die Einhaltung grundlegender rechtsstaatlicher Prinzipien gewährleistet ist.

(2) Die Ziele der Zusammenarbeit sowie die Einzelheiten der gemeinsamen Datennutzung sind vor Beginn der Zusammenarbeit zwischen dem Bundesnachrichtendienst und den beteiligten ausländischen öffentlichen Stellen in einer Absichtserklärung schriftlich niederzulegen. In die Absichtserklärung ist neben den Zielen der Zusammenarbeit insbesondere aufzunehmen, dass

1. die Daten nur für diese Ziele verwendet werden dürfen,

2. der Bundesnachrichtendienst sich vorbehält, um Auskunft über die erfolgte Verwendung der in die gemeinsame Datei übermittelten Daten zu bitten, und

3. die jeweils eingebende ausländische öffentliche Stelle auf Anfrage des Bundesnachrichtendienstes verpflichtet ist, vom Bundesnachrichtendienst eingegebene Daten unverzüglich zu sperren, zu berichtigen oder zu löschen.

(3) Die Absichtserklärung bedarf der Zustimmung des Bundeskanzleramtes.

(4) Die Eingabe von personenbezogenen Daten durch den Bundesnachrichtendienst in die gemeinsame Datei mit ausländischen öffentlichen Stellen ist nur zulässig, wenn

1. technisch sichergestellt ist, dass nur diejenigen teilnehmenden Stellen Kenntnis von den jeweiligen Daten erhalten, denen die Daten auch hätten übermittelt werden dürfen, und,

2. der Bundesnachrichtendienst die Daten auch in eigenen Dateien speichern darf, und

3. der Bundesnachrichtendienst die Daten so kennzeichnet, dass er als eingebende Stelle ersichtlich ist.

Die Eingabe durch den Bundesnachrichtendienst darf auch automatisiert erfolgen. § 43 Absatz 3 sowie §§ 44 und 45 gelten entsprechend.

(5) Der Bundesnachrichtendienst und die ausländischen öffentlichen Stellen dürfen die gespeicherten personenbezogenen Daten abfragen und diese weiterverarbeiten und übermitteln, wenn dies für die Ziele, zu denen die gemeinsame Datei errichtet wurde, erforderlich ist.

§ 94

Führung gemeinsamer Dateien mit ausländischen öffentlichen Stellen durch den Bundesnachrichtendienst

(1) Der Bundesnachrichtendienst hat für durch ihn geführte mit ausländischen öffentlichen Stellen genutzte gemeinsame Dateien in einer Errichtungsanordnung die Angaben nach § 61 Absatz 2 sowie darüber hinaus Folgendes festzulegen:

1. die Rechtsgrundlage der gemeinsamen Datei,

2. die Voraussetzungen, unter denen in der gemeinsamen Datei gespeicherte personenbezogene Daten an bestimmte Empfänger übermittelt werden dürfen, und welches Verfahren für die jeweilige Übermittlung gilt,

3. die an der gemeinsamen Datei beteiligten ausländischen öffentlichen Stellen,

4. die Absichtserklärung nach § 93 Absatz 2,

5. die Möglichkeit der ergänzenden Eingabe weiterer Daten zu den bereits über eine Person gespeicherten Daten durch die an der gemeinsamen Datei beteiligten ausländischen öffentlichen Stellen,

6. die umgehende Unterrichtung der eingebenden ausländischen öffentlichen Stellen über Anhaltspunkte für die Unrichtigkeit eingegebener Daten durch die beteiligten ausländischen öffentlichen Stellen,

7. diejenigen ausländischen öffentlichen Stellen, die zur Eingabe und zum Aufruf befugt sind,

8. die Protokollierung des Zeitpunktes des Aufrufs, der Angaben zur Feststellung des aufgerufenen Datensatzes sowie der für den Abruf verantwortlichen Stelle bei jedem Aufruf aus der gemeinsamen Datei,

9. die Zuständigkeit des Bundesnachrichtendienstes für Schadensersatzansprüche der betroffenen Person nach § 83 des Bundesdatenschutzgesetzes.

(2) Die Errichtungsanordnung bedarf der Zustimmung des Bundeskanzleramtes. Die Errichtung und der Betrieb der gemeinsamen Datei durch den Bundesnachrichtendienst können vor Abschluss des Errichtungsanordnungsverfahrens nach Satz 1 erfolgen.

(3) An einer durch den Bundesnachrichtendienst geführten gemeinsamen Datei mit ausländischen öffentlichen Stellen können im Rahmen ihrer Aufgaben auch der Militärische Abschirmdienst und das Bundesamt für den Verfassungsschutz teilnehmen.

(4) An einer vom Bundesnachrichtendienst geführten gemeinsamen Datei können sich ausländische öffentliche Stellen erst beteiligen, wenn das Bundeskanzleramtes der Errichtungsanordnung nach Absatz 1 zugestimmt hat.

(5) Eingaben und Aufrufe auf die gemeinsame Datei sind zu protokollieren.

Abschnitt 7

Ergänzende Bestimmungen und Kontrollzuständigkeiten

Unterabschnitt 1

Dienstvorschriften, Unterrichtungspflichten und Kontrollzuständigkeiten

§ 95

Dienstvorschriften

(1) Der Bundesnachrichtendienst benennt die nachrichtendienstlichen Mittel zur Erhebung personenbezogener Daten im Sinne des § 18 Absatz 1 abschließend in einer Dienstvorschrift. In dieser Dienstvorschrift ist, soweit nicht bereits gesetzlich geregelt, auch die Zuständigkeit für die Anordnung der jeweiligen nachrichtendienstlichen Mittel innerhalb des Bundesnachrichtendienstes festzulegen.

(2) Die technische und organisatorische Umsetzung der Regelungen zum Einsatz besonderer technischer Aufklärungsmaßnahmen nach Abschnitt 3 Unterabschnitt 3 ist in Dienstvorschriften festzulegen.

(3) Zum Schutz seiner Bediensteten, Dienststellen und Verschlusssachen darf der Bundesnachrichtendienst in Dienstvorschriften Regelungen zu dienst- und arbeitsrechtlichen Verhaltenspflichten zur Vermeidung von Sicherheitsrisiken erlassen. Falls es zur Vermeidung von nicht unerheblichen Sicherheitsrisiken unerlässlich ist und der Kernbereich privater Lebensgestaltung nicht betroffen wird, darf der Bundesnachrichtendienst dabei auch Bestimmungen zum Verhalten außerhalb des Dienstes treffen.

(4) Die Dienstvorschriften nach den Absätzen 1 bis 3 bedürfen der Zustimmung des Bundeskanzleramtes.

§ 96

Unterrichtung des Parlamentarischen Kontrollgremiums und des Deutschen Bundestages

Der Bundesnachrichtendienst unterrichtet das Parlamentarische Kontrollgremium

1. regelmäßig über Maßnahmen nach § 37 Absatz 3,
2. unverzüglich über eine Grundanordnung nach § 50,
3. über die Dienstvorschriften des Bundesnachrichtendienstes nach § 95 Absatz 1 und 2.

§ 97

Kontrollgegenstände die der Vorabkontrolle unterliegen

(1) Anordnungen dürfen bei den folgenden Maßnahmen und ihren Verlängerungen erst mit Feststellung ihrer Rechtmäßigkeit durch den Unabhängigen Kontrollrat vollzogen werden:

1. Auskunftsersuchen nach § 13 Absatz 1 Satz 2, die sich gegen eine der in § 12 Absatz 2 Nummer 4 und 5 genannten Stellen richten, sofern es sich nicht um Auskunftsersuchen handelt, die der Durchführung von Maßnahmen dienen, deren Rechtmäßigkeit bereits vom Unabhängigen Kontrollrat festgestellt wurde,
2. Auskunftsersuchen nach § 14 Absatz 2,
3. Betreten einer Wohnung nach § 18 Absatz 2 zur Vorbereitung und Durchführung eines nachrichtendienstlichen Mittels,
4. besonderer Einsatz nachrichtendienstlicher Mittel nach § 19 Absatz 1 oder 2,
5. eingriffsintensiver Einsatz nachrichtendienstlicher Verbindungen nach § 24 Absatz 2,
6. Nutzung einer Legende auf vertiefter Vertrauensbasis nach § 25 Absatz 2,
7. Einsatz technischer Mittel zur längerfristigen Standortfeststellung nach § 26 Absatz 2 Nummer 2,
8. längerfristige optische und akustische Überwachung nach § 27 Absatz 2 Nummer 2,
9. Öffnen von Post- und Warensendungen nach § 28 Absatz 2 Satz 1,
10. Verzicht auf die Kennzeichnung bei Übermittlung nach § 29 Absatz 7 oder § 64 Absatz 4 Satz 3,
11. strategische Aufklärungsmaßnahmen nach § 32 Absatz 1,
12. Einsichtnahme in kommunikationsbezogene Inhaltsdaten, die im Wege der strategischen Aufklärung erhoben wurden, sofern die für die Einsichtnahme verwendeten Suchbegriffe

    a) Einrichtungen der Europäischen Union oder öffentlichen Stellen der Mitgliedstaaten der Europäischen Union nach § 47 Absatz 4 Satz 1 zugeordnet werden, oder

b) Personen zugeordnet sind, deren Kommunikation einen besonderen Vertraulichkeitsschutz nach § 22 genießt,

13. Telekommunikationsüberwachung nach § 35 Absatz 2,

14. Erhebung von gespeicherten Daten aus informationstechnischen Systemen nach § 37 Absatz 2 oder 3,

15. abgegrenzte Erhebung von gespeicherten Daten aus informationstechnischen Systemen nach § 38 Absatz 2,

16. besondere Maßnahme zur Sicherung von Verschlusssachen nach § 119.

(2) Der Bundesnachrichtendienst hat dem Unabhängigen Kontrollrat zur unabhängigen Vorabkontrolle der Rechtmäßigkeit Grundanordnungen nach § 50 und deren Verlängerungen vorzulegen.

(3) Der Bundesnachrichtendienst hat dem Unabhängigen Kontrollrat folgende Kontrollgegenstände unverzüglich zur Einzelfallkontrolle vorzulegen:

1. die Weiterverarbeitung oder Übermittlung von personenbezogenen Daten aus Vertraulichkeitsbeziehungen nach § 22 Absatz 3,

2. die Weiterverarbeitung oder Übermittlung von Aufzeichnungen aus der Wohnraumüberwachung nach § 29 Absatz 4,

3. qualifizierte Aufklärungsbedarfe bei der Verarbeitung von unselektierten Metadaten im Rahmen von Kooperationen des Bundesnachrichtendienstes mit ausländischen Nachrichtendiensten nach § 44 Absatz 2,

4. die Erstreckung einer Maßnahme auf weitere Personen auf Grundlage eines Zusatzes nach § 46 Absatz 5 oder § 48 Absatz 4 Satz 1 oder auf weitere Rufnummern oder Anschlüsse auf Grundlage eines Zusatzes nach § 48 Absatz 4 Satz 2,

5. eine Weiterverarbeitung oder Übermittlung von personenbezogenen Daten aus informationstechnischen Speichern nach § 54 Absatz 2 Nummer 2,

6. Dienstvorschriften des Bundesnachrichtendienstes nach

   a) § 95 Absatz 1 Satz 1, soweit sie den Katalog der nachrichtendienstlichen Mittel zur Erhebung personenbezogener Daten betreffen, und

   b) § 95 Absatz 2, soweit sie Regelungen zur Auswertung von Daten betreffen, sowie

7. die Nichtmitteilung nach § 100 Absatz 4 Satz 1 Nummer 4 und 5, weitere Zurückstellung der Mitteilung nach § 101 Absatz 2 und endgültige Nichtmitteilung nach § 101 Absatz 3.

Stellt der Unabhängige Kontrollrat fest, dass eine Erstreckung einer Maßnahme auf weitere Personen oder Rufnummern nach Satz 1 Nummer 4 unzulässig war, so sind bereits erhobene personenbezogene Daten unverzüglich zu löschen. Die Löschung unterbleibt, soweit ein Antrag die Daten für eine Mitteilung an Betroffene oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Anordnung oder des Vorgangs von Bedeutung sein können. In diesem Fall ist die Verarbeitung der Daten einzuschränken; sie dürfen nur zu diesen Zwecken verwendet werden.

(4) Der Unabhängige Kontrollrat ist bei Errichtungsanordnungen nach § 61 Absatz 3 und § 90 Absatz 2 und § 94 Absatz 1 vor Erlass der Anordnung anzuhören. Das

Anhörungsverfahren zur Errichtungsanordnung beginnt auch mit der Übermittlung einer Sofortanordnung. Bei gemeinsamen Dateien nach § 93 Absatz 1 erstreckt sich die Prüfkompetenz des Unabhängigen Kontrollrates nur auf die Errichtung der gemeinsamen Datei durch den Bundesnachrichtendienst sowie die auf von diesem in die gemeinsame Datei eingegebenen Daten.

(5) Würde anderenfalls der Zweck der Maßnahme vereitelt oder wesentlich erschwert, kann die durch die Behördenleitung oder durch von ihr bestimmte Vertretung bereits vor Feststellung der Rechtmäßigkeit nach Absatz 1 die vorläufige Vollziehbarkeit nach Maßgabe von § 31 des UKRat-Gesetzes anordnen.

(6) Die Anordnung einer Maßnahme der Wohnraumüberwachung nach § 29 Absatz 2 darf erst vollzogen werden, wenn das Bundesverwaltungsgericht deren Rechtmäßigkeit festgestellt hat. Absatz 5 ist entsprechend anzuwenden.

(7) Beteiligter des Feststellungsverfahrens nach Absatz 6 ist der Bundesnachrichtendienst. Er legt dem Bundesverwaltungsgericht die Anordnung vor. Stehen besondere Gründe des Geheimschutzes der Vorlage an das Bundesverwaltungsgericht entgegen, wird die Vorlage dadurch bewirkt, dass die Anordnung dem Bundesverwaltungsgericht in vom Bundesnachrichtendienst bestimmten Räumlichkeiten zur Verfügung gestellt wird. Das Bundesverwaltungsgericht kann den Sachverhalt durch Anhörung des Bundesnachrichtendienstes erforschen. Mit Einverständnis des Bundesnachrichtendienstes kann der Vorsitzende oder Berichterstatter anstelle des Senats entscheiden. Gegen eine nach Satz 5 getroffene Entscheidung steht dem Bundesnachrichtendienst innerhalb von zwei Wochen nach Bekanntgabe die Beschwerde zu, auf die der Senat entscheidet. Das Verfahren des Bundesverwaltungsgerichts unterliegt den Vorschriften des materiellen Geheimschutzes. Die Mitglieder des Bundesverwaltungsgerichts sind zur Geheimhaltung verpflichtet. Für das nichtrichterliche Personal gelten die Regelungen des personellen Geheimschutzes.

§ 98

Unabhängige Kontrolle durch den Unabhängigen Kontrollrat und die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Der Bundesnachrichtendienst wird bei der Erfüllung seiner Aufgaben nach diesem Gesetz, einschließlich der technischen und operativen Fachunterstützung, unter Anwendung der Vorschriften dieses Gesetzes durch den Unabhängigen Kontrollrat kontrolliert. Das Nähere der Kontrolle regelt § 1 des UKRat-Gesetzes.

(2) Der Bundesnachrichtendienst wird bei der Verarbeitung personenbezogener Daten bei der allgemeinen Verwaltung, der Aus- und Fortbildung und soweit dies durch andere Rechtsvorschriften ausdrücklich bestimmt ist durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kontrolliert.

(3) Der Bundesnachrichtendienst ist verpflichtet, die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und ihre oder seine schriftlich besonders Beauftragten bei der Erfüllung ihrer oder seiner Aufgaben nach Absatz 2 zu unterstützen. Den in Satz 1 genannten Personen ist dabei

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 2 stehen,

2. Zutritt in alle Diensträume zu gewähren.

Dies gilt nicht, soweit das Bundeskanzleramt im Einzelfall feststellt, dass die Auskunft, die Einsicht oder der Zutritt die Sicherheit des Bundes oder eines Landes gefährden würde.

§ 99

Anwendung anderer Gesetze

(1) Bei der Erfüllung der Aufgaben des Bundesnachrichtendienstes ist das Bundesdatenschutzgesetz wie folgt anzuwenden:

1. von den Teilen 1 und 4 des Bundesdatenschutzgesetzes

   a) finden § 1 Absatz 8, § 4, § 16 Absatz 1 und 3 bis 5, die §§ 17 bis 21 sowie § 85 keine Anwendung,

   b) findet § 14 Absatz 2 mit der Maßgabe Anwendung, dass sich die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nur an die Bundesregierung sowie das Parlamentarisches Kontrollgremium, das Vertrauensgremium und den Unabhängigen Kontrollrat wenden darf; eine Befassung der für die Kontrolle des Bundesnachrichtendienstes zuständigen Gremien setzt voraus, dass sie oder er der Bundesregierung entsprechend § 16 Absatz 2 Satz 1 des Bundesdatenschutzgesetzes zuvor Gelegenheit gegeben hat, innerhalb einer von ihr oder ihm gesetzten Frist Stellung zu nehmen;

2. von Teil 3 des Bundesdatenschutzgesetzes sind die §§ 46, 49, 50, 51 Absatz 1 bis 4 sowie die §§ 52 bis 54, 62, 64, 83, 84 entsprechend anzuwenden.

(2) Die §§ 4 bis 17 des Bundeswehrbeschaffungsbeschleunigungsgesetzes finden entsprechende Anwendung auf öffentliche Aufträge zur Deckung der Bedarfe des Bundesnachrichtendienstes, auch wenn diese durch öffentliche Stellen, wie die Bundesanstalt für Immobilienaufgaben, vergeben werden und auch wenn deren geschätzter Auftrags- oder Vertragswert ohne Umsatzsteuer die Schwellenwerte nach § 106 Absatz 2 des Gesetzes gegen Wettbewerbsbeschränkungen erreicht oder überschreitet. § 145 des Gesetzes gegen Wettbewerbsbeschränkungen bleibt unberührt.

Unterabschnitt 2

Mitteilung und Auskunftsverpflichtung

§ 100

Mitteilung an betroffene Personen

(1) Erhebt der Bundesnachrichtendienst personenbezogene Daten durch die nachfolgend genannten Maßnahmen, so hat er dies den betroffenen Personen nach Beendigung der Maßnahme mitzuteilen:

1. Auskunftsersuchen

   a) nach § 13 Absatz 1 Satz 2, die sich gegen eine der in § 12 Absatz 2 Nummer 4 und 5 genannten Stellen richten, sofern es sich nicht um Auskunftsersuchen handelt, die der Durchführung von Maßnahmen dienen, die

bereits für sich genommen eine Mitteilung an den Betroffenen nach sich ziehen, und

b) nach § 14 Absatz 2,

2. Maßnahmen, die nur zulässig sind, wenn tatsächliche Anhaltspunkte dafür bestehen, dass sie erforderlich sind, um Informationen zu Bedrohungen von herausgehobener Bedeutung zu erlangen, sowie

3. Maßnahmen nach § 29 Absatz 2, § 36 Absatz 1 und § 37 Absatz 3.

(2) Nimmt der Bundesnachrichtendienst nach § 34 Einsicht in kommunikationsbezogene Inhaltsdaten, die im Wege der strategischen Aufklärung erhoben wurden, so hat er dies den betroffenen Personen mitzuteilen, wenn die Einsichtnahme zu einer Weiterverarbeitung der Daten geführt hat.

(3) Eine Mitteilungspflicht nach den Absätzen 1 und 2 besteht nur gegenüber

1. deutschen Staatsangehörigen,

2. inländischen juristischen Personen und

3. sich nicht nur vorübergehend im Bundesgebiet aufhaltenden Personen.

Eine Mitteilungspflicht nach Absatz 1 besteht darüber hinaus nur gegenüber Personen, gegen die die Maßnahme gerichtet war.

(4) Abweichend von den Absätzen 1 und 2 besteht eine Mitteilungspflicht nicht, wenn

1. eine Maßnahme zur Aufklärung einer Bedrohung erfolgte, bei der Tatsachen vorliegen, welche die Annahme rechtfertigen, dass die Bedrohung von einer fremde Macht ausging oder von einer fremden Macht gesteuert wurde und dies nicht vollständig ausgeschlossen werden kann,

2. in den Fällen des Absatzes 1 Nummer 2 und 3 die Maßnahme unter Einsatz einer nachrichtendienstlichen Verbindung im Sinne des § 23 Absatz 1 erfolgte,

3. in den Fällen des Absatzes 2 die personenbezogenen Daten unverzüglich nach Einsichtnahme gelöscht oder unkenntlich gemacht wurden, wobei die Unkenntlichmachung auch dergestalt erfolgen kann, dass die Eindeutigkeit der Daten erhalten bleiben darf, und eine rückwirkende Identifizierung der Person unmöglich oder nur mit unvertretbar hohem Aufwand möglich ist,

4. aufgrund der Umstände des jeweiligen Einzelfalls zum Schutz von besonders gewichtigen Rechtsgütern bereits zum Zeitpunkt der Begründung der Mitteilungspflicht mit an Sicherheit grenzender Wahrscheinlichkeit vorauszusehen ist, dass eine Nichtmitteilung dauerhaft geboten und verhältnismäßig ist, insbesondere, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass einer der in § 101 Absatz 1 genannten Zurückstellungsgründe dauerhaft vorliegen wird,

5. tatsächliche Anhaltspunkte dafür bestehen, dass eine Mitteilung für den Betroffenen mit nachteiligen Folgen verbunden wäre, oder

6. die betroffene Person nicht identifiziert werden kann und auch in der Zukunft eine Identifikation mit an Sicherheit grenzender Wahrscheinlichkeit nicht erfolgen kann.

In den Fällen der Nummern 4 und 5 bedarf die Nichtmitteilung der Zustimmung des Unabhängigen Kontrollrats.

(5) Die Mitteilung nach den Absätzen 1 bis 2 obliegt dem Bundesnachrichtendienst. Wurden die personenbezogenen Daten übermittelt, erfolgt die Mitteilung im Benehmen mit der empfangenden Stelle.

§ 101

Zurückstellung der Mitteilung

(1) Die Mitteilung nach § 100 Absatz 1 bis 2 kann zurückgestellt werden, solange

1. eine Gefährdung des Zwecks der Maßnahme nicht ausgeschlossen werden kann,

2. der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist.

(2) Erfolgt die nach Absatz 1 zurückgestellte Mitteilung nicht binnen zwölf Monaten nach Beendigung der Maßnahme oder nach Einsichtnahme und Weiterverarbeitung in die im Wege der strategischen Aufklärung erhobenen personenbezogenen Daten, so bedarf die weitere Zurückstellung der Zustimmung des Unabhängigen Kontrollrates. Der Unabhängige Kontrollrat bestimmt die Dauer der weiteren Zurückstellung.

(3) Nach Ablauf von fünf Jahren nach Beendigung der Maßnahme kann mit Zustimmung des Unabhängigen Kontrollrats endgültig von einer Mitteilung abgesehen werden, wenn

1. eine der Voraussetzungen des Absatzes 1 auch fünf Jahre nach Beendigung der Maßnahme noch vorliegt und

2. mit an Sicherheit grenzender Wahrscheinlichkeit zu erwarten ist, dass sie auch in Zukunft vorliegt.

§ 102

Auskunft an betroffene Personen

(1) Der Bundesnachrichtendienst erteilt einer betroffenen Person über Daten, die zu ihrer Person in einer Personendatenbank gespeichert sind, auf Antrag unentgeltlich Auskunft, soweit die betroffene Person hierzu einen konkreten Sachverhalt benennt und ein besonderes Interesse an einer Auskunft darlegt. Die Auskunft erstreckt sich auch auf solche Daten, die über eine Speicherung in einer Personendatenbank auffindbar sind. Auf andere als die in Satz 1 und Satz 2 genannten Daten erstreckt sich die Auskunft nur, wenn die betroffene Person Angaben macht, die das Auffinden der Daten in einem unter Berücksichtigung ihres Informationsinteresses angemessenen Aufwand eindeutig ermöglicht..

(2) Die Auskunft erstreckt sich nicht auf

1. die Herkunft der Daten und die Empfänger von Übermittlungen,

2. Daten, bei deren Weitergabe die Gefahr besteht, dass nachrichtendienstliche Verbindungen offengelegt würden, und

3. Daten bei deren Offenlegung eine Gefährdung operativer Vorgänge oder der Funktions- und Kooperationsfähigkeit des Bundesnachrichtendienstes zu besorgen ist.

(3) Die Auskunftserteilung unterbleibt, soweit

1. eine Gefährdung der Aufgabenerfüllung des Bundesnachrichtendienstes durch die Auskunftserteilung zu besorgen ist,

2. durch die Auskunftserteilung nachrichtendienstliche Verbindungen gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise des Bundesnachrichtendienstes zu befürchten ist,

3. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder

4. die Daten oder die Tatsache der Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.

(4) Die Entscheidung über das Unterbleiben einer Auskunftserteilung trifft die Behördenleitung des Bundesnachrichtendienstes oder eine von ihr besonders beauftragte Mitarbeiterin oder ein von ihr besonders beauftragter Mitarbeiter.

(5) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung, soweit dadurch der Zweck der Auskunftsverweigerung gefährdet würde. Die Gründe der Auskunftsverweigerung sind aktenkundig zu machen. Wird die Auskunftserteilung abgelehnt, ist die betroffene Person auf die Rechtsgrundlage für das Fehlen der Begründung und darauf hinzuweisen, dass sie sich an den Unabhängigen Kontrollrat wenden kann. Dem Unabhängigen Kontrollrat ist auf sein Verlangen Auskunft über die Ablehnung und die Gründe hierfür zu erteilen, soweit es sich nicht um Informationen nach § 13 Absatz 4 des UKRat-Gesetzes handelt. Mitteilungen des Unabhängigen Kontrollrates an die betroffene Person dürfen keine Rückschlüsse auf den Erkenntnisstand des Bundesnachrichtendienstes zulassen, sofern der Bundesnachrichtendienst nicht einer weitergehenden Auskunft zustimmt.

(6) Ein Recht auf Akteneinsicht besteht nicht.

§ 103

Rechtswegausschluss

Der Rechtsweg vor der Mitteilung an die betroffene Person ist ausgeschlossen gegen

1. die Anordnung und den Vollzug von Auskunftsersuchen nach § 13 Absatz 1 Satz 2 gegen die in § 12 Absatz 2 Nummer 4 und 5 genannten Stellen,

2. die Anordnung und den Vollzug von strategischen Aufklärungsmaßnahmen nach § 32 und

3. die Anordnung und den Vollzug von Maßnahmen der Telekommunikationsüberwachung nach § 35.

Abschnitt 8

Besondere Bestimmungen zur Sicherung der Bediensteten, Dienststellen und Verschlusssachen

Unterabschnitt 1

Begriffsbestimmungen und allgemeine Vorgaben

§ 104

Begriffsbestimmungen zur Sicherung der Bediensteten, Dienststellen und Verschlusssachen

Es bezeichnen die Begriffe:

1. „Dienststellen des Bundesnachrichtendienstes“ die Grundstücke, Gebäude, Gebäudeteile, Anlagen und sonstigen Einrichtungen des Bundesnachrichtendienstes sowie die nach § 106 Absatz 1 vorübergehend zu besonderen Sicherheitsbereichen erklärten Örtlichkeiten;

2. „qualifiziert funktionsgefährdende Tätigkeiten“ ein

   a) mit Strafe bedrohtes Handeln, das sich gegen Bedienstete des Bundesnachrichtendienstes während der rechtmäßigen Ausübung ihres Dienstes richtet, wenn die Handlungen darauf abzielen, die Ausübung des Dienstes zu stören, oder tätliche Angriffe sind,

   b) mit Strafe bedrohtes Handeln, das sich gezielt gegen Dienststellen oder Gegenstände des Bundesnachrichtendienstes richtet,

   c) mit Strafe bedrohtes Handeln, das einen unmittelbaren Bezug zu sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten aufweist,

   d) unzulässiger Betrieb unbemannter Fluggeräte nach § 21h Absatz 3 Nummer 4 der Luftverkehrs-Ordnung;

3. „Kontrolle“ die oberflächliche Suche nach Gegenständen an Personen, an oder in Taschen, mitgeführten Gegenständen und Fahrzeugen sowie in Räumen, auch unter Einsatz technischer Mittel zum Auffinden von Geräten der Informations- und Kommunikationstechnik, ohne dass ein Körperkontakt mit der betroffenen Person erfolgt;

4. „Durchsuchung“ die zielgerichtete und planmäßige Suche, auch unter Einsatz technischer Mittel,

   a) am äußeren Körper der betroffenen Person,

   b) in Kleidung und Taschen der betroffenen Person,

   c) an und in Fahrzeugen einschließlich dort befindlicher Gegenstände der betroffenen Person,

   d) in Räumen einschließlich dort befindlicher Gegenstände oder

e) in sonstigen Gegenständen der betroffenen Person, die zur Verbringung von Verschlusssachen geeignet sind;

5. „Sicherung von Verschlusssachen“ das Erkennen und Verhindern, dass

a) Geräte der Informations- und Kommunikationstechnik sowie sonstige Gegenstände, die geeignet sind, Verschlusssachen auszubringen, zu zerstören, zu verändern, zu verarbeiten, zu kopieren, unbrauchbar zu machen oder Sabotagehandlungen vorzunehmen, in Dienststellen des Bundesnachrichtendienstes unbefugt eingebracht werden oder

b) Verschlusssachen aus Dienststellen des Bundesnachrichtendienstes unbefugt ausgebracht werden;

6. „unmittelbarer Zwang“ die Einwirkung auf Personen oder Sachen durch körperliche Gewalt, ihre Hilfsmittel und durch Waffen sowie, in den Fällen des § 112 Absatz 2, der Einsatz geeigneter Mittel gegen das Fluggerät, dessen Steuerungseinheit oder Steuerungsverbindung.

§ 105

Allgemeine Vorgaben

(1) Widerspruch und Anfechtungsklage gegen die in den Unterabschnitten 2 und 3 genannten Maßnahmen haben keine aufschiebende Wirkung.

(2) Die Regelungen zur Mitbestimmung in § 80 Absatz 1 Nummer 18 und 21 des Personalvertretungsgesetzes sind nicht anzuwenden auf Regelungen oder technische Einrichtungen zur Sicherung von Bediensteten, Dienststellen oder Verschlusssachen des Bundesnachrichtendienstes.

§ 106

Besondere Sicherheitsbereiche

(1) Der Bundesnachrichtendienst kann andere Örtlichkeiten vorübergehend zu besonderen Sicherheitsbereichen erklären und sperren, soweit und solange

1. dies unter Berücksichtigung der Interessen der Allgemeinheit aus Gründen der Sicherheit zur Erfüllung dienstlicher Aufgaben des Bundesnachrichtendienstes unerlässlich ist und

2. das Bundeskanzleramt der vorübergehenden Einrichtung des besonderen Sicherheitsbereichs zugestimmt hat.

Bei Gefahr im Verzug findet Satz 1 Nummer 2 keine Anwendung. In diesem Fall ist das Bundeskanzleramt nachträglich über die vorübergehende Einrichtung des besonderen Sicherheitsbereiches zu unterrichten.

(2) Wird durch die vorübergehende Sperrung einer Örtlichkeit nach Absatz 1 die gewöhnliche Nutzung des betroffenen Grundstücks derart beeinträchtigt, dass dadurch eine Ertragsminderung oder ein sonstiger Nutzungsausfall verursacht wird, so ist eine Entschädigung in Geld zu gewähren, die diesen Nachteil angemessen ausgleicht. § 20 Absatz 2 des Gesetzes über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und verbündeter Streitkräfte sowie zivile

Wachpersonen gilt entsprechend mit der Maßgabe, dass an die Stelle der Wehrbereichsverwaltung der Bundesnachrichtendienst tritt.

§ 107

Öffentliche Hinweispflichten

Sind Dienststellen offen als solche des Bundesnachrichtendienstes erkennbar, so hat der Bundesnachrichtendienst die Öffentlichkeit durch Beschilderung darauf hinzuweisen,

1. dass eine Örtlichkeit vorübergehend zu einem besonderen Sicherheitsbereich erklärt und gesperrt wird und

2. dass der Einsatz von Maßnahmen des unmittelbaren Zwangs bei qualifiziert funktionsgefährdenden Tätigkeiten in dieser Dienststelle und in unmittelbarer Nähe zu dieser Dienststelle möglich ist.

Unterabschnitt 2

Befugnisse zur Sicherung der Bediensteten und Dienststellen

§ 108

Betroffene Personen

Die Befugnisse zur Sicherung der Bediensteten und Dienststellen des Bundesnachrichtendienstes mit Ausnahme der Befugnisse in §§ 112 und 113 dürfen sich nur richten gegen Personen,

1. die sich in einer Dienststelle des Bundesnachrichtendienstes aufhalten,

2. die eine Dienststelle des Bundesnachrichtendienstes betreten wollen,

3. die unmittelbar nach dem Verlassen einer Dienststelle des Bundesnachrichtendienstes oder dem Versuch, die Dienststelle zu betreten, verfolgt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Personen nicht berechtigt sind, sich in der Dienststelle des Bundesnachrichtendienstes aufzuhalten,

4. die sich in unmittelbarer Nähe zu einer Dienststelle des Bundesnachrichtendienstes aufhalten, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Personen eine qualifiziert funktionsgefährdende Tätigkeit planen, begehen oder begangen haben.

§ 109

Personenüberprüfung

(1) Der Bundesnachrichtendienst darf zur Sicherung seiner Bediensteten und Dienststellen die Identität einer Person feststellen.

(2) Der Bundesnachrichtendienst kann zur Feststellung der Identität die erforderlichen Maßnahmen treffen. Er kann die betroffene Person insbesondere anhalten, sie nach ihren Personalien befragen und verlangen, dass sie Ausweispapiere zur Prüfung aushändigt.

(3) Die betroffene Person kann vorübergehend festgehalten und zu einer hierfür durch die Behördenleitung des Bundesnachrichtendienstes bestimmten Person gebracht werden, wenn ihre Identität auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann. Die Person ist in diesem Fall sofort zu überprüfen. Unter den Voraussetzungen des Satzes 1 können die betroffene Person sowie die von ihr mitgeführten Sachen nach Gegenständen, die der Identitätsfeststellung dienen, durchsucht werden. Personen dürfen nur von Personen gleichen Geschlechts oder von Ärzten durchsucht werden; dies gilt nicht, wenn die sofortige Durchsuchung zum Schutz gegen eine Gefahr für Leib oder Leben erforderlich ist.

§ 110

Durchsuchung, Sicherstellung und Beschlagnahme

(1) Der Bundesnachrichtendienst darf zur Sicherung seiner Bediensteten und Dienststellen eine Person durchsuchen, wenn tatsächliche Anhaltspunkte bestehen, dass

1. diese Person eine qualifiziert funktionsgefährdende Tätigkeit plant, begeht oder begangen hat und

2. die Durchsuchung zur Auffindung von Gegenständen führt, die durch eine qualifiziert funktionsgefährdende Tätigkeit hervorgebracht wurden oder zur Begehung einer solchen Tätigkeit geeignet sind.

(2) Im Gewahrsam einer durchsuchten Person stehende Gegenstände können sichergestellt oder vorläufig beschlagnahmt werden, wenn tatsächliche Anhaltspunkte vorliegen, dass sie durch eine qualifiziert funktionsgefährdende Tätigkeit hervorgebracht oder zur Begehung einer solchen Tätigkeit geeignet sind. Die §§ 96, 97 und 110 Absatz 1 und 2 der Strafprozessordnung sind entsprechend anzuwenden.

(3) Sichergestellte oder beschlagnahmte Gegenstände sind unverzüglich, spätestens binnen drei Tagen, der Polizei oder der Staatsanwaltschaft zu übergeben. Die Pflicht zur Weitergabe dieser Gegenstände entfällt, wenn sie der überprüften Person vor Ablauf der Frist zurückgegeben oder zur Verfügung gestellt werden. Gleiches gilt, wenn über diese Gegenstände der Bundesnachrichtendienst zu verfügen hat. In diesem Fall ist der Polizei oder der Staatsanwaltschaft ein Verzeichnis dieser Gegenstände zu übersenden.

§ 111

Erweiterte Befugnisse bei qualifiziert funktionsgefährdenden Tätigkeiten

(1) Der Bundesnachrichtendienst kann eine Person, wenn tatsächliche Anhaltspunkten dafür vorliegen, dass sie eine qualifiziert funktionsgefährdende Tätigkeit plant, begeht oder begangen hat,

1. vorübergehend aus der unmittelbaren Nähe zu einer Dienststelle des Bundesnachrichtendienstes verweisen oder

2. vorübergehend das Betreten des Bereichs der unmittelbaren Nähe zu einer Dienststelle des Bundesnachrichtendienstes verbieten.

(2) Eine Person kann bei Gefahr im Verzug von einer durch die Behördenleitung des Bundesnachrichtendienstes bestimmten Person kurzzeitig festgehalten werden, wenn

1. dies unerlässlich ist, um die unmittelbar bevorstehende Begehung oder Fortsetzung einer qualifiziert funktionsgefährdenden Tätigkeit zu verhindern, oder

2. die betroffene Person

   a) bei einer qualifiziert funktionsgefährdenden Tätigkeit auf frischer Tat betroffen oder verfolgt wird, oder

   b) einer qualifiziert funktionsgefährdenden Tätigkeit dringend verdächtig ist.

Die zuständige Polizeibehörde ist unverzüglich zu informieren. Die Person darf nur solange festgehalten werden, bis eine Überstellung an die zuständige Polizeibehörde möglich ist. Die §§ 40 bis 42 des Bundespolizeigesetzes entsprechende Anwendung.

§ 112

Maßnahmen gegen den unbefugten Betrieb unbemannter Fluggeräte

(1) Der Bundesnachrichtendienst darf unbemannte Fluggeräte im Umfeld der von ihm eingesetzten Personen sowie seiner Dienststellen und besonderen Sicherheitsbereiche aufklären. Liegen tatsächliche Anhaltspunkte vor, dass ein unbemanntes Fluggerät für eine qualifiziert funktionsgefährdende Tätigkeit genutzt wird, darf der Bundesnachrichtendienst die Maßnahmen nach den §§ 109, 110 und 111 Absatz 2 gegen die Person anwenden, welche das unbemannte Fluggerät steuert, sofern geeignete polizeiliche Hilfe nicht oder nicht rechtzeitig erlangt werden kann.

(2) Der Bundesnachrichtendienst darf unbemannte Fluggeräte abwehren

1. bei Annäherung auf 100 Meter zu den von ihm eingesetzten Personen, seinen Dienststellen,

2. bei Eindringen in das geografische Gebiet der Dienststellen des Bundesnachrichtendienstes nach § 21h Absatz 3 Nummer 4 der Luftverkehrs-Ordnung oder

3. wenn tatsächliche Anhaltspunkte dafür vorliegen, dass sie für eine qualifiziert funktionsgefährdende Tätigkeit genutzt werden.

(3) Der Bundesnachrichtendienst darf ein nach Absatz 2 abgewehrtes Fluggerät sicherstellen und untersuchen.

§ 113

Einsatzsicherung

(1) Der Bundesnachrichtendienst darf zum Schutz von Leben, körperlicher Unversehrtheit oder Freiheit seiner Bediensteten und anderer Personen, die für ihn tätig sind, sowie zum Schutz eingesetzter Sachen von bedeutendem Wert erforderliche Maßnahmen durchführen, um eine gegenwärtige Gefahr abzuwehren, die im Rahmen des Einsatzes nachrichtendienstlicher Mittel nach den Abschnitten 3 und 4 auftritt. Satz 1 ist auch anzuwenden, wenn die Bediensteten des Bundesnachrichtendienstes während des Einsatzes nachrichtendienstlicher Mittel eine solche Gefahr für Leben, körperliche Unversehrtheit oder Freiheit von Dritten feststellen.

(2) Sind Personen, die für den Bundesnachrichtendienst tätig sind, zur heimlichen Informationsgewinnung in im Bundesgebiet befindlichen Wohnungen eingesetzt, darf der

Bundesnachrichtendienst im Beisein der eingesetzten Personen oder im unmittelbaren zeitlichen Zusammenhang mit dem Einsatz personenbezogene Daten heimlich mit technischen Mitteln aus der Wohnung nur erheben und aufzeichnen, soweit dies zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person unerlässlich ist.

(3) Der Bundesnachrichtendienst darf die nach Absatz 2 erhobenen personenbezogenen Daten nach den in den Abschnitten 5 und 6 getroffenen Bestimmungen nur weiterverarbeiten und übermitteln

1. zu den in Absatz 2 genannten Zwecken,

2. zur Gefahrenabwehr und

3. zur Strafverfolgung.

§ 114

Anordnung von Maßnahmen zur Sicherung der Bediensteten und Dienststellen

(1) Maßnahmen nach den §§ 109 bis 113, mit Ausnahme von Maßnahmen nach § 109 Absatz 1 und 2, bedürfen der Anordnung durch die Behördenleitung des Bundesnachrichtendienstes oder durch eine von ihr bestimmte Vertretung, die die Befähigung zum Richteramt hat. Die Anordnung ist durch den Bundesnachrichtendienst zu dokumentieren. In der Anordnung sind anzugeben:

1. Art und Beschreibung der Maßnahme,

2. die betroffenen Personen,

3. Anlass der Maßnahme,

4. bei Maßnahmen der Einsatzsicherung nach § 113 Absatz 2 die zu überwachende Wohnung oder die zu überwachenden Wohnräume und

5. Begründung der Maßnahme.

Bei Maßnahmen der Einsatzsicherung nach § 113 Absatz 2 ist die Anordnung auf höchstens einen Monat zu befristen.

(2) Ist eine Anordnung nach Absatz 1 Satz 1 auf Grund besonderer Eilbedürftigkeit nicht rechtzeitig zu erlangen, kann die Maßnahme auch ohne vorherige Anordnung durchgeführt werden, wenn ansonsten der Zweck der Maßnahme vereitelt oder wesentlich erschwert würde. Die Anordnung ist unverzüglich nachzuholen.

Unterabschnitt 3

Befugnisse zur Sicherung von Verschlusssachen

§ 115

Betroffene Personen; Mitwirkungspflicht; Belehrung

(1) Die Befugnisse zur Sicherung von Verschlusssachen mit Ausnahme des § 119 dürfen sich nur richten gegen

1. Bedienstete des Bundesnachrichtendienstes, die sich in den Dienststellen des Bundesnachrichtendienstes aufhalten,

2. Mitarbeiterinnen und Mitarbeitern anderer inländischer oder ausländischer öffentlicher Stellen, die sich in den Dienststellen des Bundesnachrichtendienstes aufhalten,

3. andere Personen, die sich mit Erlaubnis des Bundesnachrichtendienstes in seinen Dienststellen aufhalten, und

4. Personen, die sich nach dem Verlassen einer Dienststelle des Bundesnachrichtendienstes in unmittelbarer Nähe zu einer solchen Dienststelle aufhalten, wenn sie sich Maßnahmen nach den §§ 116 bis 118 entziehen oder entzogen haben.

(2) Die in Absatz 1 genannten Personen sind zur Mitwirkung bei der Durchführung von Maßnahmen zur Sicherung von Verschlusssachen verpflichtet.

(3) Der Bundesnachrichtendienst hat die in Absatz 1 genannten Personen in geeigneter Form zu belehren über

1. den ordnungsgemäßen Umgang mit Verschlusssachen,

2. die Möglichkeit, dass bei ihnen Maßnahmen nach den §§ 116 bis 118 durchgeführt werden können, sowie

3. ihre Pflicht zur Mitwirkung bei der Durchführung der Maßnahmen.

§ 116

Kontrolle und Durchsuchung von Personen, Taschen und Fahrzeugen zur Sicherung von Verschlusssachen

Zur Sicherung von Verschlusssachen darf der Bundesnachrichtendienst innerhalb seiner Dienststellen

1. verdachtsunabhängige Kontrollen von Personen, Taschen und Fahrzeugen sowie von mitgeführten Gegenständen, insbesondere an Ein- und Ausgängen, durchführen und

2. Durchsuchungen von Personen, Taschen und Fahrzeugen sowie mitgeführten Gegenständen vornehmen, wenn tatsächliche Anhaltpunkte dafür vorliegen, dass die Durchsuchung zur Sicherung von Verschlusssachen erforderlich ist.

§ 117

Kontrolle und Durchsuchung von Räumen zur Sicherung von Verschlusssachen

(1) Zur Sicherung von Verschlusssachen darf der Bundesnachrichtendienst innerhalb seiner Dienststellen

1. verdachtsunabhängige Kontrollen von Räumen durchführen und

2. Durchsuchungen von Räumen einschließlich der in den Räumen vorhandenen Gegenstände vornehmen, wenn Tatsachen die Annahme rechtfertigen, dass dies zur Sicherung von Verschlusssachen erforderlich ist.

(2) Zur Sicherung von Verschlusssachen darf der Bundesnachrichtendienst optisch-elektronische Einrichtungen zur offenen Überwachung seiner Dienststellen nach Maßgabe einer Dienstvorschrift einsetzen. In der Dienstvorschrift sind die Voraussetzungen, das Verfahren und die Grenzen der Maßnahme zu regeln. Eine Überwachung höchstpersönlich genutzter Räume ist unzulässig.

§ 118

IT-Kontrollen zur Sicherung von Verschlusssachen

(1) Zur Sicherung von Verschlusssachen darf der Bundesnachrichtendienst zu dienstlichen Zwecken überlassene Geräte der Informations- und Kommunikationstechnik herausverlangen.

(2) Zur Sicherung von Verschlusssachen darf der Bundesnachrichtendienst in Geräte der Informations- und Kommunikationstechnik, die einer Person zu privatdienstlichen Zwecken überlassen wurden, eingreifen sowie die auf den Geräten gespeicherten Informationen einschließlich personenbezogener Daten verarbeiten, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die betroffene Person eine der § 104 Nummer 2 Buchstabe c genannten Straftaten plant, begeht oder begangen hat. Die Maßnahme darf sich auch gegen Personen nach § 115 Absatz 1 richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie Informationen, die für die nach Satz 1 verdächtige Person bestimmt sind, entgegennehmen oder Informationen, die von der verdächtigen Person herrühren, für sie weitergeben. Die Sätze 1 und 2 gelten entsprechend für privatdienstliche Laufwerke und Programme, die sich auf Geräten nach Absatz 1 befinden. Der Bundesnachrichtendienst darf Geräte nach Satz 1 herausverlangen, um die in Satz 1 angegebenen Maßnahmen durchzuführen.

(3) Zur Sicherung von Verschlusssachen darf der Bundesnachrichtendienst Geräte der Informations- und Kommunikationstechnik, die eine Person vorschriftswidrig in Dienststellen des Bundesnachrichtendienstes eingebracht hat, sicherstellen oder, wenn die betroffene Person der Sicherstellung widerspricht, unverzüglich ein Abbild der auf dem Gerät gespeicherten Informationen einschließlich personenbezogener Daten zur Datensicherung erzeugen. Ein Eingriff in die sichergestellten Geräte sowie eine Verarbeitung der auf den Geräten gespeicherten oder durch ein erzeugtes Abbild erhobenen Informationen einschließlich personenbezogener Daten ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die betroffene Person eine Straftat nach Absatz 2 Satz 1 plant, begeht oder begangen hat. Die Maßnahme darf sich auch gegen Personen nach § 115 Absatz 1 richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie Informationen, die für die nach Satz 1 verdächtige Person bestimmt sind, entgegennehmen oder Informationen, die von der verdächtigen Person herrühren, für sie weitergeben. Ein Gerät ist nach spätestens 48 Stunden zurückzugeben und ein Abbild ist nach spätestens 48 Stunden zu löschen, wenn keine tatsächlichen Anhaltspunkte dafür bestehen, dass die betroffene

Person eine Straftat nach Absatz 2 Satz 1 plant, begeht oder begangen hat. Anderenfalls darf die Sicherstellung nach Satz 1 für die Dauer der sich daran anschließenden Datenerhebung, höchstens jedoch für zwei Wochen erfolgen; danach ist das Gerät unverzüglich an die betroffene Person herauszugeben. Das Gerät wird nicht an die betroffene Person herausgegeben, wenn es zur Einleitung eines strafrechtlichen Ermittlungsverfahrens an die Strafverfolgungsbehörden weitergegeben werden muss. In diesen Fällen richtet sich die Herausgabe nach den für das Ermittlungsverfahren geltenden Bestimmungen.

(4) Macht die betroffene Person in den Fällen des Absatzes 3 Gründe glaubhaft, dass für sie eine Aufrechterhaltung der Sicherstellung nicht zumutbar ist, so ist das Gerät der Informations- und Kommunikationstechnik innerhalb von 48 Stunden nach Darlegung der Gründe an die betroffene Person zurückzugeben. Der Bundesnachrichtendienst darf vor der Rückgabe ein Abbild der auf dem Gerät gespeicherten Informationen einschließlich personenbezogener Daten zur Datensicherung erzeugen.

(5) Werden in den Dienststellen des Bundesnachrichtendienstes Geräte der Informations- und Kommunikationstechnik aufgefunden, die keiner bestimmten Person zuzuordnen sind, darf der Bundesnachrichtendienst diese Geräte sicherstellen. Er hat geeignete Maßnahmen zu treffen, um die berechtigte Person ausfindig zu machen. Wenn die berechtigte Person nicht innerhalb von vier Wochen ausfindig gemacht werden kann, darf der Bundesnachrichtendienst in das Gerät mit technischen Mitteln eingreifen sowie die auf den Geräten gespeicherten Informationen einschließlich personenbezogener Daten so weit verarbeiten, wie es zur Ermittlung der berechtigten Person erforderlich ist. Wird die berechtigte Person ausfindig gemacht und kann das Gerät als dienstlich oder privatdienstlich zur Verfügung gestelltes oder als vorschriftswidrig eingebrachtes Gerät der Informations- und Kommunikationstechnik identifiziert werden, so gelten die Absätze 1 bis 3 entsprechend. Macht die berechtigte Person keine Angaben zum Gerät oder wird die berechtigte Person nicht ausfindig gemacht, so ist das Gerät

1. wie ein vorschriftenwidrig eingebrachtes Gerät der Informations- und Kommunikationstechnik nach Absatz 3 zu behandeln oder

2. für den Fall, dass der Bundesnachrichtendienst Kenntnis darüber hat, dass es sich um ein dienstliches oder privatdienstliches Gerät handelt, wie ein Gerät nach Absatz 1 oder Absatz 2 zu behandeln.

Die Frist nach Absatz 3 Satz 4 beginnt mit dem Zeitpunkt, zu dem der Bundesnachrichtendienst Kenntnis von der Identität der berechtigten Person hat.

(6) Maßnahmen nach den Absätzen 1 bis 3 dürfen auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(7) Bei Maßnahmen nach Absatz 3 und Absatz 5 Satz 3 gilt § 39 Absatz 3 entsprechend. Informationen, die mittels eines Abbildes der auf dem Gerät gespeicherten Informationen erhoben worden sind, hat der Bundesnachrichtendienst unverzüglich auf deren Relevanz zu prüfen; bestätigt sich der Verdacht einer Straftat nach Absatz 2 Satz 1 nicht, so ist das Abbild unverzüglich zu löschen.

(8) Der Bundesnachrichtendienst darf zum Zweck der Sicherstellung von Geräten der Informations- und Kommunikationstechnik in den Fällen des Absatzes 3 die betroffene Person durchsuchen, wenn diese das Gerät nicht freiwillig herausgibt.

§ 119

Besondere Maßnahmen zur Sicherung von Verschlusssachen

(1) Zur Sicherung seiner Verschlusssachen darf der Bundesnachrichtendienst in informationstechnische Systeme eingreifen, wenn der dringende Verdacht besteht, dass auf dem informationstechnischen System unbefugt Verschlusssachen oder geheimhaltungsbedürftige Informationen des Bundesnachrichtendienstes gespeichert werden.

(2) Der Bundesnachrichtendienst darf, wenn geeignete polizeiliche Hilfe nicht oder nicht rechtzeitig erlangt werden kann,

1. auf einem informationstechnischen System unbefugt gespeicherte Verschlusssachen oder geheimhaltungsbedürftige Informationen löschen und

2. personenbezogene Daten erheben, die geeignet erscheinen, die Umstände der Speicherung aufzuklären.

(3) Auf Maßnahmen nach Absatz 1 finden die §§ 21 und 22, § 39 Absatz 1 Satz 2, Absatz 2 und 3 und § 48 entsprechende Anwendung.

§ 120

Anordnung von Maßnahmen zur Sicherung von Verschlusssachen

(1) Es bedürfen der Anordnung durch

1. die oder den Geheimschutzbeauftragten des Bundesnachrichtendienstes oder einer von ihr oder ihm bestimmten Vertretung, die die Befähigung zum Richteramt hat: Maßnahmen nach den §§ 116 bis 118 mit Ausnahme von Kontrollen nach § 116 Nummer 1,

2. die Behördenleitung des Bundesnachrichtendienstes oder durch eine von ihr bestimmte Vertretung, die die Befähigung zum Richteramt hat: Maßnahmen nach den § 117 Absatz 2 und § 118 Absatz 3.

Die Anordnung sowie die im Rahmen der Maßnahmen nach Satz 1 erhobenen Informationen einschließlich personenbezogener Daten sind durch den Bundesnachrichtendienst zu dokumentieren.

(2) In der Anordnung sind anzugeben:

1. Art und Beschreibung der Maßnahme nach § 116 Nummer 2 oder nach den §§ 117 bis 118,

2. die betroffenen Personen,

3. Anlass der Maßnahme und

4. Begründung der Maßnahme.

In den Fällen des § 117 Absatz 1 Nummer 1 kann die Anordnung auch mehrere gleichgelagerte Maßnahmen innerhalb eines in der Anordnung definierten Zeitraums, der nicht länger als sechs Monate sein darf, umfassen.

(3) Ist eine Anordnung nach Absatz 1 Satz 1 auf Grund besonderer Eilbedürftigkeit nicht rechtzeitig zu erlangen, kann die Maßnahme auch ohne vorherige Anordnung durchgeführt werden, wenn ansonsten der Zweck der Maßnahme vereitelt oder wesentlich

erschwert würde. In den Fällen des § 118 Absatz 2 bis 3 und 5 darf jedoch lediglich das Herausgabeverlangen sowie die Sicherstellung des Gerätes der Informations- und Kommunikationstechnik ohne vorherige Anordnung erfolgen. Die Anordnung ist unverzüglich nachzuholen. Wird die Anordnung nach Absatz 1 nicht nachgeholt, so hat der Bundesnachrichtendienst die bereits erhobenen Daten unverzüglich zu löschen und sichergestellte Gegenstände an die betroffene Person herauszugeben.

Unterabschnitt 4

Durchführung von Maßnahmen

§ 121

Vorgaben zur Durchführung von Maßnahmen durch unmittelbaren Zwang

(1) Maßnahmen nach den Unterabschnitten 2 und 3, die auf die Herausgabe einer Sache oder auf die Vornahme einer Handlung oder auf Duldung gerichtet sind, kann der Bundesnachrichtendienst durch unmittelbaren Zwang durchsetzen. Unmittelbarer Zwang darf nur angewendet werden entsprechend den §§ 4, 5, 8 und 10 Absatz 1 Nummer 1 und 2 sowie den §§ 12 bis 14 des Gesetzes über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes. § 6 Absatz 2 und § 18 Absatz 2 des Verwaltungs-Vollstreckungsgesetzes sind entsprechend anzuwenden. Die Anwendung eines Zwangsmittels darf nur durch besonders qualifizierte und geschulte Personen erfolgen, die durch die Behördenleitung des Bundesnachrichtendienstes oder durch eine von ihr bestimmte Vertretung hierzu besonders ermächtigt wurden.

(2) Unmittelbarer Zwang darf nur angewandt werden, wenn dies den Umständen nach erforderlich ist und geschieht

1. zur Sicherung der Bediensteten und Dienststellen des Bundesnachrichtendienstes durch Maßnahmen nach Unterabschnitt 2,

2. zur Sicherung von Verschlusssachen durch Maßnahmen nach Unterabschnitt 3, wobei bei Kontrollen nach § 116 Nummer 1 an Eingängen der Einsatz unmittelbaren Zwangs ausgeschlossen ist, wenn diese dem Zweck dienen, zu verhindern, dass Geräte der Informations- und Kommunikationstechnik sowie sonstige Gegenstände, die geeignet sind, Verschlusssachen auszubringen, zu zerstören, zu verändern, zu verarbeiten, zu kopieren, unbrauchbar zu machen oder Sabotagehandlungen vorzunehmen, in Dienststellen des Bundesnachrichtendienstes unbefugt eingebracht werden.

(3) Die Durchsetzung einer Maßnahme durch unmittelbaren Zwang ist, wenn nicht der sofortige Vollzug der Maßnahme zur Verhinderung einer qualifiziert funktionsgefährdenden Tätigkeit notwendig ist, anzudrohen.

§ 122

Besondere Vorgaben zur Durchführung von Maßnahmen zur Sicherung von Verschlusssachen

(1) Bei einer Kontrolle oder Durchsuchung aufgefundene Verschlusssachen, Geräte der Informations- und Kommunikationstechnik oder sonstige Gegenstände können sichergestellt werden, wenn dies zur Sicherung von Verschlusssachen erforderlich ist. Für Geräte

der Informations- und Kommunikationstechnik gilt dies nur, soweit die jeweiligen Voraussetzungen des § 118 vorliegen.

(2) Bei der Durchsuchung nach § 116 Nummer 2, § 117 Absatz 1 Nummer 2 und § 118 Absatz 8 hat die betroffene Person das Recht, anwesend zu sein. Maßnahmen nach Satz 1, die in Abwesenheit der betroffenen Person durchgeführt worden sind, sind ihr schriftlich mitzuteilen, wenn hierdurch nicht der Zweck der Maßnahme gefährdet wird. Der betroffenen Person ist auf Verlangen eine Bescheinigung über die Durchsuchung, die im Rahmen der Durchsuchung sichergestellten Gegenstände sowie über den Grund der Durchsuchung zu erteilen.

Unterabschnitt 5

Verarbeitung von personenbezogenen Daten aus Maßnahmen zur Sicherung von Verschlusssachen

§ 123

Besondere Bestimmungen zur Verarbeitung personenbezogener Daten

(1) Der Bundesnachrichtendienst darf die für eine Durchführung von Maßnahmen nach diesem Abschnitt erforderlichen personenbezogenen Daten verarbeiten, soweit nicht besondere Regelungen in diesem Gesetz entgegenstehen. Personenbezogene Daten, die im Rahmen von Maßnahmen nach diesem Abschnitt erhoben worden sind, sind entsprechend zu kennzeichnen. Die §§ 21 und 22 gelten entsprechend.

(2) Die personenbezogenen Daten nach Absatz 1 sind bis zum Ablauf des Kalenderjahres aufzubewahren, das auf das Kalenderjahr der Erhebung folgt. Nach Ablauf der Aufbewahrungsfrist sind die Daten unverzüglich und unwiederbringlich zu löschen, es sei denn, es liegen die Voraussetzungen des Absatzes 3 vor. Daten nach Absatz 1 dürfen nicht gelöscht werden, solange und soweit die Daten für eine gerichtliche Nachprüfung der Rechtmäßigkeit erforderlich sind. § 118 Absatz 7 Satz 2 bleibt unberührt.

(3) Der Bundesnachrichtendienst darf personenbezogene Daten, die im Rahmen von Maßnahmen nach diesem Abschnitt erhoben wurden, über die Absätze 1 und 2 hinaus nur weiterverarbeiten und übermitteln, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall erforderlich ist

1. zur nachrichtendienstlichen Auslandsaufklärung, wenn die personenbezogenen Daten im Rahmen von Maßnahmen zur Sicherung der Bediensteten und Dienststellen erhoben wurden,

2. zur Aufklärung eines herausgehobenen Bedrohungsfeldes nach § 4 Absatz 4 Nummer 2 und 4, wenn die personenbezogenen Daten im Rahmen von Maßnahmen zur Sicherung von Verschlusssachen erhoben wurden,

3. zur Durchführung arbeitsrechtlicher oder disziplinarrechtlicher Maßnahmen,

4. zur Strafverfolgung oder

5. für die Sicherheitsüberprüfung von Personen.

§ 56 Absatz 2 ist mit der Maßgabe anzuwenden, dass die Prüffrist zwei Jahre beträgt. Sind die Daten für die Zwecke nach Satz 1 nicht oder nicht länger erforderlich, sind sie

unverzüglich zu löschen. Für nach Satz 1 Nummer 5 weiterverarbeitete Daten gelten die Regelungen des Sicherheitsüberprüfungsgesetzes.

(4) Daten, die zur Einsatzsicherung aus Wohnungen erhoben wurden (§ 113 Absatz 2), dürfen für andere Zwecke (§ 113 Absatz 3 Nummer 2 und 3) erst weiterverarbeitet oder übermittelt werden, wenn zuvor die Rechtmäßigkeit der Anordnung nach § 97 Absatz 6 festgestellt wurde.

(5) Stellt der Bundesnachrichtendienst im Rahmen von Maßnahmen nach Unterabschnitt 2 oder 3 fest, dass Anhaltspunkte für eine Gefährdung der Vertraulichkeit der Verschlusssache vorliegen, darf er personenbezogene Daten an die die Verschlusssache herausgebende Stelle übermitteln, soweit dies für die herausgebende Stelle zum Schutz ihrer Verschlusssache erforderlich ist.

§ 124

Schutz von minderjährigen Personen

(1) Der Bundesnachrichtendienst darf im Rahmen von Maßnahmen nach diesem Abschnitt erhobene personenbezogene Daten von minderjährigen Personen, die nicht zu den in § 108 oder § 115 genannten Personen gehören, nicht weiterverarbeiten. Die erhobenen personenbezogenen Daten nach Satz 1 sind zu löschen, es sein denn, die Trennung der personenbezogenen Daten von den Informationen, die im Rahmen von Maßnahmen nach diesem Abschnitt erhoben wurden, ist nicht oder nur mit übermäßigem Aufwand möglich. In diesem Fall ist die Verarbeitung der Daten einzuschränken.

(2) Absatz 1 gilt auch für die Verarbeitung von personenbezogenen Daten von minderjährigen Personen, die noch nicht 14 Jahre alt sind und die zu den in § 108 oder § 115 genannten Personen gehören.

Abschnitt 9

Landes- und Bündnisverteidigung

§ 125

Verteidigungs-, Spannungs- und Zustimmungsfall

(1) Im Verteidigungsfall (Artikel 115a des Grundgesetzes) finden die Regelungen dieses Abschnitts ergänzend Anwendung.

(2) Im Spannungsfall (Artikel 80a des Grundgesetzes) finden die Regelungen dieses Abschnitts ergänzend Anwendung, wenn die Bundesregierung festgestellt hat, dass die Anwendung der Regelungen dieses Abschnitts aus Gründen der Verteidigung zwingend notwendig ist. Die Bundesregierung kann die Feststellung nach Satz 1 mit der Entscheidung verbinden, dass nur bestimmte Regelungen dieses Abschnitts Anwendung finden.

(3) Die Regelungen dieses Abschnitts finden auch dann ergänzend Anwendung, wenn der Verteidigungs- oder der Spannungsfall unmittelbar bevorsteht und die Bundesregierung mit Zustimmung des Parlamentarischen Kontrollgremiums festgestellt hat, dass dies aus Gründen der Verteidigung zwingend notwendig ist (Zustimmungsfall). Absatz 2 Satz 2 gilt entsprechend.

(4) Die Bundesregierung hebt die Feststellung nach Absatz 2 Satz 1 oder Absatz 3 Satz 1 auf, wenn

1. die Voraussetzungen hierfür entfallen sind,

2. das parlamentarische Kontrollgremium es mit der Mehrheit von zwei Dritteln seiner Mitglieder verlangt oder

3. im Fall des Absatzes 2 der Deutsche Bundestag es verlangt.

(5) Der Bundesnachrichtendienst trifft die zur Durchführung der Regelungen dieses Abschnitts erforderlichen Vorbereitungen.

§ 126

Unterstützung durch andere Stellen

(1) Der Bundesnachrichtendienst darf inländische öffentliche Stellen bei der Wahrnehmung seiner Aufgaben um Unterstützung ersuchen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall erforderlich ist zur nachrichtendienstlichen Aufklärung, Abwendung oder Einschränkung der Bedrohungslage, die zur Feststellung eines der in § 125 Absatz 1 bis 3 genannten Fälle geführt hat. Die nach Satz 1 ersuchte Stelle kann die Unterstützung ablehnen, wenn durch die Unterstützungsleistung die Erfüllung ihrer eigenen Aufgaben ernstlich gefährdet würde und dadurch dem Wohl des Bundes erhebliche Nachteile bereitet würden.

(2) Inländische nicht öffentliche Stellen sind gegen Entschädigung, deren Höhe sich an den nachgewiesenen tatsächlichen Kosten orientiert, verpflichtet, den Bundesnachrichtendienst bei der Wahrnehmung seiner Aufgaben zu unterstützen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall erforderlich ist zur nachrichtendienstlichen Aufklärung, Abwendung oder Einschränkung der Bedrohungslage, die zur Feststellung eines der in § 125 Absatz 1 bis 3 genannten Fälle geführt hat, insbesondere durch

1. die Bereitstellung von technischen Mitteln, Ausrüstung oder Infrastruktur oder

2. die Mitwirkung bei der Schaffung von auch digitalen Zugängen zu Einrichtungen, technischen Systemen, Fahrzeugen, Transportgütern sowie Personen.

Stellen, die nach der BSI-Kritisverordnung kritische Dienstleistungen erbringen oder kritische Anlagen betreiben, können die Unterstützung ablehnen, soweit durch die Unterstützungsleistung die Erfüllung ihrer eigenen Aufgaben ernstlich gefährdet würde und dadurch dem Wohl des Bundes erhebliche Nachteile bereitet würden.

(3) In den Fällen des Absatzes 2 erfolgt die Unterstützungsanforderung schriftlich, soweit dies erforderlich ist, um dem Verpflichteten die Erfüllung seiner Verpflichtung zu ermöglichen. § 8 findet in Fällen des Absatzes 2 entsprechend Anwendung.

(4) Die Datenerhebung unter Mitwirkung anderer Stellen richtet sich nach § 127.

§ 127

Datenerhebung unter Mitwirkung anderer Stellen

(1) Abschnitt 2 gilt nach Maßgabe der folgenden Absätze.

(2) Der Bundesnachrichtendienst darf, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall erforderlich ist zur nachrichtendienstlichen Aufklärung, Abwendung oder Einschränkung der Bedrohungslage, die zur Feststellung eines der in § 125 Absatz 1 bis 3 genannten Fälle geführt hat, ersuchen

1. inländische öffentliche Stellen um Auskunft zu vorhandenen Daten oder um Mitwirkung nach § 11 Absatz 4 oder

2. inländische nichtöffentliche Stellen um Auskunft zu vorhandenen Daten oder um Mitwirkung nach § 15 Absatz 1.

(3) Anordnungen können auch für eine Reihe von Ersuchen, die nach Art, Umständen und Umfang bestimmt sind, getroffen werden.

(4) Die Anordnungen der Ersuchen nach Absatz 2 enthalten die folgenden Angaben:

1. Aufklärungsthema,

2. Art der Maßnahme,

3. Ziel der Maßnahme und

4. Befristung.

Der Bundesnachrichtendienst legt mit Zustimmung duch das Bundeskanzleramt fest, für welchen Zeitraum Anordnungen höchstens befristet werden dürfen. Macht der Bundesnachrichtendienst von der Möglichkeit des Satzes 2 Gebrauch, endet die Anordnung spätestens mit dem Ende der Bedrohungslage, die zur Feststellung eines der in § 125 Absatz 1 bis 3 genannten Fälle geführt hat.

(5) Zur Auskunft oder Mitwirkung verpflichtet sind alle inländischen öffentlichen und nichtöffentlichen Stellen.

§ 128

Einsatz nachrichtendienstlicher Mittel

(1) Abschnitt 3 gilt nach Maßgabe der folgenden Absätze.

(2) Der Einsatz nachrichtendienstlicher Mittel ist zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall erforderlich ist zur nachrichtendienstlichen Aufklärung der Bedrohungslage, die zur Feststellung eines der in § 125 Absatz 1 bis 3 genannten Fälle geführt hat.

(3) In den Fällen des Absatzes 2

1. finden die §§ 20 und 22 keine Anwendung,

2. gelten die Ausnahmen nach § 23 Absatz 3 Satz 1 als angeordnet und

3. findet § 31 Absatz 2 Satz 1 bei der strategischen Aufklärung keine Anwendung.

(4) Anordnungen können auch für eine Reihe von Maßnahmen, die nach Art, Umständen und Umfang bestimmt sind, getroffen werden.

(5) In den Fällen des Absatzes 2 enthält die Anordnung die folgenden Angaben:

1. Aufklärungsthema,

2. Art der Maßnahmen und

3. Befristung.

Im Verteidigungsfall legt der Bundesnachrichtendienst mit Zustimmung durch das Bundeskanzleramt abweichend von § 46 Absatz 3, § 47 Absatz 3, § 48 Absatz 3 fest, für welchen Zeitraum Anordnungen höchstens befristet werden dürfen. Macht der Bundesnachrichtendienst von der Möglichkeit des Satzes 2 Gebrauch, endet die Anordnung spätestens mit dem Ende des Verteidigungsfalls.

(6) Die Vorgaben zu Prüf-, Löschpflichten von personenbezogenen Daten sowie die Protokollierungspflichten nach § 29 Absatz 6 sind bis zum Ende des Verteidigungs-, Spannungs- oder Zustimmungsfalls ausgesetzt.

§ 129

Erweiterte nachrichtendienstliche Maßnahmen

(1) Abschnitt 4 gilt nach Maßgabe der folgenden Absätze.

(2) Die in § 125 Absatz 1 bis 3 genannten Fälle stellen zugleich eine spezifische Gefährdungslage nach § 49 Absatz 2 dar.

(3) Im Verteidigungsfall dürfen erweiterte nachrichtendienstliche Maßnahmen nach § 51 Absatz 1 zur Abwendung oder Einschränkung der Bedrohungslage, die zur Feststellung des Verteidigungsfalls geführt hat, auch ohne Grundanordnung durchgeführt werden. Sollen erweiterte nachrichtendienstliche Maßnahmen ohne Grundanordnung durchgeführt werden, bedürfen Art und Umfang der Maßnahmen der vorherigen Zustimmung durch das Bundeskanzleramt.

(4) Im Verteidigungsfall finden zur Abwendung oder Einschränkung der Bedrohungslage, die zur Feststellung des Verteidigungsfalls geführt hat, § 49 Absatz 1 Satz 2 und § 51 Absatz 3 Satz 2 keine Anwendung.

§ 130

Weiterverarbeitung personenbezogener Daten

(1) Abschnitt 5 gilt nach Maßgabe der folgenden Absätze.

(2) Der Bundesnachrichtendienst darf personenbezogene Daten weiterverarbeiten, soweit dies erforderlich ist zur nachrichtendienstlichen Aufklärung, Abwendung oder Einschränkung der Bedrohungslage, die zur Feststellung eines der in § 126 Absatz 1 bis 3 genannten Fälle geführt hat.

(3) Die im Abschnitt 5 getroffenen Vorgaben zu Prüf- oder Löschpflichten von personenbezogenen Daten sind bis zum Ende des Verteidigungs-, Spannungs- oder Zustimmungsfalls ausgesetzt.

(4) Die im Abschnitt 5 getroffenen Vorgaben zu Protokollierungspflichten sind bis zum Ende des Verteidigungs-, Spannungs- oder Zustimmungsfalls ausgesetzt.

§ 131

Übermittlung von personenbezogenen Daten

(1) Abschnitt 6 gilt nach Maßgabe der folgenden Absätze.

(2) Der Bundesnachrichtendienst darf personenbezogene Daten an andere Stellen übermitteln, soweit dies erforderlich ist zur nachrichtendienstlichen Aufklärung, Abwendung oder Einschränkung der Bedrohungslage, die zur Feststellung eines der in § 125 Absatz 1 bis 3 genannten Fälle geführt hat. Abschnitt 6 Unterabschnitt 2 mit Ausnahme von § 70 Absatz 1 und 2, § 74 Absatz 1 Nummer 1 und 2 sowie § 76 Absatz 1 und § 78 finden insoweit keine Anwendung.

(3) Der Bundesnachrichtendienst darf in den Fällen des Absatzes 2 personenbezogene Daten auch automatisiert übermitteln.

(4) Der Bundesnachrichtendienst darf gemeinsame Dateien errichten und führen sowie sich an gemeinsamen Dateien beteiligen. Der Bundesnachrichtendienst erstellt für die durch ihn geführten Dateien ein Verzeichnis. Dieses Verzeichnis soll für jede Datei folgende Angaben enthalten:

1. Bezeichnung der Datei,

2. Zweck der Datei,

3. beteiligte Stellen.

(5) Die Weiterführung einer nach Absatz 4 geführten Datei nach der Beendigung des Verteidigungs-, Spannungs- oder Zustimmungsfalls ist nur unter den Voraussetzungen von Abschnitt 6 Unterabschnitt 4 zulässig.

§ 132

Ergänzende Bestimmungen

(1) Die §§ 32 bis 34 des UKRat-Gesetzes finden keine Anwendung.

(2) Abschnitt 7 gilt nach Maßgabe der folgenden Absätze.

(3) § 97 Absatz 3 findet im Spannungs- und Zustimmungsfall mit der Maßgabe Anwendung, dass eine regelmäßige Berichtspflicht über Maßnahmen, die nach § 97 Absatz 3 der Einzelfallkontrolle unterliegen, die unverzügliche Vorlagepflicht ersetzt. Der Unabhängige Kontrollrat bestimmt in welchen Abständen die Berichte zu erstatten sind. Im Verteidigungsfall

1. entfällt die Vorabkontrolle nach § 97 Absatz 1,

2. findet § 97 Absatz 2 und 3 keine Anwendung.

(4) Der Bundesnachrichtendienst unterrichtet das Parlamentarische Kontrollgremium in regelmäßigen Abständen über seine Tätigkeit.

(5) Abschnitt 7 Unterabschnitt 2

1. ist im Spannungsfall ausgesetzt, wenn der Spannungsfall nicht länger als drei Monate anhält,

2. findet im Spannungsfall keine Anwendung, wenn der Spannungsfall länger als drei Monate anhält,

3. findet im Verteidigungsfall keine Anwendung.

Satz 1 Nummer 1 und 2 gilt im Zustimmungsfall entsprechend.

§ 133

Besondere Bestimmungen zum Schutz der Bediensteten, Dienststellen und Verschlusssachen

(1) Abschnitt 8 findet mit der Maßgabe Anwendung, dass Voraussetzung für die Anwendung der dort genannten Befugnisse ist, dass dies jeweils zum Schutz der Bediensteten, Dienststellen und Verschlusssachen erforderlich ist.

(2) Die in § 124 getroffenen Vorgaben zu Prüf- oder Löschpflichten von personenbezogenen Daten sind bis zum Ende des Verteidigungs-, Spannungs- oder Zustimmungsfalls ausgesetzt.

Abschnitt 10

Unternehmenspflichten, Anzeigepflichten, Straf- und Bußgeldvorschriften

§ 134

Kontrolle und Durchsetzung von Unternehmenspflichten

(1) Das Bundesverwaltungsamt kann Anordnungen und andere Maßnahmen treffen, um die Einhaltung der Pflichten nach den §§ 12 bis 15 sowie der auf Grund des § 138 ergangenen Rechtsverordnungen sicherzustellen. Die verpflichtete Stelle muss auf Anforderung des Bundesverwaltungsamtes die hierzu erforderlichen Auskünfte erteilen. Das Bundesverwaltungsamtes ist befugt, die Geschäfts- und Betriebsräume der verpflichteten Stelle während der üblichen Geschäfts- und Betriebszeiten zu betreten und zu besichtigen. Die Befugnisse der Bundesnetzagentur bleiben unberührt.

(2) Über die Befugnis nach Absatz 1 hinaus kann das Bundesverwaltungsamt den Betrieb des Unternehmens oder das Erbringen des betreffenden Dienstes ganz oder teilweise untersagen, wenn mildere Eingriffe zur Durchsetzung rechtmäßigen Verhaltens nicht ausreichen.

(3) Zur Durchsetzung von Maßnahmen nach den Absätzen 1 und 2 kann das Bundesverwaltungsamt nach Maßgabe des Verwaltungs-Vollstreckungsgesetzes ein Zwangsgeld bis zu 1 000 000 Euro festsetzen.

§ 135

Besondere Anzeige- und Genehmigungspflicht für ausgeschiedene Bedienstete des Bundesnachrichtendienstes

(1) § 105 Absätze 2 bis 6 des Bundesbeamtengesetzes gelten für frühere Beamtinnen und Beamte des Bundesnachrichtendienstes auch dann entsprechend, wenn es sich nicht um frühere Beamtinnen mit Versorgungsbezügen und frühere Beamte mit Versorgungsbezügen sowie um frühere Beamtinnen mit Anspruch auf Altersgeld und frühere Beamte mit Anspruch auf Altersgeld handelt.

(2) § 105 Absatz 2 bis 6 des Bundesbeamtengesetzes gelten für frühere Angestellte des Bundesnachrichtendienstes entsprechend.

§ 136

Strafvorschriften

Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer entgegen § 8 Absatz 1 Nummer 1, auch in Verbindung mit § 51 Absatz 5 Satz 2 und § 126 Absatz 3 Satz 2, eine Mitteilung macht. Wird durch die Mitteilung der Zweck der Maßnahme oder werden eingesetzte Personen gefährdet, ist die Strafe Freiheitsstrafe von drei Monaten bis zu fünf Jahren.

§ 137

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer

1. einem vollziehbaren Ersuchen nach § 12 Absatz 1, 4 Satz 1 oder Absatz 5 Satz 1, § 13 Absatz 1, 4 oder 5, § 14 Absatz 1 Satz 1 oder Absatz 2 oder § 15 Satz 1 zuwiderhandelt,

2. entgegen § 12 Absatz 3 Satz 1 nicht sicherstellt, dass eine Geheimschutzmaßnahme getroffen wird,

3. entgegen § 13 Absatz 6 Satz 1 Nummer 1 keine Personen auswählt, entgegen § 13 Absatz 6 Satz 2 eine Person betraut oder einer Anordnung nach § 13 Absatz 6 Satz 4 zuwiderhandelt,

4. entgegen § 134 Absatz 1 Satz 2 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt,

5. entgegen § 136 in Verbindung mit § 105 Absatz 5 des Bundesbeamtengesetzes eine genehmigungsbedürftige Erwerbstätigkeit oder genehmigungspflichtige sonstige Beschäftigung ohne Genehmigung aufnimmt oder

6. entgegen § 136 in Verbindung mit § 105 Absatz 2 des Bundesbeamtengesetzes eine Erwerbstätigkeit oder sonstige Beschäftigung ohne vorherige Anzeige aufnimmt oder entgegen § 136 in Verbindung mit § 105 Absatz 4 Satz 2 des Bundesbeamtengesetzes trotz vorläufiger Untersagung der Aufnahme aufnimmt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße geahndet werden

1. bei Absatz 1 Nummer 1 bis zu dreihunderttausend Euro,

2. bei Absatz 1 Nummer 2 und 3 bis zu fünfhunderttausend Euro,

3. bei Absatz 1 Nummer 4 bis zu einhunderttausend Euro,

4. bei Absatz 1 Nummer 5 bis zu fünfzigtausend Euro,

5. bei Absatz 1 Nummer 6 bis zu zehntausend Euro.

(3) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundesverwaltungsamt.

Abschnitt 11

Schlussvorschriften

§ 138

Verordnungsermächtigung

Das Bundeskanzleramt wird ermächtigt, durch Rechtsverordnung im Einvernehmen mit dem Bundesministerium des Innern, dem Bundesministerium für Finanzen, dem Bundesministerium der Verteidigung, dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium für Digitales und Staatsmodernisierung und dem Bundesministerium für Verkehr ohne Zustimmung des Bundesrates das Nähere zu regeln

1. zur technischen und organisatorischen Umsetzung der Pflicht, an Maßnahmen des Bundesnachrichtendienstes nach § 13 Absatz 5 Nummer 4 mitzuwirken;

2. zur Form von Übermittlungen nach §§ 12 bis 14 an den Bundesnachrichtendienst, soweit dazu keine Regelungen auf Grund des § 170 des Telekommunikationsgesetzes getroffen werden, insbesondere, dass Übermittlungen ganz oder teilweise auf maschinell verwertbaren Datenträgern oder durch Datenfernübertragung übermitteln müssen, einschließlich

   a) der Voraussetzungen für die Anwendung des Verfahrens,

   b) des Näheren über Form, Inhalt, Verarbeitung und Sicherung der zu übermittelnden Daten,

   c) der Art und Weise sowie der Adressierung der Übermittlung der Daten,

   d) des Umfangs und der Form der für dieses Verfahren erforderlichen besonderen Erklärungspflichten des Verpflichteten.

Zur Regelung der Datenübermittlung kann in der Rechtsverordnung auf Veröffentlichungen sachverständiger Stellen verwiesen werden. Hierbei sind das Datum der Veröffentlichung, die Bezugsquelle und eine Stelle zu bezeichnen, bei der die Veröffentlichung archivmäßig gesichert niedergelegt ist.

§ 139

Einschränkung von Grundrechten

Die Grundrechte der körperlichen Unversehrtheit (Artikel 2 Absatz 2 Satz 1 des Grundgesetzes), der Freiheit der Person (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes), des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) und der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) werden nach Maßgabe der Abschnitte 3 und 4 dieses Gesetzes eingeschränkt. Die Grundrechte auf körperliche Unversehrtheit (Artikel 2 Absatz 2 Satz 1 des Grundgesetzes) und Freiheit der Person (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes) werden nach Maßgabe der Abschnitte 8 bis 10 dieses Gesetzes eingeschränkt.

§ 140

Übergangsvorschriften

(1) Für zum Zeitpunkt des Inkrafttretens dieses Gesetzes laufende Anordnungen

1. von Auskunftsersuchen

2. von in § 46 Absatz 1 genannten Maßnahmen gilt die Anordnungsdauer nach § 46 Absatz 3,

3. von in § 47 Absatz 1 genannten Maßnahmen gilt die Anordnungsdauer nach § 47 Absatz 3 und

4. von in § 48 Absatz 1 genannten Maßnahmen gilt die Anordnungsdauer nach § 48 Absatz 3.

(2) Maßnahmen, mit Ausnahme der in § 97 Absatz 1 Nummer 9, 10, 14 und 15 genannten,

1. können bis zum … [einsetzen: Angabe des Tages und Monats der Verkündung dieses Gesetzes sowie die Jahreszahl des ersten auf die Verkündung folgenden Jahres *(BND: mindestens 12 Monate)]* auch nach Maßgabe der bis zum Inkrafttreten dieses Gesetzes geltenden Verfahrensvorschriften durchgeführt werden,

2. dürfen ab dem [… einsetzen: Angabe des Tages und Monats der Verkündung dieses Gesetzes sowie die Jahreszahl des ersten auf die Verkündung folgenden Jahres] nur fortgesetzt werden, wenn die Anordnung nach § 23 und die unabhängige Anordnungskontrolle im Sinne des § 73 erfolgt ist.

Für eine erstmalige Anordnung gilt Satz 1 Nummer 1 nur bis zum […einsetzen: Datumsangabe des Tages des sechsten der Verkündung dieses Gesetzes folgenden Monats].

(3) Die Dienstvorschrift nach § 95 Absatz 1 ist bis zum [einsetzen: Datum des ersten Tages des zwölften auf die Verkündung dieses Gesetzes folgenden Kalendermonats] neu zu erlassen. Die Dienstvorschrift enthält alle zum Zeitpunkt ihres Erlasses durch den Bundesnachrichtendienst eingesetzten nachrichtendienstlichen Mittel. Die Dienstvorschrift, soweit sie den Katalog der nachrichtendienstlichen Mittel betrifft, ist bis zum [einsetzen: … Datumsangabe] durch den Unabhängigen Kontrollrat zu prüfen.

(4) Auskunftsersuchen, die nach § 17 Absatz 1 einer Anordnung bedürfen und der Vorabkontrolle nach [§§…] unterliegen, aber bereits vor Inkrafttreten dieses Gesetzes durch

die G 10-Kommission genehmigt wurden, können aufgrund dieser Genehmigung durchgeführt werden.

(5) Die am [einsetzen: Tag vor dem Inkrafttreten des neuen Gesetzes] bestehenden Kooperationsvereinbarungen mit ausländischen öffentlichen Stellen nach § 31 der am [einsetzen: Tag vor dem Inkrafttreten des neuen Gesetzes] geltenden Fassung gelten fort.

(6) Die Mitteilungspflicht nach § 100 Absatz 1 Nummer 2 gilt nur für Maßnahmen,

1. für die bereits vor Inkrafttreten dieses Gesetzes eine Mitteilungspflicht bestand oder

2. zu denen zuvor eine Vorabkontrolle nach § 97 Absatz 1 Nummer 1 durchgeführt wurde.

(7) Die Speicherung von Daten, die vor dem 1. Januar 2022 erhoben wurden, sowie die Speicherung von Daten, die auf der Grundlage einer Maßnahme nach Absatz 1 erhoben wurden, bestimmen sich nach den §§ 19 und 20 in der am 19. Juni 2020 geltenden Fassung.

(8) Die Übermittlung von Daten, die vor dem 1. Januar 2022 erhoben wurden, sowie die Übermittlung von Daten, die auf der Grundlage einer Maßnahme nach Absatz 1 erhoben wurden, bestimmen sich nach § 24 in der am 19. Juni 2020 geltenden Fassung.

(9) Die Nachrichtendienste-Übermittlungsverordnung vom 11. Oktober 2012 (BGBl. I S. 2117), die zuletzt durch Artikel 7 Absatz 29 des Gesetzes vom 12. Mai 2021 (BGBl. I S. 990) geändert worden ist, findet auf Auskunftsersuchen des Bundesnachrichtendienstes solange weiter entsprechende Anwendung, bis eine Verordnung nach § 138 erlassen wurde.

(10) Bis zur Schaffung der technischen Voraussetzungen für die in § 34 Absatz 3 Satz 1 und § 36 Absatz 2 Satz 1 vorgesehene Kennzeichnung ist die Weiterverarbeitung der nach Abschnitt 3 Unterabschnitt 3 erhobenen personenbezogenen Daten in den bestehenden Systemen des Bundesnachrichtendienstes auch ohne die Kennzeichnung zulässig, sofern hinsichtlich der ab dem 1. Januar 2022 erhobenen Daten jeweils der Zweck und das Mittel der Datenerhebung anderweitig nachvollziehbar sind. Die Weiterverarbeitung in den strukturierten Grundlagenbanken des Bundesnachrichtendienstes ist darüber hinaus bis zur Schaffung der technischen Voraussetzungen für die Kennzeichnung von Zweck und Mittel auch dann zulässig, wenn der Zweck und das Mittel der Datenerhebung nicht für jedes Datum nachvollziehbar sind; die Übermittlung dieser Daten richtet sich insoweit nach Absatz 8. Das Bundeskanzleramt berichtet dem Parlamentarischen Kontrollgremium jährlich über den Fortschritt bei der Schaffung der technischen Voraussetzungen für die Kennzeichnung nach Satz 2.

Artikel 3

Gesetz über die Rechtskontrolle durch den Unabhängigen Kontrollrat

(UKRat-Gesetz – UKRatG)

Inhaltsübersicht

Abschnitt 1
Unabhängiger Kontrollrat und Aufgaben

§ 1 Unabhängiger Kontrollrat

§ 2 Aufgaben des Unabhängigen Kontrollrats

§ 3 Zuständigkeit; Anwendbarkeit des Bundesdatenschutzgesetzes

Abschnitt 2
Organisation und behördlicher Aufbau des Unabhängigen Kontrollrats

Unterabschnitt 1
Organisation des Unabhängigen Kontrollrats

§ 4 Sitz

§ 5 Aufbau

§ 6 Prüfung der Haushalts- und Wirtschaftsführung

§ 7 Leitung des Unabhängigen Kontrollrats

§ 8 Geschäftsordnung

§ 9 Verfahrensordnung

§ 10 Geschäftsverteilung

Unterabschnitt 2
Rechte und Pflichten der Bediensteten des Unabhängigen Kontrollrats

§ 11 Deutsche Staatsangehörigkeit; Sicherheitsüberprüfung

§ 12 Geheimhaltung; Aussagegenehmigung

Unterabschnitt 3
Befugnisse im Zusammenhang mit der Rechtskontrolle

§ 13 Befugnisse des Unabhängigen Kontrollrats

Unterabschnitt 4
Gerichtsähnliches Kontrollorgan

§ 14 Besetzung des gerichtsähnlichen Kontrollorgans

§ 15 Unabhängigkeit der Mitglieder des gerichtsähnlichen Kontrollorgans

§ 16 Vakanzen im gerichtsähnlichen Kontrollorgan

§ 17 Wahl und Ernennung der Mitglieder des gerichtsähnlichen Kontrollorgans; Wahl der Präsidentin oder des Präsidenten und der Vizepräsidentin oder des Vizepräsidenten des Unabhängigen Kontrollrats

§ 18 Ernennung und Rechtsstellung der Mitglieder des gerichtsähnlichen Kontrollorgans

§ 19 Amtszeit der Mitglieder des gerichtsähnlichen Kontrollorgans

§ 20 Ruhestand; Ruhegehalt der Mitglieder des gerichtsähnlichen Kontrollorgans

§ 21 Besoldung der Mitglieder des gerichtsähnlichen Kontrollorgans

§ 22 Weitere Rechte und Pflichten der Mitglieder des gerichtsähnlichen Kontrollorgans

§ 23 Kollegialspruchkörper und Entscheidungen des gerichtsähnlichen Kontrollorgans

§ 24 Beratungsgeheimnis

Unterabschnitt 5
Administratives Kontrollorgan

§ 25 Leitung des administrativen Kontrollorgans; Weisungen

§ 26 Prüfprogramm für das administrative Kontrollorgan; Prüfaufträge

Abschnitt 3
Ausübung der Rechtskontrolle durch den Unabhängigen Kontrollrat

Unterabschnitt 1
Rechtskontrolle durch das gerichtsähnliche Kontrollorgan; Gefahr im Verzug

§ 27 Vorabkontrolle durch das gerichtsähnliche Kontrollorgan

§ 28 Zuständigkeit für Entscheidungen in der Vorabkontrolle

§ 29 Einzelfallkontrolle durch das gerichtsähnliche Kontrollorgan

§ 30 Antrag auf Überprüfung durch den Senat

§ 31 Gefahr im Verzug

Unterabschnitt 2
Rechtskontrolle durch das administrative Kontrollorgan

§ 32 Administrative Kontrolle

§ 33 Beanstandungen; Unterrichtungen

§ 34 Qualifizierter Verstoß; Anweisungen

Abschnitt 4
Zusammenarbeit des Unabhängigen Kontrollrats mit dem Parlamentarischen Kontrollgremium

§ 35 Tätigkeitsbericht

§ 36 Öffentlicher Bericht

§ 37 Austausch mit dem Parlamentarischen Kontrollgremium und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Abschnitt 5
Sonstige Vorschriften und Schlussvorschriften

§ 38 Individuelles Ersuchen beim Unabhängigen Kontrollrat

§ 39 Schutz des Eigensicherungsbereichs

§ 40 Verfahren im Eigensicherungsbereich

§ 41 Evaluationsbericht

§ 42 Übergangsregelungen

Abschnitt 1

Unabhängiger Kontrollrat und Aufgaben

§ 1

Unabhängiger Kontrollrat

Der Unabhängige Kontrollrat ist eine oberste Bundesbehörde und nur dem Gesetz unterworfen. Der Unabhängige Kontrollrat ist bei der Erfüllung seiner Aufgaben und bei der Ausübung seiner Befugnisse unabhängig und nicht weisungsgebunden.

§ 2

Aufgaben des Unabhängigen Kontrollrats

(1) Aufgabe des Unabhängigen Kontrollrats ist die Kontrolle der Rechtmäßigkeit

1. der Verarbeitung personenbezogener Daten durch das Bundesamt für Verfassungsschutz bei der Wahrnehmung der in § 2 Absatz 1 bis 4 des Bundesverfassungsschutzgesetzes bezeichneten Aufgaben sowie der Schutzmaßnahmen nach § 60 des Bundesverfassungsschutzgesetzes und

2. der Verarbeitung personenbezogener Daten durch den Bundesnachrichtendienst bei der Wahrnehmung der in § 2 Absatz 1 des BND-Gesetzes bezeichneten Aufgabe sowie der erweiterten nachrichtendienstlichen Maßnahmen nach § 52 des BND-Gesetzes

(Rechtskontrolle).

(2) Die Rechtskontrolle erfolgt als

1. gerichtsähnliche Kontrolle

   a) vor Durchführung gesetzlich bestimmter Maßnahmen (Vorabkontrolle) und

   b) in weiteren gesetzlich vorgesehenen Fällen (Einzelfallkontrolle) und

2. administrative Kontrolle.

(3) Das Bundesamt für den Verfassungsschutz und der Bundesnachrichtendienst hören den Unabhängigen Kontrollrat vor Erlass von vorgesehenen Errichtungsanordnungen nach [§ 40 Absatz 2 Satz 1 des Bundesverfassungsschutzgesetzes und § 98 Absatz 3 des BND-Gesetzes an. § 40 Absatz 2 Satz 4 des Bundesverfassungsschutzgesetzes und § 60 Absatz 5 des BND-Gesetzes bleiben unberührt.

(4) Im Rahmen seiner gesetzlichen Aufgaben unterstützt der Unabhängige Kontrollrat das Parlamentarische Kontrollgremium bei dessen Kontrolltätigkeit.

§ 3

Zuständigkeit; Anwendbarkeit des Bundesdatenschutzgesetzes

(1) Soweit dem Unabhängigen Kontrollrat die Rechtskontrolle obliegt, besteht keine Kontrollzuständigkeit der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

(2) Für die im Rahmen der Rechtskontrolle vorgenommenen Verarbeitungen von personenbezogenen Daten durch den Unabhängigen Kontrollrat gilt § 9 Absatz 2 des Bundesdatenschutzgesetzes entsprechend.

Abschnitt 2

Organisation und behördlicher Aufbau des Unabhängigen Kontrollrats

Unterabschnitt 1

Organisation des Unabhängigen Kontrollrats

§ 4

Sitz

Der Unabhängige Kontrollrat hat seinen Sitz in Berlin. Er kann Außenstellen einrichten.

§ 5

Aufbau

(1) Der Unabhängige Kontrollrat besteht aus

1. einem gerichtsähnlichen Kontrollorgan und
2. einem administrativen Kontrollorgan.

(2) Für die Verwaltung besteht eine Präsidialabteilung.

§ 6

Prüfung der Haushalts- und Wirtschaftsführung

Der Unabhängige Kontrollrat unterliegt der Prüfung der Haushalts- und Wirtschaftsführung durch den Bundesrechnungshof, soweit seine Unabhängigkeit dadurch nicht beeinträchtigt wird. Geheimschutzbelangen ist durch den Bundesrechnungshof Rechnung zu tragen.

§ 7

Leitung des Unabhängigen Kontrollrats

(1) Der Unabhängige Kontrollrat wird von der Präsidentin oder dem Präsidenten des Unabhängigen Kontrollrats geleitet (Behördenleitung). Im Fall der Verhinderung der Präsidentin oder des Präsidenten übernimmt die Vizepräsidentin oder der Vizepräsident des Unabhängigen Kontrollrats die Behördenleitung.

(2) Die Behördenleitung vertritt den Unabhängigen Kontrollrat nach außen.

(3) Die Behördenleitung kann ihre Aufgaben auf weitere Mitglieder des gerichtsähnlichen Kontrollorgans mit deren Einvernehmen übertragen. In diesem Fall ist sicherzustellen, dass die Ausübung der Haupttätigkeit des Mitglieds des gerichtsähnlichen Kontrollorgans gewährleistet ist und das Mitglied des gerichtsähnlichen Kontrollorgans in seiner Unabhängigkeit nach § 15 nicht beeinträchtigt wird.

(4) Die Behördenleitung kann den Senat des gerichtsähnlichen Kontrollorgans mit Angelegenheiten der behördlichen Verwaltung befassen oder ihn vor eigenen Entscheidungen zur behördlichen Verwaltung hören.

§ 8

Geschäftsordnung

(1) Der Unabhängige Kontrollrat gibt sich eine Geschäftsordnung. Die Geschäftsordnung des Unabhängigen Kontrollrats wird von der Präsidentin oder dem Präsidenten erlassen oder geändert. Das Bundeskanzleramt, das Bundesministerium des Innern und das Bundesministerium der Verteidigung sind vor Erlass und vor Änderung der Geschäftsordnung anzuhören.

(2) In der Geschäftsordnung ist Geheimschutzbelangen der Nachrichtendienste des Bundes ist Rechnung zu tragen.

(3) Entscheidungen über die Geschäftsordnung ergehen

1. mit Zustimmung der Mehrheit der übrigen Mitglieder des Senates des gerichtsähnlichen Kontrollorgans und

2. im Einvernehmen mit dem Parlamentarischen Kontrollgremium.

§ 9

Verfahrensordnung

(1) Der Unabhängige Kontrollrat gibt sich eine Verfahrensordnung. Die Verfahrensordnung des Unabhängigen Kontrollrats wird vom Senat mit der Mehrheit seiner Stimmen erlassen oder geändert. Das Bundeskanzleramt, das Bundesministerium des Innern und das Bundesministerium der Verteidigung sind vor Erlass der Verfahrensordnung anzuhören.

(2) Die Verfahrensordnung regelt die Einzelheiten des Verfahrensablaufs bei der Durchführung der Rechtskontrolle.

(3) Geheimschutzbelangen der Nachrichtendienste des Bundes ist Rechnung zu tragen.

(4) Die Verfahrensordnung ist dem Parlamentarischen Kontrollgremium zur Kenntnisnahme zu übermitteln.

§ 10

Geschäftsverteilung

(1) Der Senat erlässt nach Maßgabe der Verfahrensordnung mit der Mehrheit seiner Stimmen vor Beginn jedes Geschäftsjahrs für dessen Dauer einen Geschäftsverteilungsplan, in dem

1. die Besetzung der Kollegialspruchkörper bestimmt wird,

2. die Vertretung geregelt wird und

3. die Geschäfte auf die einzelnen Kollegialspruchkörper und Mitglieder des gerichtsähnlichen Kontrollorgans verteilt werden.

(2) In dem Geschäftsverteilungsplan können Zuständigkeiten der Kollegialspruchkörper oder der Mitglieder des gerichtsähnlichen Kontrollorgans für besondere thematische Schwerpunkte vorgesehen werden.

Unterabschnitt 2

Rechte und Pflichten der Bediensteten des Unabhängigen Kontrollrats

§ 11

Deutsche Staatsangehörigkeit; Sicherheitsüberprüfung

(1) Die Bediensteten des Unabhängigen Kontrollrats müssen deutsche Staatsangehörige sein.

(2) Die Bediensteten des Unabhängigen Kontrollrats haben sich vor Aufnahme ihrer Tätigkeit einer erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlungen nach § 10 des Sicherheitsüberprüfungsgesetzes zu unterziehen. § 15 des Sicherheitsüberprüfungsgesetzes bleibt unberührt.

§ 12

Geheimhaltung; Aussagegenehmigung

(1) Die Bediensteten des Unabhängigen Kontrollrats sind zur Geheimhaltung der Angelegenheiten verpflichtet, die ihnen bei ihrer Tätigkeit oder bei Gelegenheit ihrer Tätigkeit im Unabhängigen Kontrollrat bekannt geworden sind. Dies gilt auch nach ihrem Ausscheiden aus dem Unabhängigen Kontrollrat.

(2) Über die Erteilung einer Aussagegenehmigung entscheidet die Behördenleitung. Die Genehmigung ist zu versagen, wenn

1. die Aussage dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder

2. die Erfüllung öffentlicher Aufgaben ernstlich gefährden oder erheblich erschweren würde.

Über die Erteilung einer Aussagegenehmigung für die Präsidentin oder den Präsidenten entscheidet die Vizepräsidentin oder der Vizepräsident. Sind Stellen außerhalb des Unabhängigen Kontrollrats an der Entstehung der geheimhaltungsbedürftigen Angelegenheit beteiligt gewesen, so kann die Genehmigung nur im Einvernehmen mit diesen Stellen erteilt werden. Satz 4 gilt entsprechend für die Erteilung von Aussagegenehmigungen durch andere Stellen zu geheimhaltungsbedürftigen Angelegenheiten, an deren Entstehung der Unabhängige Kontrollrat beteiligt war. Das Einvernehmen nach Satz 4 kann nur nach Maßgabe von Satz 2 verweigert werden. Die Verweigerung ist gegenüber dem Unabhängigen Kontrollrat schriftlich zu begründen.

Unterabschnitt 3

Befugnisse im Zusammenhang mit der Rechtskontrolle

§ 13

Befugnisse des Unabhängigen Kontrollrats

(1) Der Unabhängige Kontrollrat kann von dem jeweiligen Nachrichtendienst verlangen, dass ihm Akten oder andere in dessen amtlicher Verwahrung befindliche Schriftstücke und in Dateien gespeicherte Daten an einer Dienststelle des Nachrichtendienstes in der Bundesrepublik Deutschland zur Verfügung gestellt werden, soweit seine Kontrollzuständigkeit reicht. Soweit dies im Einzelfall erforderlich ist, kann verlangt werden, dass Schriftstücke im Original vorgelegt werden.

(2) Dem Unabhängigen Kontrollrat ist jederzeit Zutritt zu den Dienststellen des jeweiligen Nachrichtendienstes und Zugang zu informationstechnischen Systemen des jeweiligen Nachrichtendienstes zu gewähren, soweit Zutritt oder Zugang für die Ausübung der Kontrolle erforderlich sind. Soweit die Dienststelle und die informationstechnischen Systeme nicht in alleiniger Verfügungsberechtigung des jeweiligen Nachrichtendienstes stehen, ergreift der jeweilige Nachrichtendienst auf Verlangen des Unabhängigen Kontrollrats geeignete Maßnahmen, um dem Unabhängigen Kontrollrat Zutritt oder Zugang zu ermöglichen.

(3) Der Unabhängige Kontrollrat kann von dem jeweiligen Nachrichtendienst Auskunft zu seinen Fragen verlangen, soweit dies für die Ausübung der Kontrolle erforderlich ist.

(4) Von den Befugnissen nach den Absätzen 1 bis 3 ausgenommen sind Informationen und Angaben über operativ eingesetzte Personen, die die Feststellung der Identität dieser Personen oder anderweitig eine Enttarnung ermöglichen.

Unterabschnitt 4

Gerichtsähnliches Kontrollorgan

§ 14

Besetzung des gerichtsähnlichen Kontrollorgans

(1) Das gerichtsähnliche Kontrollorgan besteht aus acht Mitgliedern. Mitglieder des gerichtsähnlichen Kontrollorgans sind:

1. die Präsidentin oder der Präsident mit der Amtsbezeichnung Präsidentin oder Präsident des Unabhängigen Kontrollrats,

2. die Vizepräsidentin oder der Vizepräsident mit der Amtsbezeichnung Vizepräsidentin oder Vizepräsident des Unabhängigen Kontrollrats sowie

3. sechs Mitglieder mit der Amtsbezeichnung Mitglied des Senats beim Unabhängigen Kontrollrat.

(2) Mitglied des gerichtsähnlichen Kontrollorgans kann nur werden, wer

1. bis zur Ernennung als Mitglied des gerichtsähnlichen Kontrollorgans

   a) tätig gewesen ist als

      aa) Richterin oder Richter an einem obersten Gerichtshof des Bundes (richterliches Mitglied),

      bb) Bundesanwältin oder Bundesanwalt,

      cc) Beamtin oder Beamter einer obersten Bundesbehörde in einem Amt der Besoldungsgruppe B 6 oder in einem höheren Amt der Besoldungsordnung B oder

   b) Mitglied eines von einer Volksvertretung bestellten Organs oder Hilfsorgans, welches mit der Nachprüfung von Eingriffen in Artikel 10 des Grundgesetzes durch die Nachrichtendienste des Bundes betraut ist,

2. zusätzlich in dieser Tätigkeit jeweils über langjährige Erfahrung verfügt,

3. in den Fällen von Nummer 1 Buchstabe a Doppelbuchstabe cc und Buchstabe b zusätzlich über die Befähigung zum Richteramt verfügt und

4. in den Fällen der Nummer 1 Buchstabe a Doppelbuchstabe cc zusätzlich die dienstliche Tätigkeit mindestens drei Jahre lang einen fachlichen Bezug zur Arbeit von Sicherheitsbehörden ausweist.

(3) Mindestens sechs Mitglieder des gerichtsähnlichen Kontrollorgans müssen richterliche Mitglieder sein.

§ 15

Unabhängigkeit der Mitglieder des gerichtsähnlichen Kontrollorgans

Die Mitglieder des gerichtsähnlichen Kontrollorgans sind bei der Ausübung der Rechtskontrolle unabhängig und nur dem Gesetz unterworfen.

§ 16

Vakanzen im gerichtsähnlichen Kontrollorgan

(1) Der Unabhängige Kontrollrat teilt eine eingetretene oder bevorstehende Vakanz beim gerichtsähnlichen Kontrollorgan dem Parlamentarischen Kontrollgremium mit. Das Parlamentarische Kontrollgremium schreibt die Stelle daraufhin aus. Die Stellen für richterliche Mitglieder sind bei den obersten Bundesgerichten auszuschreiben. Die übrigen Stellen im gerichtsähnlichen Kontrollorgan sind öffentlich auszuschreiben.

(2) Bewerbungen sind beim Parlamentarischen Kontrollgremium einzureichen.

§ 17

Wahl und Ernennung der Mitglieder des gerichtsähnlichen Kontrollorgans; Wahl der Präsidentin oder des Präsidenten und der Vizepräsidentin oder des Vizepräsidenten des Unabhängigen Kontrollrats

(1) Die Mitglieder des gerichtsähnlichen Kontrollorgans werden vom Parlamentarischen Kontrollgremium mit einfacher Mehrheit gewählt. Die Bewerberinnen und Bewerber für die Stellen im gerichtsähnlichen Kontrollorgan, die die Voraussetzungen des § 14 Absatz 2 erfüllen, stellen sich dem Parlamentarischen Kontrollgremium vor der Wahl vor.

(2) Das Parlamentarische Kontrollgremium hört die Bundesregierung und den Unabhängigen Kontrollrat zu den zur Wahl stehenden Bewerberinnen und Bewerbern an.

(3) Das Parlamentarische Kontrollgremium wählt jeweils auf Vorschlag der oder des Vorsitzenden des Parlamentarischen Kontrollgremiums mit einfacher Mehrheit aus den gewählten Mitgliedern des gerichtsähnlichen Kontrollorgans die Präsidentin oder den Präsidenten sowie die Vizepräsidentin oder den Vizepräsidenten des Unabhängigen Kontrollrats. Die Wahl zur Präsidentin oder zum Präsidenten und zur Vizepräsidentin oder zum Vizepräsidenten des Unabhängigen Kontrollrats kann auch vor deren oder dessen Ernennung nach § 18 Absatz 1 erfolgen.

(4) Ein Mitglied des Parlamentarischen Kontrollgremiums ist von der Mitwirkung bei der Wahl ausgeschlossen, wenn die Voraussetzungen des § 41 Nummer 3 der Zivilprozessordnung vorliegen.

§ 18

Ernennung und Rechtsstellung der Mitglieder des gerichtsähnlichen Kontrollorgans

(1) Die Mitglieder des gerichtsähnlichen Kontrollorgans werden nach ihrer Wahl und der nach § 11 Absatz 2 Satz 1 durchzuführenden Sicherheitsüberprüfung von der Bundespräsidentin oder dem Bundespräsidenten zu Beamtinnen und Beamten auf Zeit ernannt. Vorbehaltlich der Regelungen dieses Gesetzes sind die Vorschriften des

Bundesbeamtengesetzes mit Ausnahme der Vorschriften über die Laufbahnen und die Probezeit anzuwenden.

(2) Sofern die nach § 11 Absatz 2 Satz 1 durchzuführende erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen zu der Annahme eines Sicherheitsrisikos führt, das der Tätigkeit der betroffenen Person entgegensteht, darf die Person nicht nach Absatz 1 Satz 1 ernannt werden.

(3) Die Mitglieder des gerichtsähnlichen Kontrollorgans leisten vor der Präsidentin oder dem Präsidenten des Deutschen Bundestages nach ihrer Ernennung folgenden Eid: „Ich schwöre, dass ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann üben werde. So wahr mir Gott helfe.“ Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

§ 19

Amtszeit der Mitglieder des gerichtsähnlichen Kontrollorgans

(1) Die Amtszeit der Mitglieder des gerichtsähnlichen Kontrollorgans beträgt zwölf Jahre. Eine Wiederwahl ist nicht zulässig. Das Beamtenverhältnis auf Zeit endet vor Ende der Amtszeit, wenn nach der Ernennung ein Sicherheitsrisiko im Sinne des § 5 Absatz 1 des Sicherheitsüberprüfungsgesetzes festgestellt wird.

(2) Das Beamtenverhältnis auf Zeit der Mitglieder des gerichtsähnlichen Kontrollorgans beginnt mit der Aushändigung der Ernennungsurkunde, wenn nicht in der Urkunde ein späterer Tag bestimmt ist.

(3) Mit Ernennung in das Beamtenverhältnis auf Zeit ruhen bei den richterlichen Mitgliedern für die Dauer der Amtszeit die Rechte und Pflichten aus dem zuletzt im Richterverhältnis auf Lebenszeit übertragenen Amt. Dies gilt nicht für die Verschwiegenheitspflicht und das Verbot der Annahme von Belohnungen, Geschenken und sonstigen Vorteilen. Bei Mitgliedern des gerichtsähnlichen Kontrollorgans, die vor ihrer Ernennung in einem Beamtenverhältnis standen, ruhen für die Dauer der Amtszeit im gerichtsähnlichen Kontrollorgan die Rechte und Pflichten aus dem zuletzt im Beamtenverhältnis auf Lebenszeit übertragenen Amt. Satz 2 gilt entsprechend.

(4) Die Amtszeit verlängert sich um den Zeitraum bis zur Wahl einer Nachfolgerin oder eines Nachfolgers. Bis dahin führen die Mitglieder des gerichtsähnlichen Kontrollorgans ihre Amtsgeschäfte fort.

(5) Verlängert sich die Amtszeit eines Mitglieds des gerichtsähnlichen Kontrollorgans nach Absatz 4, so wird ihm das Amt bis zum Ende des Kalendermonats übertragen, in dem die Geschäftsführung endet.

§ 20

Ruhestand; Ruhegehalt der Mitglieder des gerichtsähnlichen Kontrollorgans

(1) Die Mitglieder des gerichtsähnlichen Kontrollorgans treten mit Ablauf der Amtszeit, spätestens mit Vollendung des 70. Lebensjahres, aus dem Beamtenverhältnis auf Zeit in den Ruhestand. Ein Mitglied des gerichtsähnlichen Kontrollorgans ist auf Antrag aus dem Beamtenverhältnis auf Zeit in den Ruhestand zu versetzen, wenn es das Amt wenigstens

fünf Jahre bekleidet hat und das 67. Lebensjahr vollendet hat. § 52 Absatz 1 des Bundesbeamtengesetzes und § 19 Absatz 4 gelten entsprechend.

(2) Endet die Amtszeit eines richterlichen Mitglieds vor Erreichen der gesetzlichen Regelaltersgrenze nach § 48 Absatz 1 oder 3 des Deutschen Richtergesetzes, ist es auf Antrag auch aus dem Richterverhältnis auf Lebenszeit zu dem Zeitpunkt in den Ruhestand zu versetzen, zu dem sein Amt als Mitglied im gerichtsähnlichen Kontrollorgan nach Absatz 1 endet. Dies gilt entsprechend in Fällen einer Dienstunfähigkeit. § 14 Absatz 3 des Beamtenversorgungsgesetzes ist auf das Ruhegehalt aus dem nach Satz 1 beendeten Richterverhältnis auf Lebenszeit anzuwenden. Die Sätze 1 bis 3 gelten entsprechend für ein Mitglied des gerichtsähnlichen Kontrollorgans, dessen Beamtenverhältnis auf Lebenszeit nach § 19 Absatz 3 für die Dauer der Amtszeit ruht und dessen Amtszeit vor Erreichen der gesetzlichen Regelaltersgrenze nach § 51 Absatz 1 oder 2 des Bundesbeamtengesetzes endet.

(3) Tritt ein Mitglied des gerichtsähnlichen Kontrollorgans aus dem Beamtenverhältnis auf Zeit zu demselben oder einem späteren Zeitpunkt in den Ruhestand, zu dem das nach § 19 Absatz 3 ruhende Richter- oder Beamtenverhältnis auf Lebenszeit durch Eintritt oder Versetzung in den Ruhestand endet, so gilt abweichend von § 54 Absatz 2 Nummer 1 des Beamtenversorgungsgesetzes als Höchstgrenze das Ruhegehalt, das sich unter Zugrundelegung der gesamten ruhegehaltfähigen Dienstzeit und der ruhegehaltfähigen Dienstbezüge aus der Besoldungsgruppe, aus der sich das Ruhegehalt aus dem Beamtenverhältnis auf Zeit berechnet, ergibt, zuzüglich des Unterschiedsbetrags nach § 50 Absatz 1 des Beamtenversorgungsgesetzes.

§ 21

Besoldung der Mitglieder des gerichtsähnlichen Kontrollorgans

(1) Den Mitgliedern des gerichtsähnlichen Kontrollorgans wird vom Beginn des Kalendermonats an, in dem das Beamtenverhältnis auf Zeit beginnt, bis zum Ende des Kalendermonats, in dem das Beamtenverhältnis endet, ein Amt der Besoldungsgruppe B 7 übertragen.

(2) Abweichend von Absatz 1 wird der Präsidentin oder dem Präsidenten ein Amt der Besoldungsgruppe B 9 und der Vizepräsidentin oder dem Vizepräsidenten ein Amt der Besoldungsgruppe B 8 übertragen.

§ 22

Weitere Rechte und Pflichten der Mitglieder des gerichtsähnlichen Kontrollorgans

(1) Die für die Richterinnen und Richter an den obersten Gerichtshöfen des Bundes geltenden Vorschriften über Unabhängigkeit und Disziplinarmaßnahmen sind entsprechend auf die Mitglieder des gerichtsähnlichen Kontrollorgans anzuwenden. Disziplinargericht ist das Dienstgericht des Bundes in der für die Richterinnen und Richter des Bundesgerichtshofs geltenden Besetzung.

(2) Die Mitglieder des gerichtsähnlichen Kontrollorgans sehen von allen Handlungen ab, die mit den Aufgaben ihres Amtes nicht zu vereinbaren sind. § 4 des Deutschen Richtergesetzes gilt entsprechend.

§ 23

Kollegialspruchkörper und Entscheidungen des gerichtsähnlichen Kontrollorgans

(1) Beim gerichtsähnlichen Kontrollorgan bestehen die folgenden Kollegialspruchkörper:

1. Senat des Unabhängigen Kontrollrats und

2. Kammern.

(2) Die Mitglieder des gerichtsähnlichen Kontrollorgans bilden den Senat des gerichtsähnlichen Kontrollorgans. Den Vorsitz im Senat hat die Präsidentin oder der Präsident. Ist die Präsidentin oder der Präsident verhindert, hat die Vizepräsidentin oder der Vizepräsident den Vorsitz.

(3) Der Senat beruft Kammern. Die Kammern des gerichtsähnlichen Kontrollorgans bestehen jeweils mehrheitlich aus richterlichen Mitgliedern des Senats beim Unabhängigen Kontrollrat.

(4) Die Präsidentin oder der Präsident führt den Vorsitz in der Kammer, der sie oder er angehört. Die Vizepräsidentin oder der Vizepräsident führt den Vorsitz in der Kammer, der sie oder er angehört.

(5) Die Entscheidungen der Kollegialspruchkörper des gerichtsähnlichen Kontrollorgans in der Rechtskontrolle ergehen als Beschluss. Die Kollegialspruchkörper sind beschlussfähig, wenn die Mehrheit ihrer Mitglieder anwesend ist. Sie fassen ihre Beschlüsse mit einfacher Stimmenmehrheit. Bei Stimmengleichheit entscheidet die Stimme der oder des Vorsitzenden.

(6) Ein Beschluss des gerichtsähnlichen Kontrollorgans ist zu begründen, wenn

1. das gerichtsähnliche Kontrollorgan die Rechtswidrigkeit feststellt,

2. die Feststellung der Rechtmäßigkeit an bestimmte Maßgaben oder Einschränkungen geknüpft ist oder

3. die Vorlage Besonderheiten tatsächlicher oder rechtlicher Art aufweist oder von grundsätzlicher Bedeutung ist.

§ 24

Beratungsgeheimnis

Die Beratungen der Kollegialspruchkörper unterliegen dem Beratungsgeheimnis. § 43 des Deutschen Richtergesetzes gilt entsprechend.

Unterabschnitt 5

Administratives Kontrollorgan

§ 25

Leitung des administrativen Kontrollorgans; Weisungen

(1) Das administrative Kontrollorgan untersteht einer Leiterin oder einem Leiter. Sie oder er führt die Amtsbezeichnung Leiterin oder Leiter des administrativen Kontrollorgans. Die Leiterin oder der Leiter muss über die Befähigung zum Richteramt verfügen. Sie oder er steht in einem Beamtenverhältnis zum Bund. Ihr oder ihm wird ein Amt der Besoldungsgruppe B 6 übertragen.

(2) Die Leiterin oder der Leiter des administrativen Kontrollorgans unterliegt den Weisungen der Behördenleitung.

(3) Das administrative Kontrollorgan ist verpflichtet, das gerichtsähnliche Kontrollorgan bei der gerichtsähnlichen Kontrolle nach § 2 Absatz 2 Nummer 1 zu unterstützen. Es ist dem gerichtsähnlichen Kontrollorgan nachgeordnet.

§ 26

Prüfprogramm für das administrative Kontrollorgan; Prüfaufträge

(1) Der Senat des gerichtsähnlichen Kontrollorgans beschließt für einen Zeitraum von bis zu 24 Monaten ein Prüfprogramm. Das Prüfprogramm beinhaltet den Rahmen für die strukturbezogene Kontrolle durch das administrative Kontrollorgan. Dem jeweiligen Nachrichtendienst ist vor dem Beschluss Gelegenheit zur Stellungnahme einzuräumen. Der Senat kann jederzeit durch Beschluss ein laufendes Prüfprogramm ändern; in diesem Fall ist Satz 3 entsprechend anwendbar.

(2) Der Unabhängige Kontrollrat unterrichtet den jeweiligen Nachrichtendienst, die zuständige Aufsichtsbehörde sowie das Parlamentarische Kontrollgremium über das Prüfprogramm.

(3) Ein Kollegialspruchkörper des gerichtsähnlichen Kontrollorgans kann konkrete und einzelfallbezogene Prüfaufträge nur zur Durchführung der strategischen Aufklärung nach § 32 des BND-Gesetzes erteilen. Der Unabhängige Kontrollrat unterrichtet den Bundesnachrichtendienst sowie das Bundeskanzleramt über Prüfaufträge.

Abschnitt 3

Ausübung der Rechtskontrolle durch den Unabhängigen Kontrollrat

Unterabschnitt 1

Rechtskontrolle durch das gerichtsähnliche Kontrollorgan; Gefahr im Verzug

§ 27

Vorabkontrolle durch das gerichtsähnliche Kontrollorgan

(1) Die Vorabkontrolle durch das gerichtsähnliche Kontrollorgan umfasst diejenigen Fälle, in denen die Durchführung einer Maßnahme eines Nachrichtendienstes des Bundes unter dem Vorbehalt der Bestätigung der jeweiligen behördlichen Anordnung durch das gerichtsähnliche Kontrollorgan steht. Der Unabhängige Kontrollrat kann in seiner Entscheidung auch Maßgaben und Einschränkungen für die Durchführung einer Maßnahme vorsehen; diese sind bei Durchführung der Maßnahme zu beachten.

(2) Zur Ausübung der Vorabkontrolle legt der jeweilige Nachrichtendienst dem Unabhängigen Kontrollrat die jeweilige behördliche Anordnung vor. Bestätigt der zuständige Kollegialspruchkörper des gerichtsähnlichen Kontrollorgans die Anordnung, so darf der jeweilige Nachrichtendienst die jeweilige Maßnahme durchführen. Bestätigt das gerichtsähnliche Kontrollorgan die Anordnung nicht, so tritt diese außer Kraft.

(3) Das gerichtsähnliche Kontrollorgan ist zuständig für die Vorabkontrolle

1. beim Bundesamt für Verfassungsschutz für die in § 34 des Bundesverfassungsschutzgesetzes genannten Anordnungen und

2. beim Bundesnachrichtendienst

   a) für die in § 98 Absatz 1 des BND-Gesetzes genannten Anordnungen sowie

   b) für die in § 98 Absatz 2 des BND-Gesetzes genannten Anordnungen, wobei die Vorabkontrolle über diese Anordnungen stets durch den Senat zu erfolgen hat.

§ 28

Zuständigkeit für Entscheidungen in der Vorabkontrolle

(1) Der nach Maßgabe des Geschäftsverteilungsplans zuständige Kollegialspruchkörper des gerichtsähnlichen Kontrollorgans kann einem seiner Mitglieder einen Vorgang der Vorabkontrolle nach § 27 Absatz 3 Nummer 1 und 2 Buchstabe a zur alleinigen Entscheidung übertragen. Dies gilt nicht, wenn

1. der jeweilge Nachrichtendienst mit der Vorlage um eine Entscheidung des zuständigen Kollegialspruchkörper ersucht,

2. eine Anordnung einer strategischen Aufklärungsmaßnahme nach § 49 des BND-Gesetzes erstmals zur Entscheidung vorgelegt wird,

3. eine Anordnung Schwierigkeiten tatsächlicher oder rechtlicher Art aufweist oder von grundsätzlicher Bedeutung ist.

(2) Einem Mitglied des Senats beim Unabhängigen Kontrollrat können im ersten Jahr ihrer oder seiner Ernennung keine Einzelentscheidungen übertragen werden.

(3) Jedes Mitglied der zuständigen Kammer des gerichtsähnlichen Kontrollorgans kann einen Vorgang dem Senat vorlegen, wenn es der Auffassung ist, dass eine Angelegenheit von grundsätzlicher Bedeutung vorliegt.

§ 29

Einzelfallkontrolle durch das gerichtsähnliche Kontrollorgan

(1) Die Einzelfallkontrolle durch das gerichtsähnliche Kontrollorgan umfasst diejenigen Fälle, in denen der jeweilige Nachrichtendienst dem gerichtsähnlichen Kontrollorgan einen Vorgang zur Entscheidung über dessen Rechtmäßigkeit vorzulegen hat.

(2) Zur Ausübung der Einzelfallkontrolle legt der jeweilige Nachrichtendienst dem Unabhängigen Kontrollrat ein behördliches Ersuchen zur Durchführung der Einzelfallkontrolle vor.

(3) Das gerichtsähnliche Kontrollorgan ist zuständig für die Einzelfallkontrolle

1. der in § 16 Absatz 3 Satz 4, § 25 Absatz 6 Satz 2 und Absatz 7 Satz 2 und § 35 Absatz 5 des Bundesverfassungsschutzgesetzes genannten Vorgänge und

2. der in § 98 Absatz 3 des BND-Gesetzes genannten Vorgänge.

§ 30

Antrag auf Überprüfung durch den Senat

Innerhalb eines Monats nach Verkündung eines ihn betreffenden Beschlusses kann ein Nachrichtendienst beantragen, dass ein durch eine Kammer getroffener Beschluss durch den Senat überprüft wird. Der Senat entscheidet über den Antrag nach Anhörung des jeweiligen Nachrichtendienstes und der zuständigen Aufsichtsbehörde.

§ 31

Gefahr im Verzug

(1) Würde anderenfalls der Zweck der Maßnahme vereitelt oder wesentlich erschwert, so kann eine Anordnung, die der Vorabkontrolle nach § 27 unterliegt, vom jeweils für die Anordnung zuständigen Nachrichtendienst für sofort vollziehbar erklärt werden.

(2) Die für sofort vollziehbar erklärte Anordnung ist unverzüglich dem Unabhängigen Kontrollrat zur Bestätigung vorzulegen. Der jeweils zuständige Kollegialspruchkörper kann nach Maßgabe des Geschäftsverteilungsplans durch eines seiner Mitglieder entscheiden, wenn kein Fall des § 28 Absatz 1 Satz 2 vorliegt.

(3) Wird eine Anordnung, die nach Absatz 1 für sofort vollziehbar erklärt wurde, nicht binnen drei Werktagen nach Vorlage bestätigt, so tritt sie außer Kraft, es sei denn der Unabhängige Kontrollrat hat nach Absatz 4 die Fortgeltung der sofortigen Vollziehbarkeit der

Anordnung beschlossen. Eine auf Grundlage der Anordnung durchgeführte Maßnahme ist in diesem Fall unverzüglich unter Wahrung der operativen Sicherheit zu beenden.

(4) Ist dem Unabhängigen Kontrollrat eine Entscheidung über die Bestätigung binnen drei Werktagen nicht möglich, insbesondere aufgrund des Umfangs des Vorgangs oder aufgrund von Schwierigkeiten tatsächlicher oder rechtlicher Art, so soll der zuständige Kollegialspruchkörper die Fortgeltung der sofortigen Vollziehbarkeit der Anordnung beschließen, sofern nicht ernstliche Zweifel an der Rechtmäßigkeit der Anordnung bestehen. Die Entscheidung über die Bestätigung hat in diesem Fall unverzüglich zu erfolgen. Wird die für sofort vollziehbar erklärte Anordnung nicht bestätigt, tritt sie außer Kraft. Eine auf Grundlage der Anordnung durchgeführte Maßnahme ist in diesem Fall unverzüglich unter Wahrung der operativen Sicherheit zu beenden.

(5) Tritt die Anordnung nach Absatz 3 oder nach Absatz 4 Satz 3 außer Kraft, sind bereits erhobene personenbezogene Daten unverzüglich zu löschen. Die Löschung unterbleibt, wenn

1. ein Antrag nach Absatz 6 Satz 1 gestellt worden ist oder

2. die Daten für eine Mitteilung an Betroffene oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Anordnung oder des Vorgangs von Bedeutung sein können.

In diesen Fällen ist die Verarbeitung der Daten einzuschränken. Im Falle des Satz 2 Nummer 1 dürfen die Daten nur verwendet werden, wenn der Senat die Anordnung für rechtmäßig erklärt hat. Anderenfalls sind sie unverzüglich zu löschen. Im Falle des Satz 2 Nummer 2 dürfen die Daten nur zu den dort genannten Zwecken verwendet werden.

(6) Ist eine für sofort vollziehbar erklärte Anordnung nach Absatz 3 oder nach Absatz 4 Satz 3 außer Kraft getreten, kann der jeweils betroffene Nachrichtendienst beantragen, dass der Senat die Rechtmäßigkeit der außer Kraft getretenen Anordnung überprüft. In diesen Fällen ist unverzüglich der antragstellende Nachrichtendienst anzuhören. Der Senat entscheidet sodann unverzüglich über die Rechtmäßigkeit der Anordnung. Erklärt der Senat die Anordnung für rechtmäßig, so tritt sie unter Wegfall der Verwendungsbeschränkung nach Absatz 5 Satz 3 wieder in Kraft.

Unterabschnitt 2

Rechtskontrolle durch das administrative Kontrollorgan

§ 32

Administrative Kontrolle

(1) Die administrative Kontrolle erfolgt durch das administrative Kontrollorgan und umfasst

1. die Kontrolle über die Verarbeitung personenbezogener Daten sowie

2. die Kontrolle der erweiterten nachrichtendienstlichen Maßnahmen nach § 60 des Bundesverfassungsschutzgesetzes und nach § 51 des BND-Gesetzes.

(2) Die administrative Kontrolle erfolgt als anlassunabhängige und strukturbezogene Kontrolle im Rahmen des durch das gerichtsähnliche Kontrollorgan nach § 26 Absatz 1 beschlossenen Prüfprogramms, sofern kein Fall des § 26 Absatz 3 vorliegt.

§ 33

Beanstandungen; Unterrichtungen

(1) Stellt das administrative Kontrollorgan einen Verstoß durch einen Nachrichtendienst fest und hilft der jeweilige Nachrichtendienst dem Verstoß nicht ab, kann der Unabhängige Kontrollrat den Verstoß gegenüber der zuständigen Aufsichtsbehörde beanstanden und diese zur Stellungnahme innerhalb einer angemessenen Frist auffordern.

(2) Die zuständige Aufsichtsbehörde gibt eine Stellungnahme ab, in der sie die Maßnahmen darstellen soll, die aufgrund der Beanstandung getroffen worden sind.

(3) Das administrative Kontrollorgan unterrichtet den jeweiligen Nachrichtendienst, wenn beabsichtigte Vorgänge der Datenverarbeitung voraussichtlich gegen die Vorschriften über den Datenschutz verstoßen.

§ 34

Qualifizierter Verstoß; Anweisungen

(1) Stellt das administrative Kontrollorgan einen qualifizierten Verstoß fest und hilft der zuständige Nachrichtendienst dem Verstoß nach § 33 nicht ab, so soll es den Sachverhalt dem Senat vorlegen. Ein qualifizierter Verstoß ist ein Verstoß gegen

1. das Erfordernis einer Vorabkontrolle oder Einzelfallkontrolle,

2. Maßgaben und Einschränkungen, die das gerichtsähnliche Kontrollorgan bei einer Entscheidung im Rahmen der Vorabkontrolle oder der Einzelfallkontrolle vorgesehen hat, oder

3. besondere Regelungen zur Weiterverarbeitung von Daten aus Maßnahmen, die der Vorabkontrolle unterliegen.

(2) Der Senat entscheidet nach Anhörung des Nachrichtendienstes des Bundes, ob der vom administrativen Kontrollorgan festgestellte qualifizierte Verstoß vorliegt. Kommt der Senat zu dem Ergebnis, dass ein solcher Verstoß vorliegt, so kann er gegenüber dem jeweiligen Nachrichtendienst eine Anweisung zur Abhilfe treffen. Der betreffende Nachrichtendienst hat die Anweisung innerhalb einer vom Senat bestimmten Frist umzusetzen. Hat der Senat keine Frist bestimmt, so ist die Anweisung unverzüglich umzusetzen. Kommt der jeweilige Nachrichtendienst der Anweisung zur Abhilfe nicht innerhalb der bestimmten Frist oder, falls keine Frist bestimmt wurde, nicht unverzüglich nach, so ist das Parlamentarische Kontrollgremium hierüber zu unterrichten.

Abschnitt 4

Zusammenarbeit des Unabhängigen Kontrollrats mit dem Parlamentarischen Kontrollgremium

§ 35

Tätigkeitsbericht

(1) Der Unabhängige Kontrollrat erstellt für das Parlamentarische Kontrollgremium in Abständen von nicht mehr als zwölf Monaten einen Bericht über seine Tätigkeit, einschließlich etwaiger Anweisungen (Tätigkeitsbericht).

(2) Der Tätigkeitsbericht wird nach Anhörung der zuständigen Aufsichtsbehörden unter Beachtung des Geheimschutzes erstattet. Er darf sich nur auf Informationen und Gegenstände erstrecken, die der Verfügungsberechtigung der Nachrichtendienste des Bundes unterliegen. Besteht für bestimmte Informationen und Gegenstände keine Verfügungsberechtigung des jeweiligen Nachrichtendienstes des Bundes, so informiert die für diesen Nachrichtendienst zuständige Aufsichtsbehörde den Unabhängigen Kontrollrat. Auf Verlangen des Unabhängigen Kontrollrats ergreift die zuständige Aufsichtsbehörde geeignete Maßnahmen, um das Parlamentarische Kontrollgremium über die Informationen und Gegenstände unterrichten zu dürfen. Angaben zur Kontrolltätigkeit mit Bezug zu dem Einsatz menschlicher Quellen, zu nachrichtendienstlicher Technik und nachrichtendienstlicher Methodik sind allgemein zu halten.

(3) Eine zuständige Aufsichtsbehörde kann die Erstattung des Tätigkeitsberichts oder von Teilen des Tätigkeitsberichts an das Parlamentarische Kontrollgremium untersagen, soweit

1. dies aus Gründen des Wohls des Bundes oder eines Landes, insbesondere aus zwingenden Gründen des Nachrichtenzugangs oder aus Gründen des Schutzes von Persönlichkeitsrechten Dritter, notwendig ist oder

2. der Kernbereich der exekutiven Eigenverantwortung betroffen ist.

Macht eine zuständige Aufsichtsbehörde von diesem Recht Gebrauch, so hat sie dies gegenüber dem Unabhängigen Kontrollrat zu begründen. Erstreckt sich die Ablehnung nur auf Teile des Tätigkeitsberichts, so ist der Tätigkeitsbericht ohne die abgelehnten Teile zu erstatten.

§ 36

Öffentlicher Bericht

(1) Der Unabhängige Kontrollrat erstellt erstmals für den Zeitraum der Kalenderjahre 2028 bis 2030 und im Folgenden für einen Zeitraum von jeweils zwei Jahren unter Beachtung des Geheimschutzes in abstrakter Weise und nach Anhörung der zuständigen Aufsichtsbehörden einen Bericht über seine Tätigkeit in öffentlicher Form (öffentlicher Bericht). § 35 Absatz 3 gilt entsprechend. Der öffentliche Bericht kann Ausführungen zu rechtlichen Bewertungen enthalten, soweit Geheimschutzbelange nicht entgegenstehen.

(2) Der Unabhängige Kontrollrat übermittelt den öffentlichen Bericht dem Deutschen Bundestag und der Bundesregierung und macht ihn der Öffentlichkeit zugänglich. Das

Parlamentarische Kontrollgremium holt vor einer Beratung über den öffentlichen Bericht eine Stellungnahme der Bundesregierung ein.

§ 37

Austausch mit dem Parlamentarischen Kontrollgremium und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Die Rechte des Parlamentarischen Kontrollgremiums zur Kontrolle der Bundesregierung im Hinblick auf die Tätigkeiten der Nachrichtendienste des Bundes bleiben durch die Tätigkeit des Unabhängigen Kontrollrats unberührt.

(2) Der Unabhängige Kontrollrat kann sich mit dem Parlamentarischen Kontrollgremium unter Einhaltung der jeweils geltenden Geheimhaltungsvorschriften im Rahmen der jeweiligen Kontrollzuständigkeit über Angelegenheiten der Kontrolltätigkeit austauschen. § 6 des Kontrollgremiumgesetzes bleibt unberührt. Die Berichtspflichten, die für den Unabhängigen Kontrollrats gegenüber dem Parlamentarischen Kontrollgremium bestehen, bleiben von einem Austausch unberührt.

(3) Der Unabhängige Kontrollrat und die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit können sich regelmäßig unter Wahrung der jeweils geltenden Geheimhaltungsvorschriften im Rahmen ihrer jeweiligen Kontrollzuständigkeit über Angelegenheiten ihrer Kontrolltätigkeit, insbesondere grundsätzliche Fragen der einheitlichen Auslegung datenschutzrechtlicher Bestimmungen austauschen. Ausgenommen bleiben Informationen, die nicht der Verfügungsberechtigung der Nachrichtendienste des Bundes unterliegen.

Abschnitt 5

Sonstige Vorschriften und Schlussvorschriften

§ 38

Individuelles Ersuchen beim Unabhängigen Kontrollrat

Wer der Auffassung ist, durch einen Nachrichtendienst bei dessen Wahrnehmung der in § 2 Absatz 1 bezeichneten Aufgaben in seinen Rechten verletzt worden zu sein, kann den Unabhängigen Kontrollrat um Prüfung ersuchen. In dem Ersuchen sind ein konkreter Sachverhalt und ein substantiiertes Prüfinteresse darzulegen. Der Unabhängige Kontrollrat prüft die ihm übermittelten Ersuchen.

§ 39

Schutz des Eigensicherungsbereichs

(1) Der Unabhängige Kontrollrat hat in seinen Dienststellen, auf seinen Grundstücken und in seinen sonstigen Einrichtungen (Eigensicherungsbereich) zum Schutz seiner Bediensteten, Einrichtungen, Gegenstände und amtlichen Informationen vor sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten spezielle Befugnisse nach Maßgabe der folgenden Absätze. Die Ausübung des Hausrechts bleibt hiervon unberührt.

(2) Der Unabhängige Kontrollrat darf Personen, die seinen Eigensicherungsbereich betreten oder sich dort aufhalten, und von diesen Personen mitgeführte Taschen und sonstige Gegenstände sowie von diesen Personen genutzte Fahrzeuge

1. verdachtsunabhängig kontrollieren (Absatz 3 Satz 1),

2. durchsuchen (Absatz 3 Satz 2), wenn tatsächliche Anhaltspunkte für sicherheitsgefährdende oder geheimdienstliche Tätigkeiten vorliegen.

Er darf die Identität von Personen, die sich im Eigensicherungsbereich aufhalten, feststellen und dazu insbesondere eine Person anhalten, sie nach ihren Personalien befragen und verlangen, dass sie mitgeführte Ausweispapiere zur Prüfung aushändigt.

(3) Eine Kontrolle nach Absatz 2 Satz 1 Nummer 1 ist die oberflächliche Suche nach Gegenständen an Personen, an oder in Taschen oder an oder in mitgeführten Gegenständen und Fahrzeugen auch unter Einsatz technischer Mittel, ohne dass ein Körperkontakt mit der betroffenen Person stattfindet. Eine Durchsuchung nach Absatz 2 Satz 1 Nummer 2 ist die zielgerichtete und planmäßige Suche, auch unter Einsatz technischer Mittel,

1. am äußeren Körper der betroffenen Person,

2. in Kleidung und Taschen der betroffenen Person,

3. an und in Fahrzeugen der betroffenen Person einschließlich der dort mitgeführten Gegenstände sowie

4. in sonstigen mitgeführten Gegenständen der betroffenen Person, die geeignet sind, amtliche Informationen unbefugt aus dem Eigensicherungsbereich zu verbringen oder Gegenstände zu sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten in den Eigensicherungsbereich einzubringen.

(4) Der Unabhängige Kontrollrat darf innerhalb des Eigensicherungsbereichs auch unter Einsatz technischer Mittel verdachtsunabhängig Räume einschließlich der darin vorhandenen Gegenstände kontrollieren und durchsuchen. Zur dauerhaften offenen Überwachung des Eigensicherungsbereichs, darf er optisch-elektronische Einrichtungen nach Maßgabe einer Dienstvorschrift einsetzen. In der Dienstvorschrift sind die Voraussetzungen, das Verfahren und Grenzen der offenen Überwachung zu regeln. Eine Videoüberwachung höchstpersönlich genutzter Räume ist unzulässig. § 24 bleibt unberührt.

(5) Gegenstände, die sich im Eigensicherungsbereich befinden, darf der Unabhängige Kontrollrat sicherstellen und untersuchen, wenn

1. tatsächliche Anhaltspunkte dafür vorliegen, dass Gegenstände für eine sicherheitsgefährdende oder geheimdienstliche Tätigkeit verwendet werden oder mit solchen Tätigkeiten gewonnen worden sind,

2. Gegenstände vorschriftswidrig in den Eigensicherungsbereich eingebracht worden sind oder

3. Gegenstände keiner bestimmten Person zuzuordnen sind und die Sicherstellung und Untersuchung zum Schutz vor einer sicherheitsgefährdenden oder geheimdienstlichen Tätigkeit erforderlich ist.

Bei Geräten der Informations- und Kommunikationstechnik umfasst das Untersuchen auch das Eingreifen mit technischen Mitteln sowie das Verarbeiten der auf dem Gerät gespeicherten Informationen einschließlich personenbezogener Daten.

(6) Personen, die sich im Eigensicherungsbereich aufhalten, sind verpflichtet, Maßnahmen nach den Absätzen 2 und 5 zu dulden. Der Unabhängige Kontrollrat darf Maßnahmen auch in unmittelbarer Nähe des Eigensicherungsbereichs vornehmen im Fall

1. der Absätze 2 und 5 Satz 1 Nummer 1 und 2, wenn die Person sich einer Maßnahme im Eigensicherungsbereich entzieht,

2. des Absatzes 5 Satz 1 Nummer 3, wenn ein solcher Gegenstand in unmittelbarer Nähe des Eigensicherungsbereichs aufgefunden wird.

(7) Der Unabhängige Kontrollrat darf die in Absatz 8 genannten Mittel anwenden

1. zur Unterbindung eines gegenwärtigen oder unmittelbar bevorstehenden oder Beendigung eines erfolgten unbefugten Zutritts zum Eigensicherungsbereich,

2. im Eigensicherungsbereich zur Abwehr einer gegenwärtigen Gefahr für das Leben oder die körperliche Unversehrtheit von Personen oder für Einrichtungen oder Sachen von bedeutendem Wert, die den Aufgaben des Unabhängigen Kontrollrates gewidmet sind,

3. zur Durchsetzung von Maßnahmen nach den Absätzen 2, 5 und 6.

(8) Der Unabhängigen Kontrollrat kann zur Durchsetzung von Maßnahmen nach Absatz 7 folgende Mittel anwenden:

1. unmittelbare Einwirkung auf die betroffene Person oder Gegenstände (körperliche Gewalt) oder Hilfsmittel der körperlichen Gewalt; eine Fesselung der betroffenen Person ist nur dann zulässig, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass sie die mit der Durchsetzung der Maßnahme beauftragten Personen oder Dritte angreifen, Widerstand leisten oder sich der Kontrolle entziehen wird,

2. unmittelbare Einwirkung auf Gegenstände mittels körperlicher Gewalt oder durch Hilfsmittel der körperlichen Gewalt.

Mittel nach Satz 1 dürfen nur durch besonders qualifizierte und geschulte Personen angewandt werden, die durch die Behördenleitung hierzu besonders ermächtigt wurden.

(9) Bei der Durchführung von Maßnahmen nach den Absätzen 2 sowie 4 bis 7 hat der Unabhängige Kontrollrat unter mehreren möglichen und geeigneten Maßnahmen diejenigen zu treffen, die die betroffene Person am wenigsten beeinträchtigen. Eine Maßnahme darf nicht zu einem Nachteil führen, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht.

§ 40

Verfahren im Eigensicherungsbereich

(1) Maßnahmen nach § 39 Absatz 2 Satz 1 Nummer 2 und Absatz 3 und 5 bedürfen der Anordnung der Behördenleitung oder einer von ihr bestimmten Vertretung.

(2) Ist eine Anordnung nach Absatz 1 auf Grund besonderer Eilbedürftigkeit nicht rechtzeitig zu erlangen, kann die Maßnahme auch ohne vorherige Anordnung durchgeführt werden, wenn ansonsten der Zweck der Maßnahme vereitelt oder wesentlich erschwert würde. Bei Geräten der Informations- und Kommunikationstechnik darf in diesem Fall lediglich das Gerät sichergestellt werden. Die Anordnung ist unverzüglich nachzuholen. Wird die Anordnung nach Absatz 1 nicht nachgeholt, so hat der Unabhängige Kontrollrat

unverzüglich bereits erhobene Daten zu löschen und sichergestellte Gegenstände an die betroffene Person herauszugeben.

(3) Sichergestellte Gegenstände sind unverzüglich an die betroffene Person herauszugeben, sobald der Zweck der Sicherstellung entfällt. Satz 1 gilt nicht, wenn die Gegenstände zur Einleitung oder Durchführung eines strafrechtlichen Ermittlungsverfahrens an die Strafverfolgungsbehörden weitergegeben werden müssen.

(4) Bei Maßnahmen nach § 39 Absatz 2 Satz 1 Nummer 2 hat die betroffene Person das Recht, anwesend zu sein. Über eine Durchsuchung nach § 39 Absatz 2 Satz 1 Nummer 2 oder eine Sicherstellung nach § 39 Absatz 5 Satz 1 ist auf Verlangen eine Bescheinigung über die Maßnahme und den Grund der Maßnahme zu erteilen. Maßnahmen nach § 39 Absatz 5, die in Abwesenheit der betroffenen Person durchgeführt worden sind, sind ihr schriftlich mitzuteilen, wenn hierdurch nicht der Zweck der Maßnahme gefährdet wird.

(5) Bei der Untersuchung von Geräten der Informations- und Kommunikationstechnik, die nicht ausschließlich zur dienstlichen Nutzung überlassen wurden, ist sicherzustellen, dass an dem Gerät nur Veränderungen vorgenommen werden, die für die Datenverarbeitung unerlässlich sind. Vorgenommene Veränderungen sind bei Beendigung der Maßnahme, soweit technisch möglich, rückgängig zu machen. Sichergestellte Telekommunikationsendgeräte sind abweichend von Absatz 5 Satz 1 unabhängig von dem Abschluss der Maßnahmen nach § 39 Absatz 5 an die betroffene Person spätestens nach 2 Wochen herauszugeben. Macht die betroffene Person in den Fällen des Satzes 3 Gründe glaubhaft, nach denen für sie eine Aufrechterhaltung der Sicherstellung nicht zumutbar ist, so ist das mobile Endgerät innerhalb von 48 Stunden nach Darlegung dieser Gründe an die betroffene Person zurückzugeben. Der Unabhängige Kontrollrat darf vor der Rückgabe ein Abbild der auf dem Gerät gespeicherten Informationen einschließlich personenbezogener Daten zur Datensicherung erzeugen. Wirkt die betroffene Person nicht an der Erzeugung eines unverschlüsselten Abbildes mit, kann die Herausgabe des Gerätes solange zurückgehalten werden, bis ein unverschlüsseltes Abbild erzeugt ist.

(6) Die Datenerhebung zum Zweck der Erlangung von Erkenntnissen über den Kernbereich privater Lebensgestaltung ist unzulässig. Der Unabhängige Kontrollrat darf Erkenntnisse, die den Kernbereich privater Lebensgestaltung berühren, nicht verarbeiten, weitergeben oder in anderer Weise nutzen. Der Unabhängige Kontrollrat hat, soweit möglich, technisch oder auf sonstige Weise sicherzustellen, dass Erkenntnisse, die den Kernbereich privater Lebensgestaltung berühren, nicht erlangt werden. Soweit Erkenntnisse erlangt wurden, die den Kernbereich privater Lebensgestaltung betreffen, sind diese Daten unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist nach Ablauf von sechs Monaten zu löschen.

(7) Widerspruch und Anfechtungsklage gegen Maßnahmen nach § 39 haben keine aufschiebende Wirkung. Das Bundesverwaltungsgericht entscheidet im ersten und letzten Rechtszug über Klagen gegen Maßnahmen nach § 39.

§ 41

Evaluationsbericht

Der Unabhängige Kontrollrat erstellt zum 1. Januar 2030 einen Bericht zur Evaluierung der Effektivität seiner Kontrolltätigkeit und übermittelt diesen Bericht dem Parlamentarischen Kontrollgremium. Die zuständigen Aufsichtsbehörden erhalten vorab die Gelegenheit zur Stellungnahme zu diesem Bericht. § 35 Absatz 3 gilt entsprechend.

§ 42

Übergangsregelungen

(1) Dieses Gesetz gilt für den durch das Gesetz zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts vom 19. April 2021 (BGBl. I S. 771) errichteten Unabhängigen Kontrollrat.

(2) [Für Mitglieder des gerichtsähnlichen Kontrollorgans, die bis zum 31. Dezember 2026 zur Beamtin oder zum Beamten auf Zeit im gerichtsähnliche Kontrollorgans ernannt wurden, gelten die Regelung des § 45 Absatz 4 Satz 2 des BND-Gesetzes in der bis zum 31. Dezember 2026 geltenden Fassung.]

(3) [Die Prüfung von individuellen Ersuchen nach § 38 beginnt zum 1. Januar 2029.]

Artikel 4

Änderung des Bundesverfassungsschutzgesetzes zum 1. Januar 2030

Das Bundesverfassungsschutzgesetz vom … [einsetzen: Ausfertigungsdatum und Fundstelle des Bundesverfassungsschutzgesetzes nach Artikel 1 dieses Gesetzes] wird wie folgt geändert:

§ 80 Absatz 5 wird gestrichen.

Artikel 5

Änderung des Gesetzes über die Kontrolle von Kriegswaffen

Das Gesetz über die Kontrolle von Kriegswaffen in der Fassung der Bekanntmachung vom 22. November 1990 (BGBl. I S. 2506), das zuletzt durch Artikel 1 der Verordnung vom 19. Februar 2025 (BGBl. 2025 I Nr. 47) geändert worden ist, wird wie folgt geändert:

Nach § 15 Absatz 1 wird der folgende Absatz 1a eingefügt:

„(1a) Die §§ 2 bis 4a und 12 gelten nicht für den Bundesnachrichtendienst.“

Artikel 6

Änderung des Informationsfreiheitsgesetzes

Das Informationsfreiheitsgesetz vom 5. September 2005 (BGBl. I S. 2722), das zuletzt durch Artikel 44 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:

§ 3 wird wie folgt geändert:

1. Nummer 8 wird durch die folgende Nummern 8 und 9 ersetzt:

„8. gegenüber

a) den Nachrichtendiensten des Bundes,

b) dem Bundeskanzleramt, dem Bundesministerium des Innern und dem Bundesministerium der Verteidigung in deren Eigenschaften als zuständige Aufsichtsbehörden über die Nachrichtendienste und im Fall des Bundeskanzleramtes auch als Koordinierungsstelle über die Nachrichtendienste,

c) dem Unabhängigen Kontrollrat in dessen Eigenschaft als Kontrollbehörde über die Nachrichtendienste des Bundes,

d) sowie anderen Behörden und sonstigen öffentlichen Stellen des Bundes, soweit sie Aufgaben im Sinne des § 10 Nummer 3 des Sicherheitsüberprüfungsgesetzes wahrnehmen.“

2. Nach Nummer 8 wird folgende Nummer 9 eingeführt:

„9. wenn die Information Vorgänge oder Tätigkeiten von in Nummer 8 Buchstabe a genannten Stellen betrifft, insbesondere von diesen stammt oder deren Tätigkeit abbildet oder Rückschlüsse auf diese zulässt.“

Artikel 7

Änderung des Beamtenversorgungsgesetzes

Das Beamtenversorgungsgesetz in der Fassung der Bekanntmachung vom 24. Februar 2010 (BGBl. I S. 150), das zuletzt durch Artikel 11 des Gesetzes vom 27. Februar 2025 (BGBl. 2025 I Nr. 72) geändert worden ist, wird wie folgt geändert:

In § 31a Absatz 1 Satz 2 wird nach der Angabe „Eine besondere Verwendung im Ausland“ die Angabe „im Sinne des Satzes 1“ eingefügt.

Artikel 8

Änderung des Bundesbesoldungsgesetzes

Das Bundesbesoldungsgesetz in der Fassung der Bekanntmachung vom 19. Juni 2009 (BGBl. I S. 1434), das zuletzt durch Artikel 62 Absatz 2 des Gesetzes vom 4. Februar 2026 (BGBl. 2026 I Nr. 33) geändert worden ist, wird wie folgt geändert:

Nach § 56 Absatz 2 Satz 2 Nummer 2 wird die folgende Nummer 3 eingefügt:

„3. Angehörige des Bundesnachrichtendienstes, wenn das Bundeskanzleramt eine Maßnahme als entsprechende Verwendung festgelegt hat.“

Artikel 9

Änderung des Bundespersonalvertretungsgesetzes

Das Bundespersonalvertretungsgesetz vom 9. Juni 2021 (BGBl. I S. 1614), das zuletzt durch Artikel 13 des Gesetzes vom 9. Januar 2026 (BGBl. 2026 I Nr. 7) geändert worden ist, wird wie folgt geändert:

1. § 112 Absatz 4 Satz 7 wird durch den folgenden Satz ersetzt:

   „§ 55 Absatz 2 gilt nicht für die an einer Dienststelle des Bundesnachrichtendienstes im Ausland eingesetzten Beschäftigten.“

2. Nach § 113 Absatz 3 wird der folgende Absatz 4 eingefügt:

   „(4) Die Mitgliedschaft im Personalrat ruht bei Personen, die zu einer sicherheitsempfindlichen Tätigkeit nicht zugelassen sind.“

Artikel 10

Änderung des Vereinsgesetzes

Das Vereinsgesetz vom 5. August 1964 (BGBl. I S. 593), das zuletzt durch Artikel 5 des Gesetzes vom 30. November 2020 (BGBl. I S. 2600) geändert worden ist, wird wie folgt geändert:

§ 20 wird wie folgt geändert:

1. Absatz 1 wird wie folgt geändert:

   a) Satz 1 Nummer 4 und 5 wird durch die folgenden Nummern 4 bis 6 ersetzt:

      „4. einem vollziehbaren Verbot nach § 14 Absatz 3 Satz 1 oder § 18 Satz 2 zuwiderhandelt,

      5. Kennzeichen einer der in den Nummern 1 und 2 bezeichneten Vereine oder Parteien oder eines von einem Betätigungsverbot nach § 15 Absatz 1 in Verbindung mit § 14 Absatz 3 Satz 1 betroffenen Vereins während der Vollziehbarkeit des Verbots oder der Feststellung verbreitet oder öffentlich oder in einer Versammlung oder in einem von ihm verbreiteten Inhalt (§ 11 Absatz 3 des Strafgesetzbuches) verwendet oder

      6. einen Inhalt (§ 11 Absatz 3 des Strafgesetzbuches), der ein derartiges Kennzeichen darstellt oder enthält, zur Verbreitung oder Verwendung im Inland oder Ausland in der in Nummer 5 bezeichneten Art und Weise während der Vollziehbarkeit des Verbots oder der Feststellung herstellt, vorrätig hält, einführt oder ausführt,“.

   b) In Satz 2 wird nach der Angabe „Nummer 5“ die Angabe „und 6“ eingefügt.

2. In Absatz 3 wird die Angabe „Nr. 5“ durch die Angabe „Nummer 5 oder 6“ ersetzt.

Artikel 11

Änderung des Bundeskriminalamtgesetzes

Das Bundeskriminalamtgesetz vom 1. Juni 2017 (BGBl. I S. 1354; 2019 I S. 400), das zuletzt durch Artikel 11 des Gesetzes vom 23. April 2026 (BGBl. 2026 I Nr. 111) geändert worden ist, wird wie folgt geändert:

1. In § 33b Absatz 2 wird Satz 1 durch den folgenden Satz ersetzt:

   „Ausschreibungen des Bundesamtes für Verfassungsschutz nach § 10 Absatz 3 Satz 2 des Bundesverfassungsschutzgesetzes in Verbindung mit Artikel 36 Absatz 4 der Verordnung (EU) 2018/1862, nach § 4 Absatz 6 des MAD-Gesetzes in Verbindung mit Artikel 36 Absatz 4 der Verordnung (EU) 2018/1862 sowie des Bundesnachrichtendienstes nach § 11 Absatz 3 Satz 2 des BND-Gesetzes in Verbindung mit Artikel 36 Absatz 4 der Verordnung (EU) 2018/1862 erfolgen durch das Bundeskriminalamt in Amtshilfe im polizeilichen Informationsverbund.“

2. § 76 Absatz 4 wird durch den folgenden Absatz 4 ersetzt:

   „(4) Die Absätze 1 bis 3 sind nicht anzuwenden auf Ausschreibungen die veranlasst sind vom

   1. Bundesamtes für Verfassungsschutz nach § 10 Absatz 3 Satz 2 des Bundesverfassungsschutzgesetzes

   2. Militärischen Abschirmdienst nach § 4 Absatz 6 des MAD-Gesetzes und

   3. Bundesnachrichtendienst nach § 11 Absatz 3 des BND-Gesetzes.“.

Artikel 12

Änderung des Hochschulstatistikgesetzes

Das Hochschulstatistikgesetz vom 2. November 1990 (BGBl. I S. 2414), das zuletzt durch Artikel 3 des Gesetzes vom 7. Dezember 2016 (BGBl. I S. 2826) geändert worden ist, wird wie folgt geändert:

§ 2 wird durch folgenden § 2 ersetzt:

„§ 2

Erhebungsbereich

(1) Die Erhebungen erstrecken sich auf:

1. Hochschulen einschließlich der Hochschulkliniken und sonstiger der Ausbildung von Studenten dienenden Krankenanstalten,

2. staatliche und kirchliche Prüfungsämter, soweit sie Prüfungen abnehmen, die ein Studium an den Nummer 1 genannten Einrichtungen abschließen, und

3. Berufsakademien.

(2) Die Erhebung nach Absatz 1 erstreckt sich nicht auf Daten von Studierenden, Prüfungsteilnehmenden sowie Exmatrikulierten, die für die Nachrichtendienste des Bundes und der Länder ausgebildet werden.“

Artikel 13

Änderung des Aufenthaltsgesetzes

Das Aufenthaltsgesetz in der Fassung der Bekanntmachung vom 25. Februar 2008 (BGBl. I S. 162), das zuletzt durch Artikel 2 des Gesetzes vom 23. April 2026 (BGBl. 2026 I Nr. 111) geändert worden ist, wird wie folgt geändert:

§ 54 Absatz 1 Nummer 2a wird durch die folgende Nummer 2a ersetzt:

„2a. die Sicherheit der Bundesrepublik Deutschland gefährdet; hiervon ist auszugehen, wenn Tatsachen die Schlussfolgerung rechtfertigen, dass

a) er einer Vereinigung im Sinne des § 129 des Strafgesetzbuches angehört oder angehört hat oder

b) er eine nach den §§ 98 oder 99 des Strafgesetzbuches strafbare Handlung vorbereitet, vorbereitet hat, ausübt oder ausgeübt hat,“.

Artikel 14

Änderung der Verwaltungsgerichtsordnung

Die Verwaltungsgerichtsordnung in der Fassung der Bekanntmachung vom 19. März 1991 (BGBl. I S. 686), die zuletzt durch Artikel 9 des Gesetzes vom 20. Mai 2026 (BGBl. 2026 I Nr. 152) geändert worden ist, wird wie folgt geändert:

1. § 48 Absatz 2 wird durch den folgenden Absatz 2 ersetzt:

„(2) Das Oberverwaltungsgericht entscheidet im ersten Rechtszug ferner über

1. Klagen gegen die von einer obersten Landesbehörde nach § 3 Absatz 2 Nummer 1 des Vereinsgesetzes ausgesprochenen Vereinsverbote und die nach § 8 Absatz 2 Satz 1 des Vereinsgesetzes erlassenen Verfügungen,

2. Klagen, die die Aufgabenwahrnehmung der Verfassungsschutzbehörden des Bundes und der Länder nach § 2 Absatz 1 und 4 des Bundesverfassungsschutzgesetzes oder des Militärischen Abschirmdienstes nach § 2 Absatz 1 und 4 des MAD-Gesetzes betreffen.“

2. Nach § 50 Nummer 2 werden die folgenden Nummern 2a und 2b eingefügt:

„2a. über Feststellungsanträge nach § 34 Absatz 4 des Bundesverfassungsschutzgesetzes und über Klagen gegen die Information der Öffentlichkeit nach § 45 des Bundesverfassungsschutzgesetzes darüber, dass eine Vereinigung

verfassungsfeindliche Bestrebungen (§ 3 Absatz 4 Nummer 1 des Bundesverfassungsschutzgesetzes) ausführt oder ein Verdachtsfall ist,

2b über Klagen gegen Maßnahmen nach § 39 UKRat-Gesetz.“

Artikel 15

Änderung der Abgabenordnung

Die Abgabenordnung in der Fassung der Bekanntmachung vom 23. Januar 2025 (BGBl. 2025 I Nr. 24), die zuletzt durch Artikel 13 des Gesetzes vom 22. Juni 2026 (BGBl. 2026 I Nr. 192) geändert worden ist, wird wie folgt geändert:

§ 93 Absatz 8 Satz 1 Nummer 3 wird durch die folgende Nummer 3 ersetzt:

„3. den Verfassungsschutzbehörden des Bundes und der Länder, dem Militärischen Abschirmdienst und dem Bundesnachrichtendienst, soweit dies im Einzelfall für ihre gesetzlichen Aufgaben erforderlich ist.“

Artikel 16

Änderung des Zollverwaltungsgesetzes

Das Zollverwaltungsgesetz vom 21. Dezember 1992 (BGBl. I S. 2125; 1993 I S. 2493), das zuletzt durch Artikel 2 Absatz 8 des Gesetzes vom 20. März 2026 (BGBl. 2026 I Nr. 95) geändert worden ist, wird wie folgt geändert:

§ 12a wird wie folgt geändert:

1. Nach Absatz 3 wird der folgende Absatz 3a eingefügt:

„(3a) Bedienstete des Bundesnachrichtendienstes sind von den Verpflichtungen des Absatzes 1 ausgenommen und befugt, Barmittel und gleichgestellte Zahlungsmittel im Gesamtwert von 10 000 Euro oder mehr in den, aus dem oder durch den Geltungsbereich dieses Gesetzes zu verbringen.“

2. In Absatz 8 Satz 4 wird die Angabe „§ 10 des BND-Gesetzes“ durch die Angabe „den §§ 10 und 11 des BND-Gesetzes“ ersetzt.

Artikel 17

Änderung des Geldwäschegesetzes

Das Geldwäschegesetz vom 23. Juni 2017 (BGBl. I S. 1822), das zuletzt durch Artikel 15 des Gesetzes vom 22. Juni 2026 (BGBl. 2026 I Nr. 192) geändert worden ist, wird wie folgt geändert:

1. Nach § 8 Absatz 1 Satz 3 wird der folgende Satz eingefügt:

„Stehen überwiegende Sicherheitsinteressen der Bundesrepublik Deutschland der Aufzeichnung oder Aufbewahrung der Identität des Vertragspartners entgegen, so kann die Aufzeichnung und Aufbewahrung auch dergestalt erfolgen, dass eine eindeutige Identifizierung des Vertragspartners nicht möglich ist.“

2. § 26a Absatz 1 Nummer 8 wird durch die folgende Nummer 8 ersetzt:

„3. den Bundesnachrichtendienst, soweit tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall zur Erfüllung seiner Aufgaben erforderlich ist,“.

Artikel 18

Änderung des Zehnten Buches Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz

Das Zehnte Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), das zuletzt durch … geändert worden ist, wird wie folgt geändert:

§ 72 wird wie folgt geändert:

1. Absatz 1 wird wie folgt geändert:

a) Absatz 1 Satz 2 wird durch folgenden Satz ersetzt:

„Die Übermittlung ist auf Angaben über Name und Vorname sowie früher geführte Namen, Geburtsdatum, Geburtsort, derzeitige und frühere Anschriften der betroffenen Person, Namen und Anschriften ihrer derzeitigen und früheren Arbeitgeber, derzeitige und frühere berufliche Tätigkeiten sowie schulische, akademische und berufliche Abschlüsse, Lichtbilder nach § 291a des Fünften Buches Sozialgesetzbuch sowie die Anga-be, welche laufenden Geldleistungen die betreffende Person erhält, beschränkt.“

b) Nach Satz 2 wird folgende Satz eingefügt:

„Über die Angaben nach Satz 1 hinaus sind auch Angaben zur Staatsangehörigkeit und Angaben über Geldleistungen, die an betroffene Personen erbracht worden oder zu erbringen sind, zulässig, wenn die Übermittlung erfolgt für die Erfüllung einer Aufgabe

1. der Behörden für Verfassungsschutz zur Aufklärung von wenigstens erheblich beobachtungsbedürftigen Bedrohungen (§ 3 Absatz 7 und 8 des Bundesverfassungsschutzgesetzes),

2. des Bundesnachrichtendienstes zur Aufklärung von wenigstens erheblichen Bedrohungen (§§ 3, 4 des BND-Gesetzes),

3. des Militärischen Abschirmdienstes zur Aufklärung nach § 8 Absatz 2 oder 3 des MAD-Gesetzes,

4. des Bundeskriminalamtes seine Aufgaben nach den §§ 4 bis 8 des BKA-Gesetzes.“

2. Nach Absatz 2 wird der folgende Absatz 3 eingefügt:

„(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt abweichend von § 67d Absatz 1 Satz 1 der Dritte, an den die Daten übermittelt werden. Die übermittelnde Stelle prüft nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten liegt, an den die Daten übermittelt werden, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. Die ersuchende Stelle hat bei ihrem Ersuchen insbesondere anzugeben, für welche ihrer gesetzlichen Aufgaben die Übermittlung der Daten erforderlich ist.“

Artikel 19

Folgeänderungen …

Artikel 20

Außerkrafttreten

Am … [einsetzen: Datum des Tages nach der Verkündung dieses Gesetzes] treten außer Kraft:

1. das Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 295), das zuletzt durch … geändert worden ist,

2. das BND-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch … geändert worden ist und

3. das Artikel 10-Gesetz vom 26. Juni 2001 (BGBl. I S. 1254, 2298; 2017 I S. 154), das zuletzt durch … geändert worden ist.

Artikel 21

Inkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am … [einsetzen: Datum nach des Tages nach der Verkündung dieses Gesetzes] in Kraft.

(2) Artikel 4 tritt am 1. Januar 2030 in Kraft.

Anlage 1

(zu § 48 Absatz 2 Nummer 2 BVerfSchG)

1. Aufstacheln zum Verbrechen der Aggression (§ 80a StGB)

2. Vorbereitung eines hochverräterischen Unternehmens (§ 83 Absatz 2 StGB)

3. Fortführung einer für verfassungswidrig erklärten Partei (§ 84 Absatz 1 Satz 1, Absatz 2 und 3 StGB)

4. Verstoß gegen ein Vereinigungsverbot (§ 85 Absatz 1 StGB)

5. Agententätigkeit zu Sabotagezwecken (§ 87 StGB)

6. Ausübung fremder Einflussnahme und darauf gerichtete Agententätigkeit (§ 87a StGB)

7. Verfassungsfeindliche Sabotage (§ 88 StGB)

8. Verunglimpfung des Bundespräsidenten (§ 90 Absatz 1 und 3 StGB)

9. Verunglimpfung des Staates und seiner Symbole für extremistische Bestrebungen (§ 90a Absatz 3 StGB)

10. Verfassungsfeindliche Verunglimpfung von Verfassungsorganen (§ 90b Absatz 1 StGB)

11. Offenbaren von Staatsgeheimnissen (§ 95 Absatz 1 StGB)

12. Landesverräterische Ausspähung; Auskundschaften von Staatsgeheimnissen (§ 96 Absatz 2 Satz 1 StGB)

13. Preisgabe von Staatsgeheimnissen (§ 97 Absatz 1 StGB)

14. Landesverräterische Agententätigkeit (§ 98 Absatz 1 Satz 1 StGB)

15. Landesverräterische Fälschung (§ 100a Absatz 1 und 2 StGB)

16. Angriff gegen Organe und Vertreter ausländischer Staaten (§ 102 Absatz 1 erste Alternative StGB)

17. Nötigung des Bundespräsidenten und von Mitgliedern eines Verfassungsorgans (§ 106 Absatz 1 StGB)

18. Wahlbehinderung (§ 107 Absatz 1 StGB)

19. Wahlfälschung (§ 107a Absatz 2 StGB)

20. Wählernötigung (§ 108 Absatz 1 StGB)

21. Störpropaganda gegen die Bundeswehr (§ 109d Absatz 1 StGB)

22. Sabotagehandlungen an Verteidigungsmitteln (§ 109e Absatz 1 und 2 StGB)

23. Sicherheitsgefährdender Nachrichtendienst (§ 109f Absatz 1 StGB)

24. Sicherheitsgefährdendes Abbilden (§ 109g Absatz 1 StGB)

25. Anwerben für fremden Wehrdienst (§ 109h Absatz 1 StGB)

26. Öffentliche Aufforderung zu Straftaten (§ 111 Absatz 1 StGB), sofern die rechtswidrige Tat, zu der aufgefordert wird, eine besonders schwere Straftat im Sinne dieser Vorschrift ist

27. Betreiben krimineller Handelsplattformen im Internet (§ 127 Absatz 1 StGB), sofern die rechtswidrige Tat im Sinne des § 127 Absatz 1 Satz 2 eine besonders schwere Straftat im Sinne dieser Vorschrift ist

28. Bildung krimineller Vereinigungen (§ 129 Absatz 1 Satz 1 in Verbindung mit Absatz 5 Satz 1 und 2 StGB)

29. Bildung terroristischer Vereinigungen (§ 129a Absatz 3 und 5 Satz 1 zweite Alternative sowie Satz 2 StGB)

30. Sexueller Missbrauch von Schutzbefohlenen (§ 174 Absatz 1 und 2 StGB)

31. Sexueller Missbrauch von Gefangenen, behördlich Verwahrten oder Kranken und Hilfsbedürftigen in Einrichtungen (§ 174a Absatz 1 und Absatz 2 StGB)

32. Sexueller Missbrauch unter Ausnutzung einer Amtsstellung (§ 174b Absatz 1 StGB)

33. Sexueller Missbrauch unter Ausnutzung eines Beratungs-, Behandlungs- oder Betreuungsverhältnisses (§ 174c Absatz 1 und 2 StGB)

34. Sexueller Übergriff; sexuelle Nötigung; Vergewaltigung (§ 177 Absatz 1 und 2 StGB)

35. Förderung sexueller Handlungen Minderjähriger (§ 180 Absatz 2 StGB)

36. Zuhälterei (§ 181a Absatz 1 StGB)

37. Sexueller Missbrauch von Jugendlichen (§ 182 Absatz 1 und 2 StGB)

38. Aussetzung (§ 221 Absatz 1 StGB)

39. Menschenhandel (§ 232 Absatz 1 StGB)

40. Verschleppung (§ 234a Absatz 3 StGB)

41. Zerstörung wichtiger Arbeitsmittel (§ 305 a Absatz 1 StGB)

42. Gefährliche Eingriffe in den Straßenverkehr (§ 315b Absatz 1 und 2 StGB)

43. Störung öffentlicher Betriebe (§ 316b Absatz 1 und 2 StGB)

44. Störung von Telekommunikationsanlagen (§ 317 Absatz 1 und 2 StGB)

45. Beschädigung wichtiger Anlagen (§ 318 Absatz 1 StGB)

46. Bestechlichkeit (§ 332 Absatz 1 Satz 1), auch in Verbindung mit § 336 (Unterlassen der Diensthandlung),

47. § 18 Absatz 1 bis 5 und 9 des Außenwirtschaftsgesetzes,

48. § 19 Absatz 1 des Gesetzes über die Kontrolle von Kriegswaffen,

49. § 20a Absatz 1 des Gesetzes über die Kontrolle von Kriegswaffen,

50. § 22a Absatz 1 des Gesetzes über die Kontrolle von Kriegswaffen,

51. § 51 Absatz 1 des Waffengesetzes,

52. § 52 Absatz 1 des Waffengesetzes,

53. § 16 Absatz 1 des Ausführungsgesetzes zum Chemiewaffenübereinkommen.

Anlage 2

(zu § 81 Absatz 2 Nummer 2 BNDG)

1. Aufstacheln zum Verbrechen der Aggression (§ 80a StGB),
2. Vorbereitung eines hochverräterischen Unternehmens (§ 83 Absatz 2 StGB),
3. Fortführung einer für verfassungswidrig erklärten Partei (§ 84 Absatz 1 Satz 1, Absatz 2 und 3 StGB),
4. Verstoß gegen ein Vereinigungsverbot (§ 85 Absatz 1 StGB),
5. Agententätigkeit zu Sabotagezwecken (§ 87 StGB),
6. Ausübung fremder Einflussnahme und darauf gerichtete Agententätigkeit (§ 87a StGB),
7. Verfassungsfeindliche Sabotage (§ 88 StGB),
8. Verunglimpfung des Bundespräsidenten (§ 90 Absatz 1 und 3 StGB),
9. Verunglimpfung des Staates und seiner Symbole (§ 90a Absatz 3 StGB),
10. Verfassungsfeindliche Verunglimpfung von Verfassungsorganen (§ 90b Absatz 1 StGB)
11. Offenbaren von Staatsgeheimnissen (§ 95 Absatz 1 StGB),
12. Landesverräterische Ausspähung; Auskundschaften von Staatsgeheimnissen (§ 96 Absatz 2 Satz 1 StGB),
13. Preisgabe von Staatsgeheimnissen (§ 97 Absatz 1 StGB),
14. Landesverräterische Agententätigkeit (§ 98 Absatz 1 Satz 1 StGB),
15. Landesverräterische Fälschung (§ 100a Absatz 1 und 2 StGB),
16. Angriff gegen Organe und Vertreter ausländischer Staaten (§ 102 Absatz 1 erste Alternative StGB),
17. Nötigung des Bundespräsidenten und von Mitgliedern eines Verfassungsorgans (§ 106 Absatz 1 StGB),
18. Wahlbehinderung (§ 107 Absatz 1 StGB),
19. Wahlfälschung (§ 107a Absatz 1 und 2 StGB),
20. Wählernötigung (§ 108 Absatz 1 StGB),
21. Störpropaganda gegen die Bundeswehr (§ 109d Absatz 1 StGB),
22. Sabotagehandlungen an Verteidigungsmitteln (§ 109e Absatz 1 und 2 StGB),
23. Sicherheitsgefährdender Nachrichtendienst (§ 109f Absatz 1 StGB),
24. Sicherheitsgefährdendes Abbilden (§ 109g Absatz 1 und 3 StGB),

25. Anwerben für fremden Wehrdienst (§ 109h Absatz 1 StGB)

26. Öffentliche Aufforderung zu Straftaten (§ 111 Absatz 1 StGB), sofern die rechtswidrige Tat, zu der aufgefordert wird, eine besonders schwere Straftat im Sinne dieser Vorschrift ist,

27. Betreiben krimineller Handelsplattformen im Internet (§ 127 StGB), sofern die rechtswidrige Tat im Sinne des § 127 Absatz 1 Satz 2 eine besonders schwere Straftat im Sinne dieser Vorschrift ist,

28. Bildung krimineller Vereinigungen (§ 129 Absatz 1 Satz 1 in Verbindung mit Absatz 5 Satz 1 und Satz 2 StGB),

29. Bildung terroristischer Vereinigungen (§ 129a Absatz 3 und 5 Satz 1 zweite Alternative sowie Satz 2 StGB),

30. Sexueller Missbrauch von Schutzbefohlenen (§ 174 Absatz 1 und 2 StGB),

31. Sexueller Missbrauch von Gefangenen, behördlich Verwahrten oder Kranken und Hilfsbedürftigen in Einrichtungen (§ 174a Absatz 1 und 2 StGB),

32. Sexueller Missbrauch unter Ausnutzung einer Amtsstellung (§ 174b Absatz 1 StGB),

33. Sexueller Missbrauch unter Ausnutzung eines Beratungs-, Behandlungs- oder Betreuungsverhältnisses (§ 174c Absatz 1 und Absatz 2 StGB),

34. Sexueller Übergriff; sexuelle Nötigung; Vergewaltigung (§ 177 Absatz 1 und 2 StGB)

35. Förderung sexueller Handlungen Minderjähriger (§ 180 Absatz 2 StGB),

36. Zuhälterei (§ 181a Absatz 1 StGB),

37. Sexueller Missbrauch von Jugendlichen (§ 182 Absatz 1 und 2 StGB),

38. Aussetzung (§ 221 Absatz 1 StGB),

39. Menschenhandel (§ 232 Absatz 1 StGB),

40. Verschleppung (§ 234a Absatz 3 StGB),

41. Zerstörung wichtiger Arbeitsmittel (§ 305a Absatz 1 StGB),

42. Gefährliche Eingriffe in den Straßenverkehr (§ 315b Absatz 1 und 2 StGB),

43. Störung öffentlicher Betriebe (§ 316b Absatz 1 und 2 StGB),

44. Störung von Telekommunikationsanlagen (§ 317 Absatz 1 und 2 StGB),

45. Beschädigung wichtiger Anlagen (§ 318 Absatz 1 StGB),

46. Bestechlichkeit (§ 332 Absatz 1 Satz 1 StGB), auch in Verbindung mit einem Unterlassen der Diensthandlung (§ 336 StGB),

47. § 18 Absatz 1 bis 5 jeweils in Verbindung mit Absatz 6 und Absatz 9 des Außenwirtschaftsgesetzes,

48. § 19 Absatz 1 des Gesetzes über die Kontrolle von Kriegswaffen,

49. § 20a Absatz 1 des Gesetzes über die Kontrolle von Kriegswaffen,
50. § 22a Absatz 1 des Gesetzes über die Kontrolle von Kriegswaffen,
51. § 51 Absatz 1 des Waffengesetzes,
52. § 52 Absatz 1 des Waffengesetzes,
53. § 16 Absatz 1 des Ausführungsgesetzes zum Chemiewaffenübereinkommen,
54. § 18 des Transplantationsgesetzes.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Der Gesetzentwurf soll das Nachrichtendienstrecht umfassend reformieren. Hierbei soll die Rechtsprechung des Bundesverfassungsgerichts umgesetzt werden. Zugleich wird die Rechtsmaterie umfassend und nachhaltig fortentwickeln. Zum Schutz der Bürger und zentraler Gemeinwohlinteressen soll nachrichtendienstliche Tätigkeit des Bundesamtes für Verfassungsschutz im Inland und des Bundesnachrichtendienstes im Ausland im rechtsstaatlichen Rahmen wirksam, zeitgemäß und zukunftsfest gestaltet werden.

II. Wesentlicher Inhalt des Entwurfs

Das Nachrichtendienstrecht ist seit der Neuregelung mit dem Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990 (BGBl. I 2954) vielfach geändert worden, meist mit partikulärem Ansatz aktuellen Anlässen folgend. Im Ergebnis weist die Rechtsmaterie Wertungsbrüche auf und eine leitende Systematik mit zukunftsfester Ausrichtung fehlt.

Das Bundesverfassungsgericht hat insbesondere mit seinem Grundsatzurteil vom 26. April 2022 (BVerfGE 162, 1) zum Bayerischen Verfassungsschutzgesetz grundlegende Vorgaben zum Nachrichtendienstrecht getroffen (nachfolgend in BVerfGE 163, 43 [Bundesverfassungsschutzgesetz – Übermittlungsbefugnisse] bestätigt und in BVerfGE 169, 130 [Hess. Verfassungsschutzgesetz] teilweise konkretisiert). Der Gesetzentwurf setzt diese verfassungsgerichtlichen Vorgaben zum Einsatz nachrichtendienstlicher Mittel und den nötigen Verfahrenssicherungen sowie der gebotenen Nachjustierung von Übermittlungsbefugnissen um. Zudem enthält der Entwurf des BND-Gesetzes eine umfassende Regelung der Auslandstätigkeit des Bundesnachrichtendienstes, wobei eine eigene Schwellensystematik geschaffen wurde, um die aufgrund der unterschiedlichen Staatsferne differenzierte Grundrechtsrelevanz von In- und Auslandshandeln abzubilden.

Der Gesetzentwurf ist insgesamt darauf ausgerichtet, den Schutz der herausragenden Gemeinwohlinteressen, denen nachrichtendienstliche Bedrohungsaufklärung dient (BVerfGE 155, 119 - Rn. 151), wirksamer zu gestalten, indem die Aufklärungsfähigkeiten von Bundesnachrichtendienst und Bundesamt für Verfassungsschutz umfassend überarbeitet und gestärkt werden.

Die Stärkung der Fähigkeiten betrifft zeitgemäß speziell auch den Cyberraum, der einerseits Tatraum für komplexe Cyberangriffe - speziell fremder Mächte - ist und deshalb andererseits kein täterseitiger Schutzraum für unbeobachtete Tatvorbereitung sein darf, also einen wesentlichen Raum für die nachrichtendienstliche Aufklärung darstellt. Deshalb schafft das Gesetz dazu angemessene Aufklärungsbefugnisse, speziell zur Auswertung technischer Angriffsspuren in der Angriffsinfrastruktur von Cyberangriffen wie auch allgemein – unter engen Voraussetzungen – zu informationstechnischen Systemen der Bedrohungsakteure.

Zur Erfüllung staatlicher Schutzpflichten bzw. zur Vermeidung von Schutzlücken erhalten Bundesamt für Verfassungsschutz und Bundesnachrichtendienst künftig begrenzte Interventionsbefugnisse. Dabei sind die Befugnisse mit der jeweiligen nachrichtendienstlichen Aufklärung verbunden und – aufgabenadäquat – unterschiedlich ausgestaltet. Mit Blick auf das Bundesamt für Verfassungsschutz bleiben die Befugnisse im nachrichtendienstlichen

Operationsmodus verdeckter Einwirkung – ohne Zwangsausübung gegenüber Personen. Der Bundesnachrichtendienst, dessen Tätigkeit im Ausland anderen Kautelen folgt und der jenseits der Zuständigkeit inländischer Gefahrenabwehrbehörden agiert, erhält eine Reihe von Befugnissen, die es ihm ermöglichen, unmittelbar auf bevorstehende Gefahren, die er im Rahmen seiner aufklärenden Tätigkeit ausmacht, reagieren zu können. Flankiert wird dies durch die Möglichkeit, im Rahmen einer spezifischen Gefährdungslage durch fremde Mächte auch (proaktiv) einwirkend tätig zu werden, um Bedrohungen durch erweiterte nachrichtendienstliche Maßnahmen abzuwenden oder einzuschränken.

Wie bereits im MAD-Gesetz erfolgt, werden nun auch im BND-Gesetz die bisherigen zum Teil wenig klaren Verweisungen auf das Bundesverfassungsschutzgesetz durch eigene, aufgabenspezifische Regelungen ersetzt. Die umfassenden Änderungen bedingen die Neuverkündung von Bundesverfassungsschutzgesetz und BND-Gesetz, die auch Fortentwicklungen der Datenweiterverarbeitungsregelungen enthalten (einschließlich neuer Vorschriften für den Abruf von Auswertungsprodukten, die automatisiert erstellt wurden) und ein modernes, schlankes, insgesamt praxistaugliches und damit zugleich zukunftssicheres Datenschutzfachrecht schaffen.

Die Regelungen des bisherigen Artikel 10-Gesetzes werden in die Fachgesetze integriert. Die Aufspaltung ist ein historisches Relikt, das die Systematisierung und Übersichtlichkeit der Rechtsmaterie hemmt. Dies gilt auch für die Neuregelung der strategischen Aufklärung (vormals: strategische Fernmeldeaufklärung) im BND-Gesetz, welche nunmehr ein einheitliches System für die – nach wie vor unterschiedliche – Behandlung von Ausland-Ausland- und Ausland-Inland-Kommunikation vorsieht. Hierdurch erfolgt zugleich eine Umsetzung der verfassungsgerichtlichen Rechtsprechung (BVerfG, Beschluss vom 8. Oktober 2024 – 1 BvR 1743/16 u.a.).

Neu hinzu tritt das Gesetz über die Rechtskontrolle durch den Unabhängigen Kontrollrat. Hiermit wird die unabhängige Kontrolle der operativen Nachrichtendienstaufgaben institutionell zusammengeführt, indem der UKRat nicht nur die bisherigen und neuen – justizähnlichen - Vorabkontrollen von Anordnungen übernimmt (teils bisher bei der G 10-Kommission), sondern zugleich auch die – administrative – Datenschutzkontrolle von der Bundesbeauftragten für Datenschutz und Informationssicherheit. Der hierin enthaltene integrale Ansatz sorgt für eine wirksame Kontrolle aus einer Hand und stärkt zugleich durch Informations- und Berichtspflichten an das parlamentarische Kontrollgremium auch die parlamentarische Kontrolle.

III. Exekutiver Fußabdruck

Es haben keine Interessenvertreterinnen und Interessenvertreter sowie beauftragte Dritte wesentlich zum Inhalt des Entwurfs beigetragen. (Anmerkung: wird vor Verfahrensabschluss überprüft, ggf. aktualisiert)

IV. Alternativen

Zur Umsetzung der bezeichneten Ziele besteht keine alternative Möglichkeit.

V. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes ergibt sich wie folgt:

- Neuverkündung des Bundesverfassungsschutzgesetzes unter Aufhebung des Artikel 10-Gesetzes und die Änderung der Abgabenordnung: Artikel 73 Absatz 1 Nummer 10 Buchstabe b und c GG sowie für die nicht Bund-Länder-Zusammenarbeit bezogenen Aufgaben des Bundesamtes für Verfassungsschutz die Natur der

Sache, wobei ergänzend die Auskunfts- und Mitwirkungspflichten von Unternehmen auf Artikel 73 Absatz 1 Nummer 6 und 7 und Artikel 74 Absatz 1 Nummer 11 GG zu stützen sind. Eine bundeseinheitliche Regelung zu den Unternehmenspflichten ist – wie im geltenden Bundesverfassungsschutzgesetz – notwendig, da die Aufklärung bundesweiter Bedrohungen über das gesamte Bundesgebiet einheitliche Ermittlungsbefugnisse erfordert, einschließlich der komplementären Mitwirkungspflichten von Unternehmen, mit denen die Befugnisse erst wirksam werden.

- Neuverkündung des BND-Gesetzes: Artikel 73 Absatz 1 Nummer 1 GG sowie Natur der Sache (ergänzend wird auf die obigen Ausführungen hinsichtlich der Auskunfts- und Mitwirkungspflichten verwiesen),

- Gesetz über die Einrichtung des Unabhängigen Kontrollrats: Artikel 73 Absatz 1 Nummer 1, Nummer 10 Buchstabe b und c GG und die Natur der Sache,

- Änderung des Gesetzes über die Kontrolle von Kriegswaffen: Artikel 26 Absatz 2 Satz 2 GG,

- Änderung des Informationsfreiheitsgesetzes: Annex-Kompetenz zur Sachkompetenz sowie die Natur der Sache,

- Änderung des Beamtenversorgungsgesetzes: Artikel 73 Absatz 1 Nummer 8 GG,

- Änderung des Bundesbesoldungsgesetzes: Artikel 73 Absatz 1 Nummer 8 GG,

- Änderung des Bundespersonalvertretungsgesetzes: Artikel 73 Absatz 1 Nummer 8 GG,

- Änderung des Umweltinformationsgesetzes: Annex-Kompetenz zur Sachkompetenz sowie die Natur der Sache,

- Änderung des Vereinsgesetzes: Artikel 74 Absatz 1 Nummer 3 GG,

- Änderung des BKAG-Gesetzes: Folgeänderung zu Artikel 1,

- Änderung des Hochschulstatistikgesetzes: Artikel 73 Absatz 1 Nummer 11 GG,

- Änderung des Aufenthaltsgesetzes: Artikel 73 Absatz 1 Nummer 3 GG,

- Änderung der Verwaltungsgerichtsordnung: Artikel 74 Absatz 1 Nummer 1 GG (gerichtliches Verfahren),

- Änderung der Abgabenordnung: Artikel 108 Absatz 5 Satz 1 GG,

- Änderung des Zollverwaltungsgesetzes: Artikel 73 Absatz 1 Nummer 5 GG,

- Änderung des Zehnten Buchs Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz: Artikel 74 Absatz 1 Nummer 7 GG in Verbindung mit Artikel 72 Absatz 2 GG, wobei die bundeseinheitliche Regelung wie bereits in der geänderten Vorschrift erforderlich ist, weil die Aufklärung überregionaler Bedrohungen einheitliche Ermittlungsbefugnisse erfordert,

- Änderung des Geldwäschegesetzes: Artikel 73 Absatz 1 Nummer 10 Buchstabe a sowie Artikel 74 Absatz 1 Nummer 11 in Verbindung mit Artikel 72 Absatz 2 GG, wobei die bundeseinheitliche Regelung wie bereits in der geänderten Vorschrift erforderlich ist, weil die Aufklärung überregionaler Bedrohungen einheitliche Ermittlungsbefugnisse erfordert.

VI. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf hat keine Bezüge zum Recht der Europäischen Union, da er Regelungen auf dem Gebiet der nationalen Sicherheit trifft, die in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt (Artikel 4 Absatz 2 EUV; BVerfG, Beschluss vom 8. Oktober 2024 - 1 BvR 1743/16 / 1 BvR 2539/16 – Rn. 77 ff.). Er ist mit völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland geschlossen hat, vereinbar.

VII. Gesetzesfolgen

Die Regelungen tragen zur besseren Gefahrerforschung und Aufklärung von Gefahren des Extremismus und Terrorismus sowie der Spionage und Proliferation in Deutschland bei und bewirken dabei einen abgewogenen Ausgleich zwischen den damit verfolgten Gemeinwohlbelangen und den Interessen einzelner durch Datenverarbeitung in ihren Persönlichkeits- und Privatheitsrechten betroffenen Personen.

1. Rechts- und Verwaltungsvereinfachung

Die Konsolidierung der Rechtsmaterie durch Systematisierung, auch unter Eingliederung der bisher separat im Artikel 10-Gesetz getroffenen Regelungen trägt zur Harmonisierung der Verfahren und zur Verwaltungsvereinfachung bei, ebenso die Bündelung unabhängiger Kontrolle im Unabhängigen Kontrollrat.

2. Nachhaltigkeitsaspekte

Der Gesetzentwurf hat Bezüge zu Ziel 16 – „friedliche Gesellschaften“ – der Nachhaltigkeitsstrategie, insbesondere mit dem Unterziel 16.1 der Verringerung aller Formen der Gewalt und der Erhöhung persönlicher Sicherheit. Die Bezüge sind allerdings in mehrfacher Hinsicht mittelbar. Schutzgut des Verfassungsschutzes sind nicht Individualrechtsgüter, sondern die Universalrechtsgüter nach Artikel 73 Absatz 1 Nummer 10 Buchstabe b GG. Diese bilden aber den strukturellen Rahmen, in dem sich individuelle Sicherheit realisiert. Die Wirkungen sind auch insofern mittelbar, als der Verfassungsschutz eine Frühwarnfunktion hat, so dass sich diese Aufgabenwahrnehmung unter Umständen erst in vielstufigen Wirkungsketten in konkreten Sicherheitseffekten abbildet. Eine Operationalisierung statistischer Messbarkeit der Wirkungen des Gesetzes in Bezug auf den Nachhaltigkeits-Indikator ist danach nicht möglich. Mithin sind auch entsprechende prognostische Einschätzungen gegenständlich nicht eröffnet. Gleichwohl ist generell davon auszugehen, dass die effektive Aufgabenwahrnehmung des Verfassungsschutzes sich auch im Indikator 16.1 positiv niederschlägt.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Beim Bundesnachrichtendienst entstehen durch den Gesetzentwurf zusätzliche Haushaltsausgaben ohne Erfüllungsausgaben, die nicht abschließend bezifferbar sind. Geschätzt werden jährliche zusätzliche Ausgaben in Höhe von insgesamt mindestens 20 Mio. Euro für behördliche Aufwände. Die laufenden Haushaltsaugaben sind abhängig von der Entwicklung der weltweiten Krisen- und Bedrohungslagen und können höher ausfallen. Zusätzlich entstehen, in Zusammenhang mit der Anpassung von IT-Strukturen und Bereitstellung von Ausrüstungsgegenständen, einmalige Mehrausgaben in Höhe von mindestens 40 Mio.

Euro und – nach erfolgter Anpassung der IT-Strukturen – jährliche Ausgaben in Höhe von mind. etwa 15 Mio. Euro.

Der Mehrbedarf wird Gegenstand des Weiteren Haushaltsaufstellungsverfahrens zum geheimen Wirtschaftsplan des Bundesnachrichtendienstes und entsprechend zum Zuschusstitel an den Bundesnachrichtendienst (Kapitel 0414) für die Jahre 2027ff sein.

Beim Bundesamt für Verfassungsschutz entstehen durch den Gesetzentwurf zusätzliche Haushaltsausgaben ohne Erfüllungsausgaben, die nicht abschließend bezifferbar sind. Geschätzt werden jährliche zusätzliche Ausgaben in Höhe von insgesamt rd. 2 Mio. € für behördliche Aufwände. Die laufenden Haushaltsaugaben sind abhängig von der Entwicklung der inländischen Krisen- und Bedrohungslage und können höher ausfallen.

Der finanzielle Mehrbedarf des Bundesamts für Verfassungsschutz wird aus den vorhandenen Ansätzen des Bundesamts für Verfassungsschutz (Kapitel 0626) getragen.Haushaltsausgaben ohne Erfüllungsaufwand entstehen für den Unabhängigen Kontrollrat (Einzelplan 22) in Folge der personellen Aufwände für die notwendigen Verwaltungstätigkeiten einer obersten Bundesbehörde. Die Aufwände werden auf jährlich 2.100 Personentage (das entspricht zehn Planstellen/Stellen, davon sieben im höheren Dienst, zwei im gehobenen Dienst und einer im mittleren Dienst) geschätzt. Die zugehörigen Personal-, Sacheinzel- und Gemeinkosten (darunter Mieten, Reisekosten usw.) und Versorgung belaufen sich auf etwa 2,21 Mio. Euro pro Jahr.

Hinzu kommen schätzungsweise einmalige Ausgaben aus dem Erfüllungsaufwand (unten 3.c) in Höhe von 1,6 Mio. Euro sowie jährliche Ausgaben in Höhe von 0,8 Mio. Euro für die spezifische Infrastruktur (insbesondere VS-konforme Arbeitsplätze und Kommunikationssysteme), die nicht in den pauschalierten Einzel- und Gemeinkosten enthalten sind. Die jährlichen Ausgaben aus dem Erfüllungsaufwand (unten 3.c) für Tätigkeiten der gerichtsähnlichen und der administrativen Rechtskontrolle (27 Planstellen/Stellen, davon 17 im höheren Dienst, sieben im gehobenen Dienst und drei im mittleren Dienst) werden auf etwa 5,85Mio. Euro geschätzt (Personal-, Sacheinzel- und Gemeinkosten sowie Versorgung).

Insgesamt ergeben sich damit schätzungsweise für den Unabhängigen Kontrollrat Haushaltsausgaben von einmalig 1,6 Mio. Euro und jährlich 8,86 Mio. Euro. Die jährlichen Ausgaben beinhalten die Personalkosten in Höhe von 3,30 Mio. Euro für die insgesamt 37 Planstellen/Stellen zuzüglich der Sacheinzelkosten in Höhe von 1,39 Mio. Euro sowie der Gemeinkosten in Höhe von etwa 1,74 Mio. Euro und Versorgung in Höhe von 1,62 Mio. Euro sowie die jährlich anfallenden spezifischen IT-Infrastrukturkosten in Höhe von 0,8 Mio. Euro.

Einsparungen ergeben sich demgegenüber durch den Wegfall der Zuständigkeiten der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und der G10-Kommission. Dies beinhaltet sowohl Personalkosten der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (Einzelplan 21), die künftig aufgrund der künftig vorgesehenen datenschutzrechtlichen Kontrolle für die Auftragsdatenverarbeitung durch den Unabhängigen Kontrollrat nicht mehr anfallen. Außerdem betrifft dies die Aufwandsentschädigungen für Mitglieder der G10-Kommission sowie die unterstützende Tätigkeit der Geschäftsstelle der G10-Kommission (Einzelplan 02, Kapitel 0216). Diese sind im Rahmen der Haushaltsaufstellung zu prüfen.

4. Erfüllungsaufwand

[Welche finanziellen und zeitlichen Be- oder Entlastungen sind durch die geplanten Regelungen für die Bürgerinnen und Bürger, die Wirtschaft und die Verwaltung zu erwarten? Hier

sind mindestens die Angaben aus dem Vorblatt zu Buchstabe E zu übernehmen und ggf. zu erläutern. Tabellarische Darstellungen können hier die Übersichtlichkeit verbessern.]

Mit der Umsetzung des Gesetzes entstehen personelle und finanzielle Aufwände beim Bundesnachrichtendienst, um insbesondere den erweiterten Befugnissen im Rahmen der Informationsbeschaffung und der Informationsauswertung Rechnung zu tragen. Für Bürgerinnen und Bürger entsteht kein zusätzlicher Erfüllungsaufwand. Für die Wirtschaft entstehen zusätzliche Aufwände durch das Bedienen von Ersuchen des Bundesnachrichtendienstes in Höhe von etwa 50 T Euro pro Jahr. Die Aufwände werden erstattet. Für die Anpassung der IT-Strukturen entstehen im Bundesnachrichtendienst einmalige Erfüllungsaufwände im Umfang von mindestens 40 Mio. Euro. Nach erfolgter Anpassung der IT-Strukturen entstehen zugehörige behördliche Aufwände im Umfang von jährlich mindestens 15 Mio. Euro. Zudem besteht bereits ab Inkrafttreten des Gesetzes ein jährlicher Erfüllungsaufwand von mindestens 20 Mio. Euro, insbesondere zur Umsetzung der neuen Befugnisse im Bereich der Eigensicherung. Der laufende Erfüllungsaufwand ist abhängig von der Entwicklung der weltweiten Krisen- und Bedrohungslagen und kann höher ausfallen.

Mit der Umsetzung des Gesetzes entstehen personelle und finanzielle Aufwände beim Bundesamt für Verfassungsschutz, um insbesondere den erweiterten Befugnissen Rechnung zu tragen. Für Bürgerinnen und Bürger und die Wirtschaft entsteht kein zusätzlicher Erfüllungsaufwand. Für die Anpassung der IT-Strukturen entstehen beim Bundesamt für Verfassungsschutz einmalige Erfüllungsaufwände im Umfang von etwa 94 Mio. €. Nach erfolgter Anpassung der IT-Strukturen entstehen zugehörige betriebliche Aufwände im Umfang von jährlich etwa 269 Mio. €. Zudem besteht bereits ab Inkrafttreten des Gesetzes ein einmaliger Erfüllungsaufwand von rd. 51 Mio. €, insbesondere zur Umsetzung der neuen Befugnisse im Bereich der Eigensicherung. Ferner entstehen dem Bundesamt für Verfassungsschutz zusätzliche Erfüllungsaufwände in Höhe von rd. 25 Mio. € jährlichen Personalkosten sowie rd. 8 Mio. € jährlichen Sacheinzelkosten. Der jährliche Erfüllungsaufwand ist abhängig von der Entwicklung der inländischen Krisen- und Bedrohungslage und kann höher ausfallen.

Mit der Umsetzung des Gesetzes entstehen personelle und finanzielle Aufwände bei dem Unabhängigen Kontrollrat aufgrund der Erweiterung der Kontrollzuständigkeiten. Der notwendige Aufwuchs betrifft dabei sowohl die Rechtskontrolle durch das gerichtsähnliche Kontrollorgan einschließlich der damit in Verbindung stehenden prüf- wie organisationsrelevanten Unterstützungselemente als auch die Erweiterung der durch das gerichtsähnliche Kontrollorgan gelenkten Strukturkontrolle auf alle Nachrichtendienste des Bundes.

Der jährliche Erfüllungsaufwand für den Unabhängigen Kontrollrat, d. h. die Aufwände zur Durchführung der gerichtsähnlichen Rechtskontrolle und der administrativen Rechtskontrolle wird auf etwa 5.670 Personentage geschätzt. Dies entspricht 27 Personen pro Jahr. Mit diesen Aufwänden einher gehen jährliche finanzielle Aufwände im Umfang von etwa 5,85 Mio. Euro für Personal- und Sacheinzelkosten sowie Gemeinkosten und Versorgung. Hinzu kommen einmalige Aufwände von geschätzt 1,6 Mio. Euro zur Bereitstellung der für die Aufgabenerfüllung benötigten gesicherten Infrastruktur, darunter insbesondere Verschlüsselungskomponenten und VS-konforme Arbeitsplätze, sowie für die Kontrolltätigkeiten relevante Soft- und Hardware sowie jährliche Aufwände in Höhe von 0,8 Mio. Euro.

5. Erfüllungsaufwand im Landesvollzug.

Das Gesetz induziert keinen Landesvollzug mit Erfüllungsaufwand.

6. Weitere Kosten

Indirekten Kosten für die Wirtschaft, insbesondere für mittelständische Unternehmen, entstehen nicht. Auswirkungen auf die Einzelpreise und das Preisniveau sind nicht zu erwarten.

7. Weitere Gesetzesfolgen

Auswirkungen von gleichstellungspolitischer Bedeutung sind ebenso wenig ersichtlich wie verbraucherpolitische oder demografische Auswirkungen.

VIII. Befristung; Evaluierung

Da die effektive Wahrnehmung von Daueraufgaben geregelt wird, ist eine Befristung nicht sachgerecht. Gesetzesbegleitend erfolgt eine laufende Evaluierung zur Praxisbewährung der Regelungen sowohl unter Gesichtspunkten der Wirksamkeit wie der Wirtschaftlichkeit, speziell auch zu den der Vorabkontrolle des Unabhängigen Kontrollrates unterliegenden Intensiveingriffen (gestützt auch auf das periodische Berichtswesen nach dem UKRat-Gesetz).

B. Besonderer Teil

Zu Artikel 1 (Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz)

Systematisierendes Grundgerüst der Neuverkündung ist die Umsetzung der Verfassungsrechtsprechung (grundlegend BVerfGE 162, 1). Kernpunkte sind neue Regelungen zur Informationsbeschaffung und –übermittlung, verbunden mit einer verbreiterten unabhängigen Kontrolle (die zudem mit dem UKRat-Gesetz neu aufgestellt wird).

Die Informationsbeschaffung wird dadurch systematisiert, dass einerseits Maßnahmen abhängig vom Eingriffsgewicht in erheblich bzw. besonders erheblich eingreifend klassifiziert werden (§§ 16 ff.) und andererseits eine komplementäre Klassifizierung des Gefährdungspotenzials von Beobachtungsobjekten in erheblich bzw. besonders erheblich beobachtungsbedürftig (§ 3 Absatz 7 und 8) erfolgt. Das ermöglicht klare Verhältnismäßigkeitsverknüpfungen: Erhebliche Eingriffe nur bei erheblicher Beobachtungsbedürftigkeit.

Einen Schwerpunkt der fachlichen Verbesserungen bildet die wirksame Aufklärung auch im Cyberraum. Insgesamt sind Praxiserfahrungen für die fachlichen Fortentwicklungen leitend. Die Verarbeitung von Minderjährigendaten wird angesichts nicht selten auch sehr junger Akteure (aktuelles Beispiel: „Attentäterfanszene“, siehe Verfassungsschutzbericht) neu geordnet, was ebenso die Früherkennung verbessert, wenn sehr junge Menschen von terroristischen Organisationen gezielt zu Anschlägen instrumentalisiert werden.

Eine konzeptionelle Neuerung liegt darin, die Schutzaufgabe zur Schließung von Schutzlücken operativ auch dadurch zu stärken, dass das BfV Befugnisse erhält, bei besonderen Bedrohungen auch auf Tatmittel und die Informationsbasis des Angreifers „geheimdienstlich“ einzuwirken, um sein Aktionspotenzial zu hemmen.

Die umfassende Reform bezieht auch ein, dass vorab bereits Elemente hierfür in der Neuverkündung des MAD-Gesetzes (mit Artikel 1 des Gesetzes zur Stärkung der Militärischen Sicherheit in der Bundeswehr vom 9.1.2026, BGBl I Nr. 7, Seite 2) umgesetzt wurden. Ferner gehen Entwicklungen ein, die das Landesrecht bereits im Anschluss an Empfehlungen der Innenministerkonferenz (207. Sitzung am 8.12.2017, TOP 29) genommen hat,

beispielsweise mit der Nutzung von im öffentlichen Raum ohnehin vorhandener Videoüberwachung, wenn dies im Einzelfall veranlasst ist.

Der Schutz des Kernbereichs der Privatheit sowie von besonderen Berufsgeheimnissen wird erweitert gesetzlich geregelt und bei der gesamten Informationsbeschaffung gewährleistet. Vor tiefgehenden Eingriffen, bei denen mit der Gewinnung höchstprivater Informationen zu rechnen ist, muss die Anordnung durch den Unabhängigen Kontrollrat geprüft werden, der bindend über die Rechtmäßigkeit entscheidet.

Die bereits in 2023 an die Verfassungsrechtsprechung angepassten Übermittlungsbefugnisse werden angesichts jüngerer Verfassungsrechtsprechung nochmals nachjustiert, wobei zugleich weitere Unstimmigkeiten bereinigt werden.

Neu ist die gesetzliche Regelung zum Verfahren der Feststellung, dass bestimmte Bestrebungen Beobachtungsobjekt des Verfassungsschutzes sind (allein durch Präsidentin/Präsidenten des BfV) und zeitlich begrenzende Vorgaben zu Verdachtsfällen (§ 4 Absatz 2 und 3). Ebenso erstmalig geregelt sind vorgelagerte Prüffälle, in denen noch keine systematische Beobachtung erfolgt, zu deren Prüfung auch keine nachrichtendienstlichen Mittel eingesetzt werden können und die zeitlich noch enger begrenzt werden. Wesentliche rechtsstaatliche Planken werden damit nunmehr auch gesetzlich festgelegt. Verwaltungsstreitsachen werden gerade zu Fällen der Öffentlichkeitsinformation durch Eingangszuständigkeit des Bundesverwaltungsgerichts beschleunigt, was den rechtskräftigen Abschluss nicht mehr in einem mehrstufigen Instanzenzug verzögert. Dies dient der Beschleunigung sowohl wirksamen Rechtsschutzes wie auch der Befriedung durch abschließende gerichtliche Klärung.

Eine weitere rechtsstaatliche Sicherung schafft die neue, allgemeine Regelung zur Maßnahmerichtung personengezielter nachrichtendienstlicher Mittel, die eingrenzt, gegen wen solcher Einsatz zulässig ist (§ 16 Absatz 5).

Die Gliederung des Gesetzes folgt den Prozessen, in denen die Fachaufgabe wahrgenommen wird, also von der Beschaffung über die Auswertung bis zur Weitergabe der nachrichtendienstlichen Erkenntnisprodukte an deren Bedarfsträger. Bereits in der Aufgabennorm wird verdeutlicht, dass gerade in dieser Informationsweitergabe die Finalität der Aufgabe liegt (§ 2 Absatz 2 Satz 1 Nummer 2).

Zu Abschnitt 1 (Aufgaben und Zusammenarbeit der Verfassungsschutzbehörden)

Der Abschnitt greift im Wesentlichen das geltende Recht auf und entwickelt es lediglich behutsam, vornehmlich im Interesse verbesserter Normenklarheit fort.

Zu § 1 (Zusammenarbeitspflicht)

Der Paragraph führt die bisherigen §§ 1, 2 in einer Norm zusammen, da organisatorische – föderale – Gliederung (bisheriger § 2) und Zusammenarbeitspflicht (bisheriger § 1 Abs. 2 und 3) im Sachzusammenhang stehen und dabei zugleich damit korrespondieren, dass der Verwaltungszweig gesamtstaatliche Zwecke im Kern staatlicher Selbstbehauptung verfolgt. Mit der bundesgesetzlichen Vorgabe zur Behördeneinrichtung und besonderen Zusammenarbeit wird ein besonderer Zweckverbund gesamtstaatlicher Kernaufgaben etabliert. Dieser Verbundcharakter bildet sich speziell auch in der Zentralstellenfunktion des BfV (§ 5) und dem umfassenden Informationsverbund (§ 6) ab.

Zu Absatz 1

Die Regelung übernimmt den bisherigen § 1 Absätze 2 und 3.

Der Bezug des bisherigen § 1 Absatz 2 auf „Angelegenheiten des Verfassungsschutzes“ wird dabei durch Integration der Zweckbestimmung des bisherigen § 1 Absatz 1 inhaltlich

ausgefüllt. Isolierte Zwecknormen entsprechen nicht mehr aktuellen Rechtsförmlichkeitsanforderungen. Mit der Integration in den neuen § 1 Absatz 1 bleibt dennoch die Benennung der Rechtsgüter des Verfassungsschutzes erhalten. Sie sind besonders hochrangig und von hohem verfassungsrechtlichem Gewicht (BVerfGE 162, 1 - Rn. 150, 174).

Zu Absatz 2

Die Regelung entspricht dem bisherigen § 2 Absatz 1. Neben dem BfV nimmt auch der MAD Verfassungsschutzaufgaben auf Bundesebene nach § 2 Absatz 1 MADG wahr.

Zu Absatz 3

Die Regelung entspricht dem bisherigen § 2 Absatz 2.

Zu § 2 (Aufgaben der Verfassungsschutzbehörden)

Die Aufgabenregelung des bisherigen § 3 wird neu systematisiert und um Klarstellungen ergänzt.

Zu Absatz 1

Die Regelung greift die Aufgabenbereiche des bisherigen § 3 Absatz 1 auf und ergänzt Klarstellungen mit Nummer 2 Buchstabe c.

Nummer 1 entspricht dem geltenden Recht. Der Fall „ungesetzliche Beeinträchtigung der Amtsführung“ besitzt nur einen engen Anwendungsbereich. Gemeint ist allein die unmittelbare Einwirkung, etwa durch Nötigungshandlungen oder Bestechung, nicht hingegen tätigkeitserschwerende Umstände oder Fernwirkungen wie im Falle des § 188 StGB. Erst recht ist Regierungskritik keine ungesetzliche Beeinträchtigung.

Die neue Regelung in Nummer 2 Buchstabe c trägt der Integrationsöffnung und internationalen Kooperationsoffenheit des Grundgesetzes Rechnung. Wenn deutsche Hoheitsrechte auf die Europäische Union übertragen werden, verliert deren Ausübung nicht die Schutzbedürftigkeit gegenüber den vom Verfassungsschutz aufzuklärenden Bedrohungen. Gleiches gilt, wenn staatliche Aufgaben nicht in nationalen Einrichtungen, sondern in internationaler Organisation wahrgenommen werden, so dass dann die Funktionsfähigkeit der internationalen Organisation gleichermaßen Schutzobjekt sein kann. Hervorgehoben wird dabei neben der EU auch die NATO, in der Deutschland ebenso an einer kollektiven Organisation zentraler Aufgaben staatlicher Sicherheit teilnimmt. Soweit gleichwertiger Schutz nicht anderweitig gewährleistet ist, kann der nationale Verfassungsschutz die Aufklärungsaufgabe auch insoweit wahrnehmen. Der Begriff Bedrohungen bezeichnet sowohl Bestrebungen, die von Individuen - u.U. kollektiv in einem Personenzusammenschluss - betrieben werden als auch Tätigkeiten fremder Mächte. Gegenstand kann etwa die ungesetzliche Beeinträchtigung der Amtsführung durch Bestechung oder Nötigung sein oder auch eine Funktionsgefährdung durch Cyberangriffe, seien sie auf Ausforschung geheim zu haltender Informationen, seien sie auf Störung der IT angelegt. Die Aufgabe setzt einen territorialen Deutschlandbezug voraus, der beispielsweise im Wohnsitz eines Beteiligten bestehen kann oder auch einem Serverstandort in der IT-Struktur eines Cyberangriffs.

Nummer 3 enthält ergänzende Erläuterungen der bisher bereits in § 3 Absatz 1 Nummer 2 verwendeten Begriffe der sicherheitsgefährdenden und geheimdienstlichen Tätigkeiten. Beispiel einer Tätigkeit nach Buchstabe a können Akte transnationaler Repression sein, durch die ein auswärtiger Staat von ihm als Gegner eingestufte Personen in Deutschland verfolgt, unterdrückt oder einschüchtert. Hier kann vom Zweck des Vorgehens veranlasst sein, dass der Staat dem Opfer gegenüber gerade nicht verdeckt (Buchstabe b) auftritt. Solches hoheitliche Handeln verletzt regelmäßig die deutsche Gebietshoheit und beeinträchtigt zudem das Vertrauen der Bevölkerung, in Deutschland vor Verfolgung durch fremde Staaten geschützt zu sein, und damit die Sicherheit des Bundes.

Zu Absatz 2

Die bisherige Aufgabenregelung des § 3 Absatz 1 verdeutlicht nicht hinreichend die Finalität der durch Sammlung und Auswertung von Informationen betriebenen Gefahrerforschung. Die Aufklärung ist nicht Selbstzweck, vielmehr setzt der aufgabenleitende Schutzzweck des bisherigen § 1 Abs. 1 operativ die Informationsweitergabe voraus (BVerfGE 154, 152 - Rn. 217). Die Rolle als Abwehrdienst füllt der Nachrichtendienst grundsätzlich in der Funktion des Informationsdienstleisters aus.

Diese organisatorische Trennung von informationeller Erforschung durch den Nachrichtendienst und aktioneller Intervention durch Exekutivbehörden ist international nicht singulär, allerdings kein allgemeiner Standard. Beispielsweise in Österreich (Direktion Staatsschutz und Nachrichtendienst), Schweden (Säkerhetspolisen) oder den USA (Federal Bureau of Investigation) erfolgt die nachrichtendienstliche Vorfeldaufklärung - auch im Staatschutz - durch die Kriminalpolizei (Mischbehörden). Die Trennung hat indes den Vorteil, dass Informationen aus einer naturgemäß bei der Informationsgewinnung erheblich streuenden Lageaufklärung nicht als Rohinformation für die Ausübung von Zwangsgewalt verfügbar sind, sondern erst nach einem behördlich gesonderten Auswertungsprozess, der Informationen nach Relevanz filtert, validiert und verdichtet, hierdurch Privatsphäre von Informationen mit Sozialbezug abschichtet und Verantwortlichkeiten herausarbeitet, die Grundlage zielgerichteter Folgemaßnahmen sind. Das Trennungsprinzip ist danach eine organisatorische Sicherung der Erkenntnisqualität, die Risiken der informationellen Fehlsteuerung von Zwangsgewalt reduziert und hierdurch überhaupt die Grundlage schafft, verhältnismäßigkeitswahrend bereits Frühaufklärung durchzuführen (BVerfGE 162, 1 - Ls. 1). Andererseits darf solche Prozessgliederung der Abwehr nicht zu rechtsstaatlich intolerablen Schutzlücken führen. Die informationellen Abwehrbefugnisse der Erkenntnisweitergabe werden deshalb in § 60 punktuell für besondere Bedrohungen durch eng umgrenzte aktionelle Befugnisse nachrichtendienstlichen Gepräges ergänzt, wenn bei der Gefahraufklärung solche Handlungsbedarfe bekannt werden und situativ unmittelbares Einschreiten durch BfV zum wirksamen Rechtsgüterschutz erfordert. Damit wird die nachrichtendienstliche Grundaufgabe nicht erweitert, sondern lediglich situativ eintretenden Handlungsbedarfen Rechnung getragen, ähnlich der Nothilfesituation bei Gelegenheit der Eigensicherung nach § 28 Absatz 1 Satz 1.

Satz 1 verdeutlicht, dass die Informationsweitergabe (Nummer 1) die Finalität der Erkenntnisgewinnung (Nummer 2) und damit ebenso originäre Verfassungsschutzaufgabe ist, wie die Aufklärung.

Satz 2 nimmt die bereits gegenwärtig ausgeführte Aufgabe der Aussteigerprogramme ausdrücklich in das Gesetz auf. Die Verfassungsschutzbehörden besitzen hier bereits ein Entschließungsermessen zur Aufgabenwahrnehmung.

Der bisherige § 3 Absatz 3 BVerfSchG ist dem neuen § 2 Absatz 2 als Satz 3 angefügt. Der Satz trifft keine konstitutive Regelung (das Grundgesetz gilt ohne einfachgesetzlichen Anwendungsbefehl), sondern hat Signalcharakter, der spezifisch auf die operative nachrichtendienstliche Aufgabe zielt und deshalb systematisch unmittelbar in diesem Zusammenhang herausgehoben wird.

Zu Nummer 1

Das BfV ist ein Abwehrdienst, dessen informationelle Gefahrerforschung originär auf operative Anschlussmaßnahmen zur Abwehr der Bedrohung ausgerichtet ist. Diese Finalität besitzt Steuerungsgehalt bereits für die Ausrichtung der nachrichtendienstlichen Informationsgewinnung und -auswertung, die auf operativ nutzbare Erkenntnisse zielt und dazu die Perspektive operativer Möglichkeiten und Bedarfe einbezieht. Verfassungsschutz verfolgt einen ganzheitlichen Schutzansatz sowohl universeller, situativer und indizierter Prävention und dies gleichermaßen auf strategischer wie operativer Ebene und dabei gleichermaßen

auf gefahrenabwehrende wie strafverfolgende Anschlussmaßnahmen gerichtet. Sämtliche Akteure mit Aufgaben in diesem umfassenden Bedarfsträgerspektrum sind danach Informationsadressaten. Dies schließt auch die Öffentlichkeit zur Sensibilisierung und für eine geistig-politische Auseinandersetzung etwa mit Extremismus ein. Die Information kann auch eine Schutzberatung einschließen, wie sie das BfV beispielsweise beim präventiven Wirtschafts- und Wissenschaftsschutz intensiv wahrnimmt.

Soweit die Information mit der Übermittlung personenbezogener Daten Eingriffsgehalt hat, ist dazu eine Befugnis erforderlich, die im Abschnitt 3 geregelt ist.

Zu Nummer 2

Der Aufklärungsgegenstand der Bestrebungen und Tätigkeiten nach Absatz 1 bezieht phänomenologisch allgemeine Gefahren ein, die angesichts der Bedrohung herausragender Rechtsgüter (§ 1 Absatz 1; BVerfGE 155, 119 - Rn. 151) bereits mit niedriger Risikoschwelle relevant sind. Dem trägt der nachrichtendienstliche Auftrag der Frühaufklärung Rechnung, Dieser Ansatz der Frühaufklärung kommt in Absatz 1 Satz 1 Nummer 1 mit dem Begriff „frühzeitig“ zum Ausdruck. Nachrichtendienstliche Frühaufklärung ist Ausdruck der Grundentscheidung des Grundgesetzes für eine wehrhafte Demokratie und des Selbstbehauptungswillens des Rechtsstaates (BVerfGE 143, 101 - Rn. 126; 146, 1 - Rn. 110). Die Frühaufklärung bezeichnet den Einsatzpunkt der Aufgabe, beschränkt die Aufklärung aber nicht etwa auf eine Frühphase der Gefahrerforschung. Die Aufgabe findet ihre Grenze erst mit dem Übergang zum Einsatz aktioneller/exekutiver Befugnisse zur Unterbrechung des gefährdenden Ablaufs. Dies ist Sache der Polizei- und Ordnungsbehörden. Zusammenarbeit und Übergabe bei der Gefahrerforschung sind situativ vom Einzelfall abhängig und auf Optimierung der Gefahrenabwehr ausgerichtet.

Aufgabe ist in jedem Fall die objektiv zutreffende Sachverhaltsklärung. Es geht – wie auch in exekutiven Amtsermittlungen – nicht darum, einseitig belastende Informationen zu gewinnen, sondern ein sachlich zutreffendes Bild des Bedrohungsgeschehens. Das Qualitätsziel sind wertige Erkenntnisse, die sachgerechte Grundlage für sachlich richtige Anschlussmaßnahmen sein können.

Zu Absatz 3

Satz 1 übernimmt den bisherigen § 4 Abs. 1 Satz 5 in die Aufgabennorm. Die Verfassungsschutzbehörde darf nicht verdachtsunabhängig ins Blaue hinein, quasi erst zur Schöpfung eines Verdachts oder zur Generierung von Daten auf Vorrat Informationen systematisch sammeln. Allerdings können im Vorfeld systematischer Beobachtung solche Anhaltspunkte zur Prüfung einer Aufgabe vor allem aufgrund offener Erkenntnisquellen gewonnen werden (BVerfGE 162, 1 – Rn. 188 f.).

Die Regelung verdeutlicht zugleich, dass die Aufklärung bei tatsächlichen Anhaltspunkten verpflichtende Aufgabe ohne Entschließungsermessen ist. In den Fällen des Satzes 2 liegt es hingegen im Ermessen der Verfassungsschutzbehörde, ob sie tätig wird. In anderen Fällen verbleibt dem BfV die Möglichkeit durch priorisierende Ressourcensteuerung zugleich Anforderungen wirtschaftlicher Verwaltung Rechnung zu tragen. So kommt auch bei Personenzusammenschlüssen, bei denen keine Anhaltspunkte für erhebliches Gefährdungspotenzialität besteht, in Betracht, die Beobachtungsaufwände sachgerecht auf niedrigem Niveau begrenzt zu halten. Dabei bleibt im Blick, ob sich die Einschätzung der Gefährdungspotenzialität womöglich fortentwickelt.

Zu Nummer 1

Der Schutz der EU oder einer internationalen Organisation ist u.U. auch gesondert organisiert oder wird anderweitig angemessen wahrgenommen, z.B. von einem anderen Mitgliedstaat. In den Fällen der Nummer 1 verbleibt dem BfV daher im Interesse einer

wirtschaftlichen Aufgabenwahrnehmung das pflichtgemäße Ermessen, nicht nur wie, sondern bereits ob es seinerseits tätig wird.

Zu Nummer 2

Die Regelung behält das bisher in § 4 Abs. 1 Satz 3 verankerte Entschließungsermessen bei der Beobachtung von Einzelpersonen unverändert bei. Wie bisher erfolgt keine komplementäre Regelung zu Tätigkeiten nach Absatz 2 Nummer 2. Mit der Finalität der Unterstützung einer fremden Macht (sei es objektiv aufgrund deren Steuerung, sei es subjektiv nach der Täterplanung, etwa bei Vorbereitungen zum Geheimnisverrat bereits vor Kontaktierung des Abnehmers) besteht generell der Unterstützungszusammenhang zum außerordentlichen Gefährdungspotenzial einer fremden Macht. Dies belässt keinen Raum für ein Entschließungsermessen.

Zu Absatz 4

Der Absatz regelt erstmals die Eigensicherung als Fachaufgabe. Bisher erschloss sich diese Aufgabe im Bundesverfassungsschutzgesetz erst im Zusammenhang besonderer Befugnisregelungen (beim Einsatz nachrichtendienstlicher Mittel: § 9 Absatz 1 Satz 1 Nummer 2; bei der Liegenschaftssicherung: §§ 26b, 26c). Im Kern ist die Aufgabe bereits von Absatz 2 erfasst, da die wesentlichen Angriffe auf die Funktionsfähigkeit des BfV von den dort bezeichneten Bedrohungen ausgehen und die Funktionsfähigkeit des BfV selbst Element der Sicherheit des Bundes ist (vgl. § 3 Absatz 2 Nummer 2). Dies deckt die Angriffsszenarien, vor denen das BfV sich schützen muss, aber noch nicht umfassend ab. Motivierend können dabei auch kommerzielle Interessen sein oder eine nicht politisch bestimmte Aversion gegenüber Nachrichtendiensten, etwa mit verschwörungstheoretischem Hintergrund oder auch infolge einer psychischen Erkrankung.

Unbeschadet dieser fachrechtlichen Differenzierung zwischen politisch motivierten und anders motivierten Störern handelt sich um eine Gefahrenabwehraufgabe für die Rechtsgüter des Verfassungsschutzes und damit materiell Verfassungsschutz. Dies unterscheidet die Aufgabe von Funktionsannexen wie Zentralverwaltungsangelegenheiten, z.B. Personalverwaltung oder Sachmittelbeschaffung und rechtfertigt den Einbezug in den operativen Aufgaben- und Befugniskanon, wie bereits bisher mit § 9 Absatz 1 Satz 1 Nummer 2 der Fall.

Schutzgut der Eigensicherung ist die Funktionsfähigkeit der Behörde bezogen auf die dafür wesentlichen Mittel der Aufgabenwahrnehmung. Der bisher im Bundesverfassungsschutzgesetzt verwendete Begriff „Quellen“ (der eine Beschränkung auf Informationsquellen suggeriert) wird nunmehr durch den passenderen und nun in § 3 Absatz 6 legaldefinierten Begriff „verdeckte Hilfspersonen“ ersetzt, da sämtliche für das BfV verdeckt tätige Personen, also nicht nur Vertrauenspersonen und Informanten, sondern auch Gewährspersonen und Legendengeber umfasst sind, ebensowie Beliehene, wie z. B. Mitarbeitende von Post- und Paketdienstleistern, die das BfV bei der Brief- und Paketüberwachung unterstützen (insofern verdeckt, als die Wahrnehmung der Unterstützungsaufgabe wiederum vertraulich erfolgt). Ebenso umfassend ist der Begriff der „Einrichtungen“ zu verstehen. Er umfasst beispielsweise die gesamte IT-Infrastruktur der Verfassungsschutzbehörden.

Die spezielle Aufgabe betrifft einerseits eine vorsorgende Aufgabenwahrnehmung, also unabhängig davon, ob im Einzelfall bereits Anhaltspunkte für eine Gefährdung vorliegen. Beispiel dafür sind die Kontrollen für den Zugang zu den Liegenschaften, die Jedermann betreffen, nicht allein Personen, zu denen solche Anhaltspunkte vorliegen (Liegenschaftssicherung, § 64). Zudem umfasst die Sicherungsaufgabe den Schutz vor jedweden die Sicherheit gefährdenden Tätigkeiten, also nicht nur solchen, die für eine fremde Macht ausgeführt werden. Zur Vermeidung von Missverständnissen wird dafür deshalb künftig nicht mehr der in § 3 Absatz 1 Nummer 2 mit anderem Inhalt verwendete Begriff der „sicherheitsgefährden“ Tätigkeit verwendet, sondern im Interesse klarerer Regelung der neue Begriff der „funktionsgefährdenden“ Tätigkeit eingeführt.

Zu Absatz 5

Absatz 5 übernimmt den bisherigen § 3 Absatz 2 in einer verschlankten Version. Die bisherigen Nummern 1 und 2 sind besondere Fälle der Nummer 4, an die im Bundesverfassungsschutzgesetz aber keine besonderen Rechtsfolgen geknüpft werden, so dass kein Bedarf für gesonderte Regelung besteht.

Zu Nummer 1

Bereits die allgemeine Aufgabe nach Absatz 1 schließt die Information anderer Stellen, die Verfassungsschutzerkenntnisse benötigen, ein. Dies ist beschränkt auf der Verfassungsschutzbehörde vorliegende Informationen (wobei allenfalls zur Klärung des Ersuchenssachverhalts ergänzende Erhebungen aus offenen Quellen erfolgen können, z.B. Klärung, welche Personen Organfunktionen bei einer juristischen Person besitzen, wenn zu dieser angefragt wird). Die Mitwirkungsaufgabe nach Absatz 5 Nummer 1 geht darüber hinaus, indem auch Sicherheitsermittlungen durchzuführen sein können (vgl. § 12 SÜG). Der wesentliche Unterschied zu den Aufgaben nach Absatz 1, einschließlich der Übermittlung personenbezogener Daten, besteht bei der Mitwirkungsaufgabe darin, dass die mitwirkende Verfassungsschutzbehörde nicht aufgrund tatsächlicher Anhaltspunkte im Einzelfall zur Aufklärung von Bedrohungen tätig wird (Voraussetzung nach Absatz 3 Satz 1), sondern vorbeugend, um zu vermeiden, dass ungeeignete Personen spezielle Tatgelegenheiten oder -mittel zur Schädigung von Verfassungsschutzgütern haben, etwa durch Zugang zu Verschlusssachen oder lebenswichtigen Einrichtungen (z.B. SÜG, § 12b AtG) oder durch Sicherungsaufgaben in solchem Zusammenhang (z.B. § 7 LuftSiG, § 34a GewO) oder legalen Besitz von Waffen oder Sprengstoffen (§ 5 WaffG, § 8a SprengG). In diesen gesetzlich besonders geregelten Risikosachverhalten schließt die Mitwirkungsaufgabe deshalb als Vorsorgemaßnahme ein, dass zu der betroffenen Person, auch wenn aktuell keine verfassungsschutzrelevanten Erkenntnisse zu ihr vorliegen, aus dem Mitwirkungsverfahren Daten bei der Verfassungsschutzbehörde gespeichert bleiben. Dies ist notwendig, um bei künftig anfallenden Erkenntnissen ohne weiteres den besonderen Risikosachverhalt, der die Mitwirkung veranlasst hatte, zu erkennen, damit die Verfassungsschutzbehörde dann von sich aus der zuständigen Stelle nachberichten kann. Die Anzahl solcher Vorsorgespeicherungen wird gemäß § 33 in den jährlichen Verfassungsschutzberichten mitgeteilt (Strukturdaten).

Die speziellen Befugnisse der Mitwirkungsaufgabe sind als Vorsorgemaßnahmen allgemein im Sicherheitsüberprüfungsgesetz sowie den speziellen Gesetzen, die das jeweilige Verfahren der vorbeugenden Personenüberprüfung einrichten, geregelt. Die vorsorgende Verbundspeicherung bleibt integral in der Speicherbefugnis des Bundesverfassungsschutzgesetzes erhalten (bisheriger § 10 Abs. 1 Nr. 3 / neuer § 36 Absatz 2 Satz 1 Nummer 3 zur Weiterverarbeitung) wobei Fachgesetze ergänzende Regelungen treffen (z.B. § 20 Abs. 2 SÜG).

Die Regelung fasst die bisherigen § 3 Absatz 2 Nummern 1, 2 und 4 zusammen, da Nummer 1 und 2 nur Spezialfälle von Nummer 4 sind und die Ausdifferenzierung im Gesetz funktionslos beleibt, da sich keine gesonderten Rechtsfolgen daran knüpfen.

Zu Nummer 2

Die Nummer entspricht den bisherigen § 3 Abs. 2 Satz 1 Nummer 5 mit Sätzen 3 und 4. Während die Sicherheitsüberprüfung zum vorbeugenden personellen Geheimschutz auch bei Personen, die in der Wirtschaft Verschlusssachenzugang benötigen, von Nummer 1 erfasst ist (§§ 24 ff. SÜG), betrifft Nummer 2 „Firmenüberprüfungen“ nach Maßgabe der Bestimmungen des Geheimschutzhandbuchs des BMWE. Hierbei wird vor der Aufnahme von Unternehmen in die Geheimschutzbetreuung (und damit vor Abschluss des öffentlich-rechtlichen Vertrages, der Voraussetzung für die Übertragung von VS-Aufträgen ist) vorsorglich insbesondere geprüft, ob eine Gefahr der Einflussnahme durch ausländische

Nachrichtendienste auf das Unternehmen besteht. Dazu können im Einzelfall auch Sicherheitsermittlungen erfolgen, indem Informationen von BAMAD und BND oder ausländischen Behörden, insbesondere Nachrichtendiensten beigezogen werden. Die Mitwirkungsaufgabe bedingt die vorsorgetypische Unternehmensspeicherung im Nachrichtendienstlichen Informationssystem, um bei nachträglich anfallenden Informationen die Risikolage der Geheimschutzbetreuung zu erkennen.

Zu Nummer 3

Die Reglung entspricht dem bisherigen § 3 Abs. 2 Nummer 3.

Zu § 3 (Begriffsbestimmungen)

§ 3 greift den bisherigen § 4 auf. Die über Legaldefinitionen hinausgehenden Regelungen im bisherigen § 4 Abs. 1 Sätze 3 und 4 (Entschließungsermessen bei Beobachtung von Einzelpersonen) sowie Satz 5 (Einsatzschwelle planmäßiger Beobachtung) sind systematisierend nunmehr in § 2 Absatz 3 aufgenommen.

Die Begriffsbestimmungen des bisherigen § 4 Absatz 1 genügen – unter Einbezug der Rechtsprechung dazu – bereits den Anforderungen der Normenklarheit (BVerfGE 162, 1 , – Rn. 184 ff.) und zwar auch zur Einsatzschwelle für nachrichtendienstliche Mittel (a.a.O. Rn. 186). Sie sind nunmehr im Interesse zusätzlicher Klarheit auf die Definitionen des Operationsmodus in Absatz 1 und die Präzisierung der Schutzgüter in Absatz 2 und 3 aufgeteilt.

Die Definitionen der Absätze 1 bis 5 konkretisieren die Aufgabenregelung in § 2 Absätze 1-3, gelten mithin wie diese ebenso für deren Vollzug durch Landesverfassungsschutzbehörden. Die Absätze 6 bis 10 treffen dagegen Begriffserläuterungen zu den Befugnisregelungen des BfV und sind danach für den Landesvollzug grundsätzlich irrelevant. Eine harmonisierte Entwicklung des Verfassungsschutzrechts in Bund und Ländern ist rechtspolitisch allerdings insgesamt anstrebenswert.

Zu Absatz 1

Der bisherige § 4 Absatz 1 enthält implizit auch eine Definition der Bestrebungen, die hier gesondert aufgegriffen wird. Da es sich bei der bisherigen Formulierung „ziel- und zweckgerichtet“ um Synoyme handelt, wird sie zu „zielgerichtet“ verschlankt.

Zu Absatz 2

Die Konkretisierung der Verfassungsschutzgüter in Absatz 2 übernimmt die entsprechenden Begriffsbestimmungen des bisherigen § 4 Absatz 1. Weitergehende Konkretisierungen hat die Rechtsprechung zu entsprechenden Normen geleistet. So schließt der Schutz der Funktionsfähigkeit der staatlichen Einrichtungen vor erheblichen Beeinträchtigungen den Schutz vor Einwirkungen durch Gewalt und Drohungen mit Gewalt auf die Wahrnehmung staatlicher Funktionen ein, wobei z.B. bereits die Anwesenheit möglicher Helfer terroristischer Gewalttäter die Fähigkeit des Staates, sich nach innen und nach außen gegen Angriffe und Störungen zur Wehr zu setzen, beeinträchtigt und somit seine Sicherheit gefährdet (BVerwGE 123, 114/120 - Rn. 21). Umfasst ist ebenso der Fall, dass die Bestrebungen geeignet sind, das Vertrauen der Bevölkerung zu erschüttern, vor gewaltsamen Einwirkungen in ihrem Staat geschützt zu sein (BGHSt 62, 102 - Rn. 22; Gesetzesbegründung zu § 89a StGB, BT-Drs. 16/12428, S. 14). Im Ergebnis ist die Innere Sicherheit auch ein Zustand des friedlichen und gewaltfreien Zusammenlebens der Bevölkerung (Roth, in: Schenke/Graulich Ruthig, §§ 3, 4 BVerfSchG Rn. 59). Um praktischen Anforderungen der Entwicklungsoffenheit von Konkretisierungen zu genügen, bleibt es auf der Gesetzesebene bei der bisherigen Regelung.

Zu Absatz 3

Im neuen Absatz 3 erhält der bisherige § 4 Absatz 2 eine an die jüngere Verfassungsrechtsprechung (BVerfGE 144, 20 [NPD]) angepasste Systematik.

Das Grundgesetz sieht eine wehrhafte Demokratie vor. Diese wehrhafte Demokratie bildet zugleich den Freiheitsrahmen für einen offenen Prozess der politischen Willensbildung, sogar einzelne Elemente der Verfassung kritisch zu hinterfragen (BVerfG a.a.O. - Rn. 535). Der Begriff der freiheitlichen demokratischen Grundordnung umfasst daher nur jene zentralen Grundprinzipien, die für den freiheitlichen Verfassungsstaat schlechthin unentbehrlich sind. Dies betrifft nicht nur das Begriffsverständnis zu Art. 21 Absatz 2 GG (BVerfG a.a.O. Ls. 3), sondern ebenso zum Bundesverfassungsschutzgesetz, denn der diskursive Freiheitsrahmen der Verfassung ist auch kein Gegenstand hoheitlicher Ausforschung unter Einsatz nachrichtendienstlicher Intensivbefugnisse.

Diese zentralen Grundprinzipien bedürfen zur Operationalisierung für die Verfassungsschutzaufgabe konkretisierender Ableitungen. Auch solche Ableitungen können wiederum vielfältig diskutabel und in einer freien Wissenschaft und offenen Gesellschaft auch vielfältig diskussionsbedürftig sein. Auch dieser Diskursraum und komplementäre politische Operationalisierungen sind nicht nachrichtendienstliches Beobachtungsfeld. Auch hier ist also nur das zwingende Substrat geeignet zur maßstäblichen Konkretisierung des Prinzips. Dagegen sind Positionen, zu denen vertretbar abweichende Mindermeinungen bestehen, als Anknüpfung der hoheitlichen Überwachungsaufgabe ungeeignet.

In Absatz 3 sind zu den staatsorganisatorischen Grundprinzipien solche zwingenden Ableitungen, die der Verfassungsrechtsprechung entnommen sind, mit aufgeführt. Vergleichbar den Erwägungen zur Sicherheit des Bundes ist ebenso bei den Staatsorganisationsprinzipien auch der Schutz der Funktionalität eingeschlossen, wie speziell zur Beeinträchtigung der Amtsführung bereits in der Aufgabennorm in § 2 Absatz 1 Nummer 1 ausdrücklich angesprochen. Auf noch detailliertere gesetzliche Festlegungen wird auch hier aber im Interesse der Entwicklungsoffenheit unter Berücksichtigung auch von Erkenntnissen in Rechtsprechung und Wissenschaft abgesehen.

Die Menschenwürdegarantie ist normativ komplexer, weshalb gesetzliche Fixierungen hier von vornherein weniger geeignet erscheinen, die Verwaltungspraxis nachhaltig anzuleiten. Zu nennen wären hier aber die Wahrung personaler Individualität, Identität und Integrität sowie die elementare Rechtsgleichheit (BVerfG a.a.O. Ls. 3.a, Rn. 539). Ein Politikkonzept, das auf die Ausgrenzung, Verächtlichmachung und weitgehende Rechtlosstellung von gesellschaftlichen Gruppen gerichtet ist, wäre mithin gegen die Menschenwürdegarantie gerichtet (BVerfG a.a.O. Rn. 635) und somit Anlass zur nachrichtendienstlichen Beobachtung.

Zu Absatz 4

Der Absatz enthält eine neue Legaldefinition zur Vereinfachung von Regelungen, die tatbestandlich an diese Sachverhalte anknüpfen. Die Begriffsbestimmung enthält sowohl den Oberbegriff (Bedrohungen) wie auch Bezeichnungen der einzelnen Teilbereiche. Der bereits alltagssprachlich ebenso wie in der Fachsprache eingeführte Begriff der „verfassungsfeindlichen“ Bestrebungen wird in Nummer 1 dabei nunmehr auch in das Gesetz eingeführt.

Zu Absatz 5

Zur Anknüpfung in Datenverarbeitungsbefugnisregelungen wird die Begriffsdefinition des Beteiligten eingeführt. Entsprechend der sicherheitsrechtlichen Materie ist der zurechenbare Kausalbeitrag zur Bedrohung maßgeblich. Dem störungs- und störerbezogenen Gefahrenabwehrrecht ist an sich die Unterscheidung von Täter und Teilnehmer, speziell Gehilfe/Unterstützer, fremd. Gleichwohl wird im nachrichtendienstlichen Sicherheitsrecht in Bezug auf Bestrebungen wegen des typischerweise höheren Potenzials „täterschaftlichen“ Handelns an der bisherigen besonderen Regelung zu Unterstützern mit der

Qualifikationsanforderung einer nachdrücklichen Unterstützung festgehalten (Nummer 2, bisher § 4 Abs. 1 Satz 2), um insoweit das Beobachtungsfeld angemessen zu begrenzen. Für eine entsprechende Unterscheidung in Bezug auf Tätigkeiten nach § 2 Abs. 2 Nummer 3 ist dagegen weiter kein Raum, da dem fördernden Bezug auf eine fremde Macht generell außerordentliches Gefährdungspotenzial inhärent ist.

Zu Absatz 6

Der bisher im Bundesverfassungsschutzgesetzt beispielsweise in § 9 Absatz 1 Satz 1 Nummer 2 verwendete Begriff „Quellen“ (der eine Beschränkung auf Informationsquellen suggeriert) wird nunmehr durch den passenderen Begriff „verdeckte Hilfspersonen“ ersetzt (so beispielsweise im neuen § 2 Absatz 4). Der Begriff umfasst sämtliche für das BfV verdeckt tätige Personen, also nicht nur Vertrauenspersonen und Informanten, sondern z.B. auch logistisch unterstützende Gewährspersonen und Legendengeber, also Personen, die logistische oder sonstige Hilfe leisten, ohne Informations-„Quellen“ zu sein. Über die Aufzählung im bisherigen § 8 Absatz 2 hinaus werden wegen ihrer besonderen Bedeutung nunmehr auch Informanten speziell aufgeführt. Dies sind Privatpersonen, die in Einzelfällen oder gelegentlich wegen ihrer Kontakte zu einem Beobachtungsfeld Hinweise geben, in Abgrenzung zu Vertrauenspersonen also nicht planmäßig zur gesteuerten Informationsbeschaffung eingesetzt werden, somit in der Typik des Einsatzmittels auch nicht gleiches – erhebliches – Eingriffsgewicht erreichen, sondern eher einem Zeugen in anderen Verfahren entsprechen (dem ggf. auch Vertraulichkeit zugesagt wird).

Zu Absatz 7

Mit den Absätzen 6 und 7 erfolgen Legaldefinitionen zur Beobachtungsbedürftigkeit. Hierüber wird das Gemeinwohlinteresse an der Aufklärung abstufend gewichtet, um damit das Rechtfertigungspendant zu abgestuft gewichteten Grundrechtseingriffen bei der Informationsbeschaffung zu bilden (vgl. speziell §§ 17 ff.): Erheblich eingreifende Aufklärungsmaßnahmen nur bei erheblich beobachtungsbedürftigen Bedrohungen und besonders erheblich eingreifende Maßnahmen nur bei besonders erheblicher Beobachtungsbedürftigkeit.

Diese Systematisierung setzt die Vorgaben der Verfassungsrechtsprechung um (BVerfGE 162, 1 – Rn. 192 f., 204), die zugleich auch die maßgeblichen Aspekte für die Gewichtung des Gefährdungspotenzials und der resultierenden Beobachtungsbedürftigkeit benannt hat (Rn. 194 ff.).

Mit Absatz 6 und 7 werden zwei Stufen qualifizierter Beobachtungsbedürftigkeit definiert. Die erste Qualifikationsstufe bildet die erhebliche Beobachtungsbedürftigkeit (Absatz 6). Noch gewichtiger ist die besonders erhebliche Beobachtungsbedürftigkeit (Absatz 7). Wie bei der Erforschung von Bedrohungen insgesamt genügt auch für die Gewichtung der Bedrohung bereits ein auf tatsächlichen Anhaltspunkten beruhender Verdacht.

Da Tätigkeiten nach § 2 Absatz 1 Nummer 3 vom Machtpotenzial eines Staates getragen sind, sind sie generell besonders erheblich beobachtungsbedürftig. Die erste Qualifikationsstufe der erheblichen Beobachtungsbedürftigkeit bezieht sich damit allein auf Bestrebungen nach § 2 Absatz 1 Nummern 1 und 2 und funktionsgefährdende Tätigkeiten nach § 2 Absatz 4.

Die Beurteilung der Gefährdungspotenzialität wird in Absatz 6 mit den Sätzen 2 bis 4 in abgestufter Intensität gesteuert. Satz 2 enthält eine ergebnisbindende Vorgabe (vgl. BVerfGE 169, 130 - Rn. 153). Satz 3 bezeichnet Kriterien, die für die Beurteilung maßgeblich sind, anders als nach Satz 2 aber nicht zwingend zur Einstufung als erheblich beobachtungsbedürftig führen. Nach Satz 4 sind diese Kriterien wiederum differenzierend zu gewichten. Die in Nummer 1 aufgeführten Kriterien führen regelmäßig zur Qualifikation, halten aber eine abweichende Bewertung im Einzelfall offen, speziell wenn das Vorgehen vollkommen dilettantisch ist (BVerfG a.a.O. Rn. 156, 159). Einbezogen sind auch funktionsgefährdende Tätigkeiten. Gewichtend wird dabei einerseits der besondere Eigensicherungsbedarf

des BfV berücksichtigt und andererseits der Umstand, dass mit dem besonderen Schutzgut (eine konkrete Einrichtung) zudem typischerweise eine größere Störungsnähe als bei der Bedrohung abstrakter Kollektivgüter (wie der freiheitlichen demokratischen Grundordnung) verbunden ist. Auch hier gilt allerdings, dass vollkommen dilettantische, letztlich risikofreie Tätigkeiten nicht das Gewicht erheblicher Beobachtungsbedürftigkeit erreichen. Nummer 2 und 3 enthalten dagegen Kriterien, die im Einzelfall offen zu bewerten sind und danach bei erheblichem Aktionspotenzial oder erheblichem Beeinflussungsumfang ebenso indiziell sind. Maßgeblich ist eine Gesamtbeurteilung, nach der das gegen die Schutzgüter des § 1 Absatz 1 gerichtete Handeln erfolgreich sein kann (Potentialität). Da insoweit bereits der nachrichtendienstliche Verdacht (tatsächliche Anhaltspunkte) die Erforschungsaufgabe eröffnet, bedeutet dies, dass es immerhin möglich erscheinen muss, dass die Verfassungsschutzgüter im Sinne solcher Potenzialität konkret bedroht sind. Das bedroht sein bleibt dabei im Vorfeld der Gefahr, betrachtet also auch Möglichkeiten perspektivischer Entwicklung.

Die Indikatoren in Satz 3 benennen die besonders praxisrelevanten Kriterien zur sachbezogenen Klassifizierung der Beobachtungsbedürftigkeit von Beobachtungsobjekten des Bundesamtes für Verfassungsschutz. Die Kriterien sind der Verfassungsrechtsprechung entnommen (BVerfGE 162, 1 - Rn. 194 ff.). Der Kriterienkatalog ist nicht abschließend, d.h. die Verwaltungspraxis bleibt offen für eine ebenso sachgerechte Einstufung atypischer Sachverhalte erheblicher Beeinträchtigungseignung.

Gerade in dem vom Verfassungsschutz aufzuklärenden Vorfeldbereich sind Bewertungen aufgrund geringer Tatsachendichte in besonderem Maße von Erfahrung, Fachwissen und nachrichtendienstlichen Erkenntnislagen abhängig, über die die Verfassungsschutzbehörde verfügt (BVerfGE 169, 130 - Rn. 149). Sie trifft eine prognostische Risikoabschätzung von hoher Komplexität (deutlich höher als etwa eine Störungsprognose im Sachverhalt einer bereits konkreten Gefahr), dies sowohl hinsichtlich des bedrohlichen Phänomens (der Bestrebungen und ihrer Erfolgsperspektive) als auch des Wirkungsbezugs zu Kollektivrechtsgütern (mit der ihnen inhärenten Komplexität einer Beeinträchtigungsanalyse). Die Abschätzung enthält sowohl wertende als auch prognostische Elemente, welche die Charakterisierung einer Annahme als „richtig“ oder „falsch“ nicht bezüglich aller Einzelheiten zulassen. Für diese Potenzialitätsbeurteilung besitzt das BfV deshalb eine Einschätzungsprärogative (vgl. BVerfG Beschluss vom 08. Dezember 2011 – 1 BvR 1932/08 – Rn. 38), die der politischen Kontrolle des Parlamentarischen Kontrollgremiums unterliegt.

Die Qualifikation der Gefährdungspotenzialität beruht auf den speziell zur jeweiligen Bedrohung vorliegenden tatsächlichen Anhaltspunkten, also konkreten Verdachtserkenntnissen, nicht allein auf allgemeinen Erfahrungssätzen. Gegenstand der Qualifikation sind jeweils bestimmte Bestrebungen oder Tätigkeiten (in der Diktion des Bundesverfassungsgerichts: bestimmte nachrichtendienstlich beobachtungsbedürftige Gruppierungen oder Aktionen).

Die Begriffsbestimmungen der neuen Absätze 6 und 7 sind für die Anwendung der Regelungen zur Informationsbeschaffung in §§ 16 ff. bedeutsam und betreffen damit lediglich den Gesetzesvollzug des Bundesamtes für Verfassungsschutz (anders als die Regelungen in Absatz 1 bis 5, die die Aufgabennorm des § 2 definitorisch konkretisieren und mit deren Anwendungsbereich auch für die Landesverfassungsschutzbehörden gelten).

Zu Nummer 1

Zu Buchstabe a

Die Gewaltorientierung ist ein besonders starker Indikator von Gefährdungspotenzialiät. Nur ganz besondere Einzefallumstände können ganz ausnahmsweise eine abweichende Bewertung tragen. Die Regelung kommt dabei auch nur zum Tragen, wenn es sich nicht bereits um Bestrebungen nach Satz 2 handelt, bei denen sich die Gewaltorientierung bereits in der Begehung von Straftaten manifestiert.

Zu Buchstabe b

Auch bei volksverhetzenden Bestrebungen gibt es Überschneidungen mit Bestrebungen nach Satz 2, bei denen die bindende Qualifikation nach Satz 2 vorgeht. Auch soweit der hetzende Modus Operandi nicht mit strafbarem Handeln verknüpft ist (etwa wenn Bestrebungen nach § 2 Absatz 1 Nummer 2 Buchstabe b durch Hetze gegen Bevölkerungsgruppen in anderen Staaten betrieben werden), sind abweichende Einstufungen bei aggressiv menschenverachtend betriebenen Bestrebungen jenseits vollkommen dilettantischen Vorgehens kaum vorstellbar.

Zu Buchstabe c

Buchstabe c verknüpft die Bedrohungsqualifikation mit Qualifikationsanforderungen, die im Vereinsrecht als Verbotsvoraussetzungen entwickelt und in der Rechtsprechung ausgeformt worden sind (vgl. etwa BVerwGE 134, 275 - Rn. 44, 81). Bereits der Begriff der Bestrebungen setzt zwar ein aktives, nicht jedoch ein auch kämpferisch-aggressives Vorgehen voraus (BVerfGE 162, 1 – Rn. 185). Hierzu genügt nicht, gegen die elementaren Grundsätze der Verfassung gerichtete Vorstellungen zu verbreiten, maßgeblich ist vielmehr, dass der Wille, die verfassungsfeindlichen Ziele zu verwirklichen, tragend ist, etwa indem die geschützten Verfassungsgrundsätze fortlaufend untergraben werden sollen (BVerwG, 21.09.2020 - 6 VR 1.20 (6 A 5.20) - Rn. 16; 24.06.2025 - BVerwG 6 A 4.24 – Rn. 149). Die Schwelle wird beispielsweise erreicht, wenn zum Kampf gegen diese Grundsätze aufgerufen wird (BVerfGE 149, 160 – Rn. 108, 144) oder dieser Kampf durch eine Atmosphäre der Angst betrieben wird. Es reicht also nicht Verbalradikalismus, es muss auch kämpferisch, etwa mit agitatorischer Rhetorik (BVerwG, 24.06.2025 - BVerwG 6 A 4.24 – Rn. 151) auf das Verhalten gezielt werden, sei es mit dem Ziel, aktive Unterstützung zu gewinnen oder diese z.B. durch Indoktrination zu stärken (vgl. Verbot „Artgemeinschaft“, Verfassungsschutzbericht 2023, S. 84), sei es mit einer Atmosphäre der Einschüchterung von Bürgern, die sich für die Werteordnung der Verfassung engagieren. Dies ist verfassungsrechtlich zugleich eine grundrechtsbeschränkende Schwelle (Artikel 9 Absatz 2, Artikel 18 GG). Die Beobachtungsbedürftigkeit folgt hier nicht mehr allein aus dem Erfordernis der Informiertheit der Bürgergesellschaft im demokratischen Prozess der gesellschaftlichen Auseinandersetzung mit Extremismus (Verfassungsschutz durch Öffentlichkeitsaufklärung), sondern unmittelbar aus dem Ordnungsrahmen des demokratischen Diskurses. Die Schwelle bezeichnet also einen Qualitätssprung verfassungsfeindlicher Bestrebungen, der qualifizierte Beobachtungsbedürftigkeit indiziert. Die Schutzrichtung ergibt sich nach Satz 1 aus den in § 2 Absatz 1 genannten Schutzgütern, bezieht mithin den Gedanken der Völkerverständigung mit ein, beispielsweise kämpferisch-aggressive Bestrebungen, die die militante Beseitigung Israels unterstützen. Die materielle Anknüpfung an Qualifikationskriterien des öffentlichen Vereinsrechts ändert nicht den Charakter der nachrichtendienstlichen Erforschung von Bedrohungen. Veranlassend sind dabei tatsächliche Anhaltspunkte, nicht erst die verbotsrechtfertigende Überzeugungsgewissheit. Demzufolge ist auch nicht vorausgesetzt, dass bereits gesicherte Erkenntnisse darüber vorliegen, dass die Bestrebungen durch solchen Operationsmodus geprägt sind. Die Aufklärung kann gerade auch der Klärung dienen, welche Bedeutung die Form des kämpferisch-aggressiven Vorgehens bei der Zielverfolgung hat. Für die Qualifikation als erheblich Beobachtungsbedürftig genügen mithin Erkenntnisse zum kämpferisch-aggressiven Vorgehen, auch wenn zunächst offen ist, ob dies prägend für die Bestrebungen ist.

Buchstaben a und b sind Spezialfälle kämpferisch-aggressiven Vorgehens, die im Interesse der Normenklarheit und angesichts ihres noch stärker beurteilungsleitenden Gehalts gesondert aufgeführt werden. Auch bei sonstiger kämpferisch-aggressiver Vorgehensweise besteht zwar die Regelvermutung der erheblichen Beobachtungsbedürftigkeit. Komplementär zur Anwendungsbreite dieser Indikation müssen hier gleichwohl auch weitere Sachverhaltsumstände für eine Gesamtwürdigung betrachtet werden. Insbesondere dann, wenn Kriterien nach Nummern 2 oder 3 hinzutreten, wäre auch hier lediglich bei vollkommen dilettantischem Vorgehen eine abweichende Beurteilung begründet.

Zu Buchstabe d

Buchstabe d berücksichtigt, dass gerade Abschottung eine Aufklärung auch mit nachrichtendienstlichen Mitteln bedingt (BVerfGE 162, 1 - Rn. 196). Einem planmäßig verschleiernden Vorgehen korrespondiert das Erfordernis, die Bestrebungen – auch zur Bewertung ihrer Potenzialität – ebenso unter Einsatz verdeckter Maßnahmen aufzuklären, um die Verschleierung zu durchbrechen.

Zu Nummer 2

Nummer 2 knüpft – ebenso wie Nummer 3 – an das Wirkungspotenzial von Bestrebungen an (BVerfGE 162, 1 - Rn. 195). Aus den benannten Indikatoren folgt noch nicht per se die Qualifikation der erheblichen Beobachtungsbedürftigkeit, vielmehr müssen hierzu noch die konkreten Sachverhalte betrachtet und darauf bewertet werden, ob sich hieraus die nach Satz 1 vorausgesetzte Eignung ergibt. Maßgeblich ist also, ob Aktionspotenzial und Einflussnahme in diesem Sinne erheblich sind.

Maßgeblich für das nach Nummer 2 indizielle Aktionspotenzial sind insbesondere die Anzahl der Beteiligten, deren Mobilisierungsfähigkeit, der Organisationsgrad und die Finanzkraft. Aktionspotenzial folgt aus qualifizierenden Fähigkeiten, besondere Wirkungen zu erzielen, unabhängig davon, ob diese dazu auch bereits erkennbar eingesetzt werden. Wenn etwa Anhaltspunkte für extremistische Netzwerke in Bereichen öffentlicher Verwaltung bestehen, begründet dies erhebliche Aufklärungsbedürftigkeit, denn hier können potenziell solche Funktionen für extremistische Ziele missbraucht werden, zudem wird in jedem Fall das Vertrauen in die Verwaltung geschädigt.

Zu Nummer 3

Nummer 3 bezieht sich auf die Wirkungsweise von Bestrebungen (BVerfGE 162, 1 - Rn. 195 und 197). Relevant sind etwa erlangte öffentliche Ämter und Mandate oder auch tatsächlich wirkungsbreite überregionale oder regelmäßige Publikationen, Bündnisse oder Unterstützerstrukturen. Darunter fallen insbesondere auch solche Bestrebungen, die ohne feste oder regional etablierte Organisationsstruktur über ihre gewählten Verbreitungsformen gezielt eine breite Anhängerschaft für sich gewinnen können, etwa als politische „Influencer“ auf reichweitestarken sozialen Medien. Als weitere erhebliche Wirkungsweise gelten auch der systematische Einsatz von Desinformationen oder eine Beeinflussung durch eine Atmosphäre der Angst. Bei der Gewichtung können auch Zielgruppen der Einflussnahme bedeutsam sein, etwa nach Beeinflussbarkeit (typischerweise bei Minderjährigen erhöht) oder Folgereichweiten (bei Beeinflussung von ihrerseits nichtextremistischen zivilgesellschaftlichen Organisationen). Fähigkeiten bzw. Aktionspotenzial sowie gesellschaftliche Einflussnahme können sich auch aus dem Zusammenwirken verschiedener Beobachtungsobjekte ergeben, die u.U. bewusst arbeitsteilig spezialisiert kooperieren. Insoweit ist eine schutzgutbezogene Gesamtbetrachtung nötig, die solchen Fähigkeiten- und Wirkungsverbund als solchen würdigt und seine Teile nach der Gesamtbedrohung klassifiziert. Die Betrachtung der Einflussnahme muss gegebenenfalls auch zielgruppenbezogen erfolgen und dabei speziell die Ausrichtung auf besonders vulnerable Gruppen und die Folgen von deren Beeinflussung würdigen. Dies gilt etwa bei gezielter Ausrichtung auf Minderjährige, die entwicklungsbedingt besonders beeinflussbar sein können und deren Folgeaktivitäten mit jugendtypischem Eifer unter begrenzter Reflektion und Impulskontrolle erwartbar sind, dabei zudem besonders anschlussfähig für weitere Jugendliche, die nach einer Identitätsvergewisserung über sinnstiftende Ideale und einer Zugehörigkeit vermittelnden peer group sind.

Zu Absatz 8

Absatz 7 regelt die gegenüber erheblicher Beobachtungsbedürftigkeit nochmals besonders erhebliche Beobachtungsbedürftigkeit.

Zu Nummer 1

Zu Buchstabe a

Buchstabe a ist ein Qualifikationstatbestand gegenüber Absatz 6 Satz 2. Der Modus Operandi schließt hier die Begehung schwerer Straftaten ein, was ein Gefährdungspotenzial darstellt, das auch besonders erheblich eingreifende Überwachungsmaßnahmen zur Aufklärung der Bestrebungen rechtfertigt. Unerheblich ist, ob es sich dabei um Erfolgs- oder Gefährdungsdelikte handelt. Entscheidend ist die Indikation des Unrechtsgehalts durch den Strafrahmen, damit des Maßes der Rechtsfeindlichkeit und hieraus abgeleitet des Gefährdungspotenzials der Bedrohung.

Zu Buchstabe b

Mit Buchstabe b tritt als Qualifikationselement die Fortsetzung der Tätigkeiten eines verbotenen Vereins als Ersatzorganisation hinzu. Hier ist das Vertrauen der Bevölkerung in die Funktionsfähigkeit der Herrschaft des Rechts und damit die Sicherheit des Bundes qualifiziert gefährdet, wenn der Staat das ausgesprochene Verbot nicht wirksam durchsetzen und dazu Nachfolgeaktivitäten effektiv, auch unter Einsatz besonders erheblich eingreifender Methoden aufklären kann.

Im Übrigen werden legalistische Bestrebungen von der Qualifikationsstufe der besonders erheblichen Beobachtungsbedürftigkeit nicht erfasst. Dies ist nicht bereits verfassungsrechtlich vorgegeben (extremistische Großparteien mit womöglich beachtlicher Vertretung in Verfassungsorganen, insbesondere den Parlamenten, können im Gefährdungspotenzial die Bedrohung durch militante Kleingruppen sogar übersteigen). Rechtspolitisch erscheint für die gesellschaftliche Akzeptanz nachrichtendienstlicher Frühaufklärung aber weiter angemessen, besonders erheblich intensive Eingriffe auf Phänomene zu beschränken, die nicht allein in Ihrer Potenzialität, sondern auch bereits in ihrem Modus Operandi durch kriminelles Vorgehen evident gefährlich sind. Vorausgesetzt ist damit, dass solche Modalität zur Zielverfolgung eingesetzt wird, nicht hingegen, dass sie ausschließlich derart erfolgt. Es qualifiziert also bereits hinreichend, dass die Ziele jedenfalls auch in dieser Weise verfolgt werden. Dabei behält die nachrichtendienstliche Aufgabe zur Frühaufklärung mit relativer Niederschwelligkeit ihren Mehrwert gegenüber erst polizeilichen Ermittlungen, die eine höhere Gefahrkonkretisierung voraussetzen würden. Außerdem lassen sich nur im nachrichtendienstlichen Blickfeld auch Querbezüge – etwa zu legalistischen Bestrebungen – umfassend in ein Gesamtbild einbeziehen.

Zu Nummer 2

Wegen des dahinterstehenden Machtpotenzials werden sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht mit Nummer 2 generell als besonders erheblich beobachtungsbedürftig klassifiziert.

Zu Nummer 3

Zu Buchstabe a

Buchstabe a bezeichnet Sachverhalte mit besonders besonders erheblichen Gefährdungspotenzial aufgrund funktionsgefährdender Tätigkeiten. Bedienstete und verdeckt eingesetzte Hilfspersonen besitzen Insiderwissen, das besonders schädigend eingesetzt werden kann. Personen mit Liegenschaftszugang, wie etwa Wartungspersonal zu technischen Einrichtungen, haben besondere Kenntnisse, Ausforschungs- und Einwirkungsmöglichkeiten, die auch bei früherem Zugang noch Wissensbasis mit besonderem Schädigungspotenzial bleiben. Ebenso einbezogen sind weitere für das BfV ausgeübte sicherheitsempfindliche Tätigkeiten (§ 1 Absatz 2 SÜG), die zwar nicht mit einem Liegenschaftszutritt, aber doch mit sicherheitsrelevanten Einblicken in die Arbeit oder die Infrastruktur des BfV, beispielsweise Software-Anbieter und Planungsbüros.

Zu Buchstabe b

Ebenso besitzen Cyberangriffe auf das BfV besonderes Gefährdungspotenzial. Dies gilt gleichermaßen für Angriffe, die Informationen ausforschen sollen, wie für Angriffe, die die Funktion des IT-Systems beeinträchtigen sollen. Bezeichnet ist das Mittel der funktionsgefährdenden Tätigkeit. Eine Störung muss noch nicht herbeigeführt sein. Es reichen also tatsächliche Anhaltspunkte zum Vorgehen der Angreifer, es muss nicht bereits zum unerlaubten Zugriff gekommen sein.

Zu Buchstabe c

Die Regelung erfolgt wertungssynchron zu Nummer 1 Buchstabe a. Erfolgt die Tätigkeit für eine fremde Macht, handelt es sich um eine sicherheitsgefährdende Tätigkeit, deren Qualifikation gemäß Nummer 2 erfolgt, so dass es bei solchem Potenzialhintergrund nicht noch zusätzlich auf Straftatenbegehung ankommt

Zu Absatz 9

Die Regelung übernimmt im Wesentlichen die Legaldefinition aus dem bisherigen § 19 Absatz 3.

Zu Nummer 1

In Nummer 1 wird zur systematischen Transparenz der Bezug zu den Verfassungsschutzzwecken mit dem Verweis auf § 1 Absatz 1 hergestellt. Die auch in der Aufgabennorm mit § 2 Absatz 1 Nummer 2 Buchstabe b aufgeführten originären Verfassungsschutzgüter der Völkerverständigung und des friedlichen Zusammenlebens der Völker bleiben einbezogen.

Zu Nummer 2

Die neue Formulierung ersetzt den allgemeinen Bezug auf „überstaatliche Einrichtungen“ durch den Bezug auf die Europäische Union, die damit bedeutungsgerecht speziell herausgestellt wird. Im Übrigen bleiben internationale Organisationen erfasst, dabei auch solche, denen Deutschland Hoheitsrechte übertragen hat (also in der bisherigen – in der völkerrechtlichen Fachbegrifflichkeit unüblichen – Diktion „überstaatliche“ Einrichtungen).

Zu Nummer 3

Die Regelung ist unverändert übernommen.

Zu Nummer 4

Der bisherige Begriff der „körperlichen Integrität“ wird – inhaltsgleich - durch den grundrechtlichen Begriff der körperlichen Unversehrtheit ersetzt, um den Bezug klarer zu machen. Da die Begriffsbestimmung als Anknüpfung für Schutzaufgaben dient, wird der Individualrechtsgüterschutz erweitert, indem einerseits auch die sexuelle Selbstbestimmung einbezogen wird (vgl.BVerfGE 156, 65 - Rn. 277) und andererseits eine allgemeine Öffnung für gleichgewichtige Schutzerfordernisse vorgenommen wird (beispielsweise Gesundheit, BVerfGE 133, 277 - Rn. 203; auch komplexere Rechtsgüter wie das Kindeswohl können u.U. berührt sein).

Entsprechend der Regelungssystematik sind lediglich Rechtsgüter benannt, nicht Eingriffsmodalitäten. Der bisherige Bezug auf „eine erhebliche Gefährdung im Einzelfall“ entfällt daher, zumal die Formulierung eher missverständlich war (der Bezug auf eine „Gefährdung im Einzelfall“ ist als konkrete Gefahr missdeutbar, was im nachrichtendienstlichen Kontext nicht gemeint sein kann). Die Regelung kommt daher auf die in der Gesetzespraxis übliche Regelungsweise zurück, die auch in der Verfassungsrechtsprechung abgesichert ist (vgl. BVerfGE 162, 1 – Rn. 298 f., 311). Ist bei einem Eingriffssachverhalt im Eingriffszeitpunkt

damit zu rechnen, dass die anlassgebende Situation das zu schützende Rechtsgut der körperlichen Unversehrtheit oder Freiheit nur unerheblich gefährdet, bleibt dies unter Anwendung der Verhältnismäßigkeitsschranke zu würdigen.

Zu Absatz 10

Die Regelung greift die bisher in § 19 Absatz 2 enthaltene Legaldefinition auf (da hier lediglich die Gefährdungssituation von Rechtsgütern definiert wird, ohne speziellen Bezug auf besonders gewichtige Rechtsgüter). Erläuterungen zum Begriffsverständnis enthalten die Gesetzgebungsmaterialien der Vorschrift (BT-Drs. 20/9345, Seite 23).

Zu Absatz 11

Der Begriff der besonderen Befugnisse ist Oberbegriff für nachrichtendienstliche Mittel und qualifiziert eingreifende sonstige Befugnisse, wie qualifizierte Ersuchen um Unternehmensauskünfte (die über Bestandsdatenerhebung hinaus gehen, § 12 Absatz 3).

Zu § 4 (Bedrohungsaufklärung durch das Bundesamt für Verfassungsschutz)

Die Sachzuständigkeitsregelung des bisherigen § 5 wird einerseits zur originären Nachrichtendienstaufgabe des BfV (neuer § 4) und andererseits zu seiner Zentralstellenfunktion (neuer § 5) übersichtlicher in gesonderten Paragraphen geregelt.

Zu Absatz 1

Die Regelung entspricht dem bisherigen § 5 Absatz 1. Dessen Nummer 2 wird hier der neuen Systematik angepasst, die die Bedeutungsgewichtung nicht selektiv unter Bezug auf Gewaltorientierung, sondern sachgerechter nach Beobachtungsbedürftigkeit und hierzu mit einem breiteren Indikatorenmodell vornimmt. Der neue Satz 2 trägt dem Umstand Rechnung, dass der Begriff der Bedrohung gemäß § 3 Absatz 4 auch funktionsgefährdende Tätigkeiten einschließt, die Eigensicherungsaufgabe (§ 2 Absatz 4) hingegen wie bisher vom BfV wahrgenommen wird, ohne dass es dazu eines Benehmens mit dem LfV bedürfte.

Zu Absatz 2

Der Absatz trifft neue Regelungen zur Behandlung von Beobachtungsobjekten. Die Einstufung als Beobachtungsobjekt ist die Grundentscheidung zur systematischen Beobachtung, die bei einem Personenzusammenschluss nachfolgend eine Vielzahl von Personen betreffen kann. Wegen dieser grundlegenden Bedeutung wird die Entscheidung mit Satz 2 nunmehr gesetzlich dem Präsidenten oder der Präsidentin des BfV vorbehalten. Dabei handelt es sich nach § 2 Absatz 3 Satz 1 grundsätzlich um eine gebundene Entscheidung (Ermessen nur in den Fällen des § 2 Absatz 3 Satz 2). Dennoch liegt eine relevante Verfahrenssicherung darin, dass die behördeninterne Feststellung der Voraussetzungen dem Präsidenten oder der Präsidentin vorbehalten ist, zumal dem eine komplexe Sachverhaltsbewertung zugrunde liegt. Die Entscheidung hat behördeninterne Funktion, sie ist nicht auf eine unmittelbare Rechtswirkung nach außen gerichtet.

Satz 3 kategorisiert die Beobachtungsobjekte danach, ob lediglich ein Verdacht verfassungsfeindlicher Bestrebungen besteht oder diese vom BfV als gesichert eingeschätzt werden. Speziell an den Verdachtsfall knüpfen sich besondere Rechtsfolgen für die Überprüfung einer Fortsetzung der Aufklärung (Absatz 3) wie auch die Öffentlichkeitsunterrichtung (§ 45 Absatz 1 Satz 2). Allgemein gehört es zur Fachlichkeit, bei Übermittlungen den Empfänger auch über den Erkenntnisstand zu informieren, also darüber, ob lediglich Anhaltspunkte für eine mitgeteilte Schlussfolgerung vorliegen oder Tatsachen abschließend geklärt sind.

Zu Absatz 3

Der Absatz trifft spezielle Maßgaben zu Verdachtsfällen, in denen einerseits die Einsatzschwelle systematischer Beobachtung auch mit nachrichtendienstlichen Mitteln aufgrund tatsächlicher Anhaltspunkte erreicht ist (BVerfGE 162, 1 – Rn. 186), andererseits aber nach dem Erkenntnisstand noch nicht gesichert ist, dass es sich tatsächlich um verfassungsfeindliche Bestrebungen handelt. Dieser bloßen Verdachtslage entspricht die gesetzlich vorgeschriebene periodische Überprüfung (Satz 2) sowie die zeitliche Begrenzung durch eine Verhältnismäßigkeitsabwägung von Beobachtungsdauer und Beobachtungsbedürftigkeit unter Einbezug der Verdachtsdichte (Satz 3) sowie der Verfahrenssicherung durch - parlamentsverantwortliche – Entscheidung des Bundesministeriums des Innern in Ausnahmefällen eines 5 Jahre übersteigenden Verdachtsfalls. Solche Verdachtsfallfortsetzung muss Ausnahme sein, kann aber notwendig sein, wenn etwa sehr große Personenzusammenschlüsse (zugleich Indikator hoher Gefährdungspotenzialität) mit inhomogenen und womöglich intransparenten, u.U. klandestin operierenden Strömungen Beobachtungsobjekt sind und aufgrund intern komplexer Verhältnisse unübersichtlich ist, ob die extremistischen Kräfte den Personenzusammenschluss bereits nachhaltig so beherrschen, dass sie verfassungsfeindliche Ziele in der Ausrichtung des Personenzusammenschlusses durchsetzen können.

Neben der periodischen Überprüfung der Verdachtsverdichtung ist der Verdachtsfall (gegenüber einer gesicherten Einstufung) vornehmlich für die Außendarstellung bedeutsam, in der darauf hinzuweisen ist, dass lediglich der Verdacht, aber noch keine gesicherte Erkenntnis vorliegt (§ 45 Absatz 1 Satz 2). Für einzelne nachrichtendienstliche Maßnahmen ist dagegen nicht wesentlich, ob Bestrebungen bereits als gesichert extremistisch erkannt sind oder zunächst nur der Verdacht solcher Bestrebungen besteht (anders beim bloßen Prüffall, Absatz 4). Wesentliche Aufgabe der Verfassungsschutzbehörden ist gerade, als Frühaufklärungssystem verdachtsbasierte Gefahrerforschung niederschwellig (deshalb institutionell getrennt von polizeilichen Zwangsbefugnissen) durchzuführen. Allerdings setzt jede Maßnahme eine konkrete Verhältnismäßigkeitsbeurteilung voraus (§ 8 Absatz 3, § 30 Absatz 3), die ihrerseits nicht allein folgenbezogen vorzunehmen ist, sondern auch die veranlassende Erkenntnisdichte einbeziehen muss. Dies betrifft vornehmlich die die Maßnahmerichtung begründende Erkenntnislage (§ 16 Absatz 5). In einem frühen Stadium der Verdachtsfallbearbeitung kann aber auch geboten sein, ebenso die Basiserkenntnislage zum Beobachtungsobjekt in eine Gesamtabwägung der Verhältnismäßigkeit einzelner Maßnahmen einzubeziehen.

Zu Absatz 4

Der Absatz regelt den sogenannten Prüffall, in dem noch keine systematische Beobachtung stattfindet, sondern zunächst von allgemeinen Erkenntnissen veranlasste Verdachtsschöpfung unter Beschränkung der Informationssammlung vornehmlich auf offene Quellen erfolgt (vgl. BVerfGE 162, 1 – Rn. 189), um zu klären, ob ein Verdacht begründet ist. Auch hier erfolgt keine Prüfung ins Blaue hinein, die anlassgebende Tatsachengrundlage ist jedoch noch nicht verdachtstragend, legt aber immerhin nach fachlicher Einschätzung unter Einbezug nachrichtendienstlichen Erfahrungswissens eben solche Prüfung nahe. Diese Veranlassung durch den konkreten Sachverhalt bringt die Voraussetzung der „ersten Anhaltspunkte“ zum Ausdruck. Der Sache nach müssen auch hier also tatsächliche Anhaltspunkte vorliegen, die allerdings noch nicht die hinreichende Aussagekraft haben, bereits eine nachrichtendienstliche Beobachtung rechtfertigenden Verdacht zu begründen, sondern zunächst eher vage in Richtung möglicher Bestrebungen hindeuten.

Satz 2 beschränkt die Verdachtsvorprüfung auf Maßnahmen geringer Eingriffsintensität. Nachrichtendienstliche Mittel dürfen zu Ermittlungen in einem Prüffall nicht eingesetzt werden. Wesentliche Erkenntnisgrundlage sind allgemein zugängliche Quellen. Hierbei darf es auch in einer Weise vorgehen, bei der nicht offen erkennbar wird, dass das BfV Daten erhebt, etwa bei Internetermittlungen. Dabei darf es nach Satz 3 jedoch kein schutzwürdiges

Vertrauen in Anspruch nehmen, etwa indem Vertrauensbeziehungen in Internetforen aufgebaut würden (die grundsätzlich nicht vom Vertrauen in die Identität anderer Teilnehmer geprägt sind). Im Übrigen kommt auch eine büromäßige Abklärung etwa durch Registerabfragen in Betracht. Fallen beim Einsatz nachrichtendienstlicher Mittel gegen ein Beobachtungsobjekt Informationen (etwa aus Zusammenarbeitsbezügen) an, die zugleich Anhaltspunkte für extremistische Bestrebungen des Prüffalls darstellen, dürfen diese auch zur Bewertung des Prüffalls herangezogen werden. Hierbei handelt es sich nicht um eine Erhebung zum Prüffall, sondern eine Zweckänderung nach § 36 Absatz 1 Satz 3.

Diese Prüfphase im Verdachtsvorfeld bleibt zeitlich eng begrenzt (Satz 3) und kann nur Ausnahmsweise über 2 Jahre hinaus erstreckt werden, dies jedoch nur mit der Verfahrenssicherung eines Entscheidungsvorbehalts beim Präsidenten oder der Präsidentin des BfV. Diese Billigung kann für höchstens 2 Jahre erfolgen, allerdings nach deren Ablauf wiederholt werden („jeweils“). Bei der Wiederholungsoption handelt es sich um eine Reserveregelung für äußerst außergewöhnliche Sachverhalte. Es ist kaum vorstellbar, einen Prüffall über 4 Jahre hinaus fortzusetzen. Tritt ein solcher besonders exotische Sachverhalt dennoch auf, muss auch hier jedoch angemessen verfahren werden können.

Zu § 5 (Zentralstellenaufgaben des Bundesamtes für Verfassungsschutz)

Die Regelung übernimmt die Regelungen des bisherigen § 5 Absatz 2 bis 5 (dessen Absatz 1 ist in § 4 Absatz 1 aufgenommen, da nunmehr einerseits originäre Aufklärungsaufgabe und andererseits Zentralstellenfunktion in gesonderten Paragraphen geregelt werden). Die gesetzlich neu geregelte Eigensicherungsaufgabe (§ 2 Absatz 4) ist in der Regelung des Absatzes 1 Satz 1 nicht eingeschlossen, d.h. solche zentrale Auswertung ist nicht gesetzlich obligatorisch, sondern flexibler dem pflichtgemäßen Ermessen des BfV überlassen.

Absatz 3 nimmt die Option, dass der MAD einvernehmlich in Koordination und Unterstützung einbezogen wird, im Gesetz auf. In der Praxis wird dies bereits gelebt, insbesondere mit der Teilnahme der MAD-Leitung an den vom BfV veranstalteten periodischen Tagungen der Amtsleitungen der Verfassungsschutzbehörden und der Teilnahme des MAD am NADIS.

Absatz 4 Satz 2 enthält neu eine Informationspflicht zum Auslandsverkehr, damit die Zentralstelle insoweit den Gesamtüberblick behält und nötigenfalls koordinativ tätig werden kann (vgl. bereits § 3 Absatz 4 Satz 2 BKAG). Das BfV ist gegebenenfalls seinerseits nach den allgemeinen Vorschriften verpflichtet, die Informationen weiterzugeben, beispielsweise nach § 6 Absatz 1 an den MAD, wenn für dessen Aufgaben ebenfalls relevant.

Zu § 6 (Gegenseitige Unterrichtung der Verfassungsschutzbehörden; nachrichtendienstliches Informationssystem)

Zu Absatz 1

Die Regelung übernimmt den bisherigen § 6 Abs. 1, bezieht aber auch hier (bislang nur in Absatz 2) den MAD mit ein, da er sachlich kongruente Aufgaben in seinem speziellen Zuständigkeitsbereich hat. Diese bisher bereits in § 3 Abs. 3 Satz 1 MADG getroffene Regelung zum MAD erfolgt damit im Interesse besserer Regelungstransparenz künftig synchron auch im Bundesverfassungsschutzgesetz.

Die Regelung bezieht nicht mehr die Mitwirkungsaufgaben ein (§ 2 Abs. 5 bzw. § 2 Abs. 3 MADG), deren Kern darin besteht, Sicherheitsermittlungen und Vorsorgespeicherung abgelöst von bereits vorhandenen tatsächlichen Anhaltspunkten für Bedrohungen durchzuführen. Liegen hingegen solche Anhaltspunkte vor, folgt die Übermittlungspflicht bereits aus der Relevanz für die Aufgaben nach § 2 Absatz 1, auch soweit eine Anschlussnutzung zudem noch für die Mitwirkungsaufgabe nach § 2 Absatz 5 erfolgen wird. Deren Einbezug in die Regelung des Absatzes ist danach sachlich unnötig und im Ergebnis eher verwirrend.

Die im Abschnitt 3 generell gewählte Voraussetzung, dass die Übermittlung auf Grund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist, wird hier bereichsspezifisch eingepasst, indem das Erfordernis der „relevanten“ Informationen durch den Bezug auf „bestimmte Bedrohungen“ konkretisiert wird. Eine solche Parallelisierung legt das Bundesverfassungsgericht in seinem Urteil zum Bayerischen Verfassungsschutzgesetz nahe (BVerfGE 162, 1 - Rn. 258; Verfahrensgegenstand war allerdings nicht die Übermittlung zwischen Verfassungsschutzbehörden). Die Relevanz-Voraussetzung fordert, dass die Übermittlung konkret veranlasst ist, mithin nicht gewissermaßen ins Blaue bzw. anlassfrei auf Vorrat erfolgt. Beim Teilen von Informationen im Verfassungsschutzverbund muss dabei berücksichtigt werden, dass die Aufgabe nach § 2 Absatz 1 (wie im bisherigen § 3 Absatz 1) gemeinsame Aufgabe der Verfassungsschutzbehörden ist. Wesentlicher Inhalt dieser Aufgabe ist auch ein umfassendes Lagebild sowie das Erkennen auch länderübergreifender Phänomene. Erst mit dem Zusammenführen von Informationen werden unter Umständen Zusammenhänge erkennbar, die sich aus der isolierten Sicht einer Landesbehörde womöglich nicht erschließen, beispielsweise bei je regionalen Vorgängen in verschiedenen Ländern, die jedoch einem gemeinsamen Vorgehensmuster folgen. Die je eigene Aufgabe zur Aufklärung bestimmter Bestrebungen oder Tätigkeiten verlangt danach grundsätzlich den Abgleich im Verbund darauf, ob dort ergänzende aufklärungsrelevante Informationen vorliegen, was einen entsprechenden Informationsaustausch voraussetzt. Dies bringt die aktuelle Formulierung in § 6 Absatz 1 zum Ausdruck (vgl. BT-Drs. 18/4654, S. 22). Eine atomisierende Zersplitterung von Informationen in Insellösungen, die erst nach erkannten – tatsächlich der Aufgabe nach aber zu erforschenden – Zusammenhangsanhaltspunkten im Verfassungsschutzverbund weitergegeben würden, war zentraler Kritikpunkt des NSU-Untersuchungsausschusses des Deutschen Bundestages (BT-Drs. 17/14600, S. 864: „Nach den Feststellungen des Ausschusses hatten mehrere Verfassungsschutzbehörden Informationen gewonnen, die für die Suche nach dem Trio bedeutsam gewesen wären. Diese Informationen wurden aber teilweise nicht oder unzureichend ausgewertet, nirgends zusammengeführt und nicht verlässlich für die Ermittlungen nutzbar gemacht.“). Unter Berücksichtigung dieser Besonderheiten der integralen Verbundaufgabe zur Aufklärung wird an der bereichsspezifischen Regelung der Informationsteilhabe im Verbund festgehalten.

Der Bezug auf bestimmte Bedrohungen verschließt dabei auch nicht die Zusammenarbeit in aufgabenrelevanten Querschnittsprojekten, die nicht allein in Bezug auf bestimmte Bedrohung nutzbar sind, für die aber bestimmte Bedrohungen anlassgebend sind, um diesbetreffende Aufgaben verbessert wahrnehmen zu können. Ein Beispiel wäre etwa ein wissenschaftliches Auswertungsprojekt, das Radikalisierungsverläufe nicht nach Beobachtungsobjekten, sondern übergeordnet, z.B. für Phänomenbereiche (wie Rechtsextremismus oder Islamismus) analysiert. Die Erkenntnisse können innerbehördlich zur personenbezogenen Aufgabenpriorisierung (nach Gefährdungspotenzialen) wie auch im Informationsweg zur Gestaltung von externen Präventionsprojekten nutzbar sein, was jeweils auch den Aufgaben in Bezug auf die anlassgebenden Bedrohungen dient. Ein weiteres Beispiel wäre die Fortentwicklung der eigenen Methodik durch den Austausch von guten Praktiken unter Bezug auf Realfälle und dort erzielte Erfolge. Auch dies ist kein Informationsaustausch „ins Blaue“, sondern konkret veranlasst und unmittelbar auf die Aufgabenwahrnehmung bezogen.

Zu Absatz 2

Die Regelung übernimmt den bisherigen § 6 Absatz 2, wobei der MAD nunmehr nicht lediglich fakultativ, sondern obligatorisch einbezogen wird (die vorausgegangen fakultative Regelung berücksichtigte, dass die Umsetzung zunächst technische Voraussetzungen hat, die zwischenzeitlich realisiert sind). Ergänzend aufgenommen sind Speicherungen über funktionsgefährdende Tätigkeiten, die nicht notwendig in den umfassenden Informationsaustausch nach Absatz 1 einzubeziehen sind, aber für die anderen verbundbeteiligten Behörden immerhin in der Verbunddatenbank auffindbar sein müssen, wenn beteiligte Personen auch ihnen gegenüber Bedeutung erlangen. Da der neue Absatz 1 die Mitwirkungsaufgaben nicht mehr erfasst, wird als Folgeänderung die weiter gebotene Speicherung im

nachrichtendienstlichen Informationssystem nunmehr in Satz 2 speziell ergänzt. Der nähere Datenkranz ist ggf. fachgesetzlich geregelt (vgl. etwa § 20 Absatz 2 SÜG oder § 7 Absatz 9 LuftSiG, § 5 Absatz 5 Satz 4 WaffG). In die Verarbeitungsregelung des Satzes 3 wird nunmehr die Datenpflege nach § 38 in Korrektur eines vorausgegangenen Redaktionsversehens ausdrücklich einbezogen. Diese Verarbeitungsregelungen regeln bundesrechtlich auch die Datenverarbeitung der Landesbehörden in der Verbunddatenbank des Bundes (kompetenziell unproblematisch: BVerfGE 133, 277 – Rn. 97). Abweichende Landesregelungen zur Datenverarbeitung in Amtsdateien der Länder werden dadurch im Interesse einer harmonisierten Rechtsgrundlage, die auch für ein bruchfreies Gesamtbild der Erkenntnislage bedeutsam ist, verdrängt. Die bundesrechtliche Regelung betrifft dabei allein vorhandene Daten und verpflichtet also nicht etwa zu Datenerhebungen. Die dies betreffenden landesrechtlichen Schranken bleiben mithin unberührt.

Zu Absatz 3

Die Regelung übernimmt den bisherigen § 6 Absatz 3. Die Verweisung auf § 64 BDSG wird durch Bezug auf den allein einschlägigen Absatz 3 präzisiert. Gleichzeitig wird der Wortlaut redaktionell so gefasst, dass nicht der Eindruck entsteht, allein das BfV sei zur Gewährleistung der Sicherheit der Datenverarbeitung verpflichtet (bisher: … trifft „die“ Maßnahmen), da einzelne Pflichten – wie die Speicherkontrolle – ebenso die verbundbeteiligten Stellen für ihren Bereich betreffen. Die Weiterverarbeitungsregelung (Zweckbindung, Löschungsfrist) erfolgt nunmehr zu Protokolldaten querschnittlich vereinheitlicht in § 36 und § 38.

Zu § 7 (Weisungsrechte des Bundes)

Die Regelung übernimmt den bisherigen Paragraphen, räumt aber nunmehr das Weisungsrecht dem Bundesministerium des Innern ein. Die bisher vorgesehene Kollegialentscheidung der Bundesregierung ist nicht geboten und dem geregelten Sachverhalt - eines bereits erfolgenden Angriffs mit unter Umständen raschem Handlungsbedarf - auch nicht angemessen. Insoweit wird die ursprüngliche Zuständigkeit der - dort sachlich sogar breiter gefassten - Weisungskompetenz des Bundes in § 5 Absatz 2 BVerfSchG 1950 (BGBl. I S. 682) wiederhergestellt.

Zu Abschnitt 2 (Aufklärung)

Der Abschnitt enthält Befugnisse zu Eingriffen unterschiedlicher Intensität. Bei qualifizierten Eingriffen erfolgt eine abstufende Kategorisierung in erhebliche bzw. sogar besonders erhebliche Eingriffe. Die Maßnahme-Klassifizierung folgt der in der Verfassungsrechtsprechung vorgezeichneten Abstufung (BVerfGE 141, 220 – Rn. 107 f.), wonach etwa die Erhebung von Telekommunikationsverkehrsdaten, der Einsatz von Vertrauensleuten oder längerfristige Observationen qualifiziert eingriffsgewichtig sind (erheblich eingreifend) und die Telekommunikationsinhaltsüberwachung nochmals gewichtiger (besonders erheblich eingreifend) ist. Diese Klassifizierung des Eingriffsgewichts dient der Verknüpfung mit der komplementären Abstufung der Eingriffsrechtfertigung durch abgestufte Beobachtungsbedürftigkeit (§ 3 Absatz 6 und 7). Die noch gewichtiger eingreifenden Maßnahmen der Online-Überwachung und Wohnraumüberwachung haben in dem System eine Sonderstellung, weshalb dazu keine allgemeine Gewichtungsklassen gebildet, sondern die Voraussetzungen jeweils speziell in der besonderen Befugnisnorm geregelt werden.

Zu Unterabschnitt 1 (Allgemeine Informationsgewinnung, Mitwirkungspflichten)

Der Unterabschnitt regelt den Lebenssachverhalt der Informationsgewinnung. Der erschöpft sich nicht in Maßnahmen des BfV, speziell Übermittlungsersuchen, sondern schließt die Übermittlung anderer Stellen an das BfV für dessen Aufgaben ein.

Zu § 8 (Allgemeine Datenerhebung)

Die Regelung entspricht weitgehend den Erhebungsbestimmungen des bisherigen § 8. Regelungsbedarf besteht grundsätzlich nur zu personenbezogene Daten, da zur Verarbeitung sonstiger Informationen keine Befugnis benötigt wird. Gleichwohl bleibt die Regelung auch auf sonstige Informationen erstreckt, da andere Regelungen des Unterabschnitts auch komplementäre Übermittlungspflichten begründen und diese auch Sachinformationen einschließen sollen. Eine differenzierende Regelung könnte zu unnötigen Umkehrschlüssen führen, wonach § 8 fälschlich als Erhebungsverbot zu Sachinformationen interpretiert werden würde. Die Weiterverarbeitung wird nunmehr systematisch gesondert in Unterabschnitt 4 geregelt.

Zu Absatz 1

Satz 1 entspricht der bisherigen Erhebungsregelung in § 8 Absatz 1 Satz 1. Die Einwilligungsregelung des bisherigen letzten Halbsatzes erfolgt, da auch künftig auf die Datenverarbeitung in allen Phasen bezogen, in den allgemeinen Datenschutzregelungen (§ 68 Nummer 2). Entgegenstehende besondere Regelungen sind nicht nur Gegennormen, die Datenerhebung speziell ausschließen, sondern ebenso spezialgesetzliche Befugnisregelungen, die die Erhebungsvoraussetzungen besonders regeln und damit der allgemeinen Befugnis vorgehen. Auf den bisherigen speziellen Bezug auf Regelungen des Bundesdatenschutzgesetzes kann verzichtet werden, da nach § 69 anwendbare Vorschriften einer Erhebung nach § 8 Absatz 1 Satz 1 nicht entgegenstehen.

Satz 2 trifft eine neue Schwellenregelung für qualifizierte Fälle personenbezogener Informationssammlung. Das Einzelfallerfordernis bringt zum Ausdruck, dass die Informationssammlung konkret veranlasst ist, also nicht lediglich auf Vorrat ins Blaue erfolgt. Damit ist beispielsweise die Voraussetzung bei Personen per se erfüllt, zu denen den Fallumständen nach ihre Beteiligung an Bedrohungen zu prüfen ist oder zu denen bereits Anhaltspunkte für eine Beteiligung vorliegen, so dass hieraus veranlasst ist, die vorliegenden Erkenntnisse für die Bedrohungsaufklärung durch dazu geeignete Maßnahmen um weitere relevante Informationen bzw. Spurenansätze anzureichern. Bürokratielasten, etwa zusätzliche Dokumentationserfordernisse, sind mit der Regelung nicht verbunden. Die Einzelfallveranlassung erschließt sich regelmäßig ohne weiteres aus dem Bearbeitungszusammenhang.

Die Datenerhebung bezieht sich aus allgemein zugänglichen Quellen (eine Erhebung bei Dritten ist in § 9 geregelt und dort insgesamt an die Schwelle der Einzelfallerforderlichkeit gebunden). In der Kenntnisnahme öffentlich zugänglicher Informationen, etwa dem Aufruf einer allgemein zugänglichen Webseite im World Wide Web, liegt zwar grundsätzlich kein Grundrechtseingriff (BVerfGE 120, 274 – Rn. 308). Anders verhält es sich, wenn Informationen gezielt zusammengetragen werden (a.a.O. Rn. 309). Insofern ist eine Befugnis erforderlich, die allerdings lediglich dem einfachen Eingriffsgehalt Rechnung tragen muss, also keine qualifizierten Voraussetzungen erfordert. Die Nummern erfassen im Vorgehen (systematisch) oder dem Mittel (Biometrie) qualifizierte Sachverhalte, so dass die Befugnis hierzu nicht allein final (auf die herausragenden öffentlichen Interessen der Verfassungsschutzaufgabe), sondern auch situativ (im Einzelfall veranlasst) eingegrenzt wird.

Zu Nummer 1

Die Nummer regelt den Sachverhalt, dass Daten systematisch zusammengeführt werden sollen, was auf einen gegenüber punktuellen Erhebungen gewichtigeren Eingriff zielt. Für das Eingriffsgewicht maßgebend ist die personengerichtete Zusammenführung. Eine Sammlung, die nicht auf eine Zielperson bezogen ist (sondern z.B. Massendaten nach Mustern oder Trends auswertet), fällt nicht hierunter.

Zu Nummer 2

Nach gegenwärtigem Nutzungsverhalten von internetbasierten digitalen Diensten dienen bildbasierte Informationen spezifisch auch der Erfassung von Situationen der Privatheit. Dies ist nicht auf die Person beschränkt, die ein Bild ins Internet einstellt, sondern schließt weitere abgebildete Personen ein. Im Vergleich mit einer alphanumerischen Recherche können biometrisch basierte Suchen daher womöglich mit größerer situativer Streubreite auch Privatheit erschließen. Deshalb werden sie an eine besondere Erhebungsschwelle gebunden.

Ein weiterer Anwendungsfall ist die biometrische Echtzeit-Auswertung einer Videoüberwachung, um einen automatisierten Hinweis zu erhalten, wenn Zielpersonen an überwachten Örtlichkeiten erscheinen.

Der Abgleich erfolgt mit biometrischen Daten, die das BfV selbst gespeichert hat oder die im Nachrichtendienstlichen Informationssystem mit Zugriffsrecht des BfV nach § 6 Absatz 2 von Landesverfassungsschutzbehörden gespeichert sind. Die Regelung enthält keine Befugnis zu einer Vorratsdatenspeicherung für Zwecke des biometrischen Abgleichs.

Zu Absatz 2

Der Absatz trifft Ergänzungsregelungen zum biometrischen Abgleich nach Absatz 1. Nach Satz 1 ist die Nutzung von Diensten außerhalb der EU subsidiär gegenüber der Nutzung eines Dienstes in der EU, wenn mit diesem das Erkenntnisziel gleichermaßen erreicht werden kann (Abstriche an der Aufklärungsqualität müssen somit nicht in Kauf genommen werden). Satz 2 regelt eine spezielle Löschungspflicht zu unnötigen Daten. Da solche Erhebungen als sensibel angesehen werden, trifft Satz 3 eine besondere Kontrollvorkehrung.

Zu Absatz 3

Die Regelung entspricht dem bisherigen § 8 Absatz 4.

Zu Absatz 4

Der Absatz greift den bisherigen § 8 Absatz 5 auf.

Zu § 9 (Datenerhebung bei Dritten)

Der Begriff des Dritten folgt der Definition in Artikel 4 Nummer 10 der Datenschutz-Grundverordnung (EU), umfasst also jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten. Die Regelung trifft mithin allgemeine Vorgaben für die Datenerhebung sowohl bei öffentlichen wie auch nicht-öffentlichen Stellen. Speziell zu öffentlichen Stellen enthält § 10 besondere ergänzende Regelungen, die die Anwendung des allgemeinen § 9 aber nicht insgesamt verdrängen. Insbesondere die Verschwiegenheitspflicht des Absatzes 3 zu BfV-Ersuchen ist auch von öffentlichen Stellen zu beachten und beschränkt beispielsweise auch das Auskunftsrechts des Betroffenen gegenüber solcher ersuchten Stelle.

Zu Absatz 1

Für den Bereich der öffentlichen Stellen entspricht die Regelung in Satz 1 dem bisherigen § 18 Absatz 3 Satz 1. Die Formulierung folgt mit dem Erfordernis der Einzelfallerforderlichkeit neuerer Praxis (vgl. etwa bisherigen § 8d), die eine anlasslose, nur final angeleitete und begrenzte Erhebung „ins Blaue“ bzw. „auf Vorrat“ ausschließt (vgl. BVerfGE 155,119 – Rn. 218, ferner 145, 155, 228, 232). Nicht verschlossen wird hierdurch, Ersuchen anlassbezogen auch als Dauerersuchen oder für bestimmte Anlässe generell formuliert zu stellen.

Das Erfordernis der Erforderlichkeit zur Aufklärung schließt im Übrigen nicht nur Informationen über die Bedrohungen selbst ein, sondern beispielsweise auch über die der Aufklärung dienenden Informationszugänge und –mittel, etwa bei der Überprüfung der Nachrichtenehrlichkeit einer Quelle.

Der Anwendungsbereich der Regelung ist die Aufklärung von Bedrohungen nach § 3 Absatz 4. Sicherheitsermittlungen im Rahmen der Mitwirkungsaufgaben nach § 2 Absatz 5 sind im Falle der Nummer 1 im jeweiligen besonderen Gesetz geregelt (speziell § 12 SÜG) und im Fall der Nummer 2 in der Aufgabennorm selbst begrenzt und insoweit mit der Befugnis nach § 8 Absatz 1 durchführbar.

Sätze 2 und 3 übernehmen den bisherigen § 8 Absatz 1 Sätze 2 und 3. Die Übermittlung der für das Ersuchen notwendigen Angaben ist zur wirksamen Gestaltung der Beschaffungsbefugnis deren Inhalt und nicht etwa zusätzlich an Übermittlungsvoraussetzungen nach dem 3. Abschnitt zu messen.

Zu Absatz 2

Satz 2 gestaltet die Befugnis zur Vollregelung der Beschaffung, die im Interesse der Normenklarheit komplementär zur Erhebung zugleich die Übermittlungszulässigkeit regelt. Soweit besondere gesetzliche Übermittlungsschranken bestehen, gehen diese jedoch vor. Besonderen Regelungen sind Vorschriften, die speziell die Übermittlung an Verfassungsschutzbehörden regeln (z.B. § 5 Absatz 5 Nummer 2 und 6 Satz 1 Nummer 3 BSIG) oder eine gerade abschließende Regelung (auch gegenüber Verfassungsschutzbehörden) treffen, indem allgemeine verfassungsrechtliche Vorgaben der Weiterverarbeitung fachrechtlich abweichungsfest umgesetzt werden (z.B. § 12 Absatz 3 BKAG). Dazu zählen auch berufliche Verschwiegenheitspflichten, die auch gegenüber Sicherheitsbehörden gelten (z.B. § 43a Absatz 2 BRAO, auch in Verbindung mit § 30).

Angesichts der die Übermittlung einschließenden Vollregelung beschränkt sich die Prüfungsverantwortung der ersuchten Stelle ebenso auf solche gesetzliche Übermittlungsregelungen ihres Fachrechts, die in der vorstehend beschriebenen Weise der Übermittlung entgegenstehen. Ist die Übermittlung von einem Ersuchen veranlasst, trägt die ersuchende öffentliche Stelle allgemein die grundsätzliche Verantwortung für die Zulässigkeit der Übermittlung, die ersuchte Stelle prüft nur, dass im Ersuchen auf die Verfassungsschutzaufgabe Bezug genommen ist (ohne nähere Spezifizierung, die regelmäßig unter Geheimschutzerwägungen auch ausscheidet) und im Übrigen solche besonderen Rechtsvorschriften ihres Fachrechts, die ausnahmsweise der bereichsspezifischen Übermittlungsregelung des Absatzes 2 aus den dargestellten Gründen noch vorgehen (vgl. § 15 Absatz 2 Satz 2 und 3 BDSG 1990).

Das bisherige Dokumentationserfordernis nach § 18 Absatz 5 zu Übermittlungsersuchen an Behörden wird nicht aufgegriffen. Das Gesetz bezweckt auch Bürokratieentlastung, um dafür gebundene Ressourcen besser für die operative Schutzaufgabe des BfV einzusetzen. Eine generelle Dokumentationspflicht ist nicht geboten (vgl. BVerfGE 155, 119 - Rn. 250). Dass wesentliche Vorgänge aktenkundig zu machen sind, ergibt sich allgemein aus dem rechtsstaatlichen Grundsatz der Aktenmäßigkeit der Verwaltung, ohne dass dies einer fachgesesetzlichen Bekräftigung bedürfte. Dies gilt gleichermaßen für das Verwaltungshandeln nach dem Bundesverfassungsschutzgesetz. Festgehalten wird hingegen an der speziellen Regelung von Dokumentationspflichten bei besonderen Fällen in den dies betreffenden Spezialregelungen.

Zu Absatz 3

Der Absatz übernimmt bisher speziell in § 8b Absatz 5 zu Unternehmensauskünften enthaltene Pflichten in die allgemeine Erhebungsregelung, da sie sachgerecht allgemein gelten sollten (vgl. bereits die allgemeine Regelung in § 57 Absatz 5 BDSG). Es liegt im pflichtgemäßen Ermessen des BfV, den Dritten ggf. auch auf die Pflicht hinzuweisen. Dies ist nicht

durchgängig situationsgerecht, weshalb insoweit keine allgemeine gesetzliche Regelung erfolgt. Speziell zu Unternehmensauskünften sieht der neue § 12 Absatz 4 Satz 4 einen solchen Hinweis jedoch für Ersuchen in Textform allgemein vor.

Zu Nummer 1

Nummer 1 übernimmt die bisherige Regelung aus § 8b Absatz 4 Satz 2 und wahrt die grundsätzlich gebotene Vertraulichkeit von Ermittlungen des BfV allgemein. Die Regelung geht als lex specialis allgemeinen Mitteilungsregelungen wie etwa § 111 Absatz 2 Satz 3 BBG vor. Der letzte Halbsatz verdeutlicht, dass dies auch gegenüber Verdachtsmeldepflichten an Behörden gilt. Ersucht das BfV beispielsweise eine Bank um Finanzauskünfte, ist dieses Ersuchen also keine Tatsache, die die Bank zu einer Verdachtsmeldung nach § 43 GwG veranlassen würde. Die Informationsflüsse im öffentlichen Bereich erfolgen sachgerechter zwischen den betroffenen öffentlichen Stellen nach dem dafür maßgeblichen Recht.

Zu Nummer 2

Die Nummer übernimmt verallgemeinernd das bisher speziell zu Unternehmensauskünften getroffene Nachteilsverbot des bisherigen § 8b Absatz 5 Satz 1.

Zu § 10 (Übermittlung durch inländische öffentliche Stellen)

Die Regelung knüpft an die bisherigen Bestimmungen in § 18 Absatz 1 bis 4 für Übermittlungen an das BfV in systematischer Neugliederung an und integriert dabei zugleich die besonderen Dauerersuchen nach dem bisherigen § 17 Absatz 2 und 3. Die Anwendbarkeit auf Landesverfassungsschutzbehörden ist nunmehr querschnittlich in § 75 geregelt. Nach Satz 2 ist die Übermittlungspflicht für Landesbehörden gegenüber dem BfV subsidiär gegenüber Übermittlungspflichten an die Verfassungsschutzbehörde des Landes, die sich landesrechtlich bestimmt.

Zu Absatz 1

Der Absatz entspricht den bisherigen § 18 Absatz 3 Satz 1 und Absatz 3a. Satz 1 verstärkt die allgemeine Befugnis des § 9 Absatz 1 dabei zur Pflicht. Entgegenstehende Übermittlungsregelungen sind spezielle fachgesetzliche Regelungen zur Übermittlung an Verfassungsschutzbehörden oder Regelungen, die allgemeine Verfassungsvorgaben – auch für Übermittlungen an Verfassungsschutzbehörden – umsetzen, etwa zur Weiterverarbeitung von Informationen aus einer Online-Überwachung oder Wohnraumüberwachung (vgl. BVerfGE 141, 220 – Rn. 283).

Das Steuergeheimnis nach § 30 AO ist gemäß dessen Absatz 4 Nummer 5 Buchstabe a generell keine entgegenstehende Sondervorschrift, da die dem Ersuchen zugrunde liegende Bedrohung generell das zwingende öffentliche Übermittlungsinteresse zur Abwehr erheblicher Nachteile für das Gemeinwohl begründet. Dies verdeutlicht nunmehr im neuen § 10 allgemein auch der neue Absatz 4 Nummer 5, so dass es sich erübrigt, die spezielle Regelung des bisherigen § 18 Absatz 3a fortzuführen.

Der ausdrückliche Einbezug von Personaldaten in Satz 1 stellt klar, dass die Übermittlungsregelung alle vorliegenden Daten einschließt, also nicht nur die aus der operativen Verwaltungsaufgabe, sondern ebenso aus der Binnenverwaltung der Behörde. Hierbei können gerade Personaldaten von Bedeutung sein, insbesondere weil es besonders wichtig ist, Extremisten kein Wirkungsfeld im öffentlichen Dienst unter Nutzung staatlicher Ressourcen zu eröffnen. Die Regelung stellt damit zugleich den speziellen Anwendungsvorrang der besonderen Regelung für Übermittlungen an das BfV gegenüber allgemeinen Vorschriften des Personaldatenschutzes klar, was das Mitteilungsverbot nach § 9 Absatz 3 einschließt. Für Spontanübermittlungen von Landesbehörden gilt nach Absatz 4 Satz 3 der Vorrang der Übermittlung an die Landesverfassungsschutzbehörde.

Die Durchführung der Übermittlung – etwa durch Aktenübersendung oder Gewährung von Akteneinsicht – wird gesetzlich nicht näher geregelt, sondern bleibt angemessener Ausgestaltung im Verwaltungsvollzug unter Beachtung von Wirtschaftlichkeitserfordernissen überlassen.

Zu Nummer 1

Zur Beantwortung eines Ersuchens darf die ersuchte Stelle neben den ihr bereits bekannten Daten nach Nummer 1 auch Daten aus allgemein zugänglicher Quellen nutzen. Dies entspricht dem bisherigen § 17 Absatz 1. Der eigentliche Sinn der Regelung liegt darin, dass das Ersuchen keine weitergehenden Ermittlungen der ersuchten Stelle für das BfV anstoßen soll und dazu auch keine Datenverarbeitungsbefugnis schafft. Dies ergibt sich allerdings bereits allgemein aus dem Vorbehalt des Gesetzes. Hiervon zu unterscheiden ist, wenn die ersuchte Stelle für eigene Aufgaben Datenerhebungen vornimmt und die Erkenntnisse auf Ersuchen auch übermittelt.

Zu Nummer 2

Nummer 2 stellt klar, dass die Übermittlungspflicht in geeigneten Fällen technisch auch durch Einrichtung eines Abrufverfahrens umgesetzt werden kann. Eine Parallelregelung für die umgekehrte Übermittlungsrichtung enthält § 58 Absatz 3. Geeignet sind insbesondere solche Sachverhalte, in denen die Übermittlung unter Abfrage eines Dateisystems erfolgt und im Einzelfall keine entgegenstehenden Übermittlungsregelungen zu prüfen sind (weil sie vorliegend nicht bestehen, oder ihre Beachtung im Wege der technischen oder organisatorischen Beschränkung von Zugriffsrechten zu gewährleisten ist). In diesem Fall kann das automatisierte Abrufverfahren unter Umständen die wirtschaftlichere Variante gegenüber händischer Bearbeitung sein (die hier keine inhaltliche Funktion hat) und den Zusatznutzen bieten, Bearbeitungsfehler zu vermeiden und Informationen verzögerungsfrei auch außerhalb der Bürostunden der ersuchten Behörde verfügbar zu machen, zudem datenschutzfreundlich ohne menschliche Kenntnisnahme der Abfrage (die ansonsten möglicherweise als bemakelnd interpretiert würde und informelle negative Effekte für den Betroffenen bei der Sachbearbeitung in der angefragten Stelle haben könnte). Die nähere Organisation, speziell die Abrufdokumentation (zur wirksamen Datenschutzkontrolle und im Interesse gesicherten Geheimschutzes vorzugsweise beim BfV) bleibt den beteiligten Stellen überlassen.

Zu Absatz 2

Der Absatz übernimmt die entsprechenden Regelungen aus dem bisherigen § 18 Absatz 4 und 5.

Zu Absatz 3

Absatz 3 regelt Ausschreibungen, die im nationalen Recht als „polizeiliche Beobachtung“ bezeichnet werden (vgl. § 47 Absatz 1 Nummer 1 BKAG) und im Unionsrecht als „verdeckte Kontrolle“ (vgl. Art. 36 f. EU (VO) 2018/1862). Der Sache nach handelt es sich um Ersuchen, beim Antreffen der Personen bestimmte dabei angefallene Erkenntnisse mitzuteilen. Da sie ausschließlich öffentliche Stellen betrifft, erfolgt die Regelung in § 10. Sie greift die Bestimmungen des bisherigen § 17 Absatz 2 und 3 auf, wobei Erkenntnisziel gemäß dem Aufklärungsbedarf nicht allein grenzüberschreitende Bewegungen sind. Datenschutzfreundlich erfolgt in Satz 1 Nummer 1 und 2 eine spezielle gesetzliche Regelung zu dem Personenkreis, zu dem Ausschreibungen möglich sind. Obgleich die Maßnahme weniger gewichtig eingreifend ist (BVerfGE 165, 1 –– Rn. 174), erfolgt für nationale Ausschreibungen eine Schwellenanhebung gegenüber dem bisherigen § 17 Absatz 2, indem künftig erheblich beobachtungsbedürftige Bedrohungen vorausgesetzt werden. Für Ausschreibungen in EU-Systemen sind die unionsrechtlichen Voraussetzungen maßgeblich. Die EU besitzt zwar keine Regelungskompetenz zum Bereich der nationalen Sicherheit ihrer Mitgliedstaaten (Artikel 4 Absatz 2 Satz 3 EUV, BVerfG, Beschluss vom 8. Oktober 2024 - 1 BvR 1743/16,

1 BvR 2539/16 [BND – Cybergefahren] - Rn. 77 ff.). Sie regelt jedoch die Zwecksetzung ihrer Einrichtungen. Im Rahmen der nationalen Sicherheit bestimmen die Mitgliedstaaten autonom, diese im Rahmen des EU-rechtlich erlaubten Zwecks auch für nachrichtendienstliche Ausschreibungen zu nutzen. Die in Artikel 36 Absatz 4 EU (VO) 2018/1862 vorausgesetzte nationalrechtliche Erlaubnis enthält dieser Absatz. Dabei sind gemäß Satz 1 in jedem Fall erheblich beobachtungsbedürftige Bedrohungen vorausgesetzt. Das Unionsrecht greift im Ergebnis nur, wo es enger ist, weil dann der nationale Gesetzgeber nicht darüber hinaus gehen kann, insoweit dann aber die Entscheidung trifft, den unionsrechtlichen Rahmen auszuschöpfen.

Zu Absatz 4

Die Spontanübermittlungsregelung greift die Regelungen der bisherigen § 18 Absätze 1 bis 2 auf. Sie unterscheidet künftig zwischen einer Befugnis, die phänomenunabhängig besteht, und einer Verpflichtung, die nur für bestimmte Stellen phänomenunabhängig besteht, im Übrigen aber allgemein auf Phänomene beschränkt ist, die auch für fachunkundige Stellen als verfassungsschutzrelevant erkennbar sind.

Neben den hier querschnittlich behördenbezogen getroffenen Regelungen bestehen auch bereichsspezifisch gestaltete Spontanübermittlungspflichten in Fachgesetzen (wie etwa § 32 Absatz 3 Satz 1 GwG), die auch weiterhin daneben anzuwenden bleiben.

Unberührt von der gesetzlichen Spontanübermittlungspflicht bleibt die Übermittlungspflicht auf Ersuchen nach § 9 Absatz 1 in Verbindung mit § 10 Absatz 1. Hiervon zu unterscheiden sind unterstützende Materialien, die den nach Absatz 2 übermittlungspflichtigen Stellen erläutern, woran sie einen Sachverhalt erkennen, den die Stelle nach Absatz 4 Satz 2 übermitteln muss.

Zu Nummer 1

Die Regelung des bisherigen § 18 Absatz 2 wird zur Übermittlungspflicht verstärkt. Dies korrespondiert dem bisherigen § 22 Absatz 2, der nunmehr in § 49 Absatz 2 übernommen ist, und trägt dem Erfordernis eines engen Informationsaustauschs beim Schutz der besonders gewichtigen Rechtsgüter bei, denen die nachrichtendienstlichen Aufgaben dienen.

Zu Nummer 2

Das BSI ist neu aufgenommen, da auch insoweit eine besonders enge Kooperation der Sicherheitsbehörden mit breiten Aufgabenberührungen nötig ist.

Zu Nummer 3

In Nummer 3 sind gegenüber dem bisherigen § 18 Absatz 1b Justizvollzugsbehörden ergänzt. Speziell mit Justizvollzugsanstalten ist eine enge Kooperation nötig, etwa hinsichtlich der Haftentlassung inhaftierter Extremisten oder auch Radikalisierungsentwicklungen bei Gefangenen.

Zu Nummer 4

Die Regelung entspricht dem bisherigen § 18 Absatz 1a.

Zu Nummer 5

Die Regelung greift § 51 Absatz 3 Satz 3 AO auf. Bei den anlassgebenden Bedrohungssachverhalten besteht generell zur Abwehr erheblicher Nachteile für das Gemeinwohl ein zwingendes öffentliches Interesse an der Übermittlung. Angesichts der neuen allgemeinen Regelung erübrigt sich auch, die Sonderreglung des bisherigen § 18 Absatz 3a

fortzuschreiben. Mit der Übernahme der Regelung der Abgabenordnung ist der Begriff der Finanzbehörde im Sinne von § 6 Absatz 2 AO zu verstehen.

Zu Nummer 6

Die Regelung entspricht dem bisherigen § 18 Absatz 1. Der neuen Systematik würde grundsätzlich entsprechen, wertungskonsistent allgemein auf erheblich beobachtungsbedürftige Bedrohungen abzustellen anstelle der bisher selektiven Ausrichtung bei Bestrebungen auf Gewalt. Solche Verbreiterung ist für fachfremde Behörden in der Sachverhaltswürdigung allerdings nur begrenzt praktikabel. Deshalb bleibt eine Begrenzung auf Phänomene, die auch für fachfremde Behörden als verfassungsschutzrelevant einordenbar sind erhalten. Diese Erkennbarkeit geht aber über den bisherigen Gewaltbezug hinaus und muss auch volksverhetzende Bestrebungen einbeziehen. Ebenso erkennbar ist die Straftatenbegehung, die aber vorrangig zu einer Mitteilung an Strafverfolgungsbehörden führen sollte. Die Übermittlungsbefugnis nach Satz 1 besteht aber auch hierzu, so dass es im Ermessen der öffentlichen Stelle bleibt, die Information zugleich auch oder womöglich alternativ dem BfV zu übermitteln.

Zu Absatz 5

Die Regelung weist auf zu beachtende Zweckbindungen – z.B. nach § 25 Absatz 6 BKAG – hin. Für Informationen, die durch Online-Überwachung oder Wohnraumüberwachung gewonnen worden sind, erfolgt mit Satz 2 zur Weiterverabeitung die Gleichstellung mit Informationen, die das BfV selbst mit solchen Maßnahmen gewonnen hat. Damit wird der Rechtsprechung des Bundesverfassungsgerichts zum von ihm so genannten Prinzip der hypothetischen Datenneuerhebung Rechnung getragen, die eine zweckändernde Datenweiterverarbeitung so gewonnener Informationen nicht nur an zweckbezogene Voraussetzungen knüpft (die mit den Verfassungsschutzaufgaben immer erfüllt sind), sondern zudem besondere Schwellenanforderungen stellt (BVerfGE 141, 220 – Rn. 291).

Zu Absatz 6

Die Regelung greift Vorgaben des bisherigen § 18 Absatz 1a auf. Dessen Satz 3 wird bedarfsgerecht angepasst. Der überragende Anteil des Auslandsverkehrs des Bundesamtes für Verfassungsschutz vollzieht sich mit Partnerländern zu deren Einschätzung der Einbezug des BAMF keinen Mehrwert bietet. Wenn das BfV beispielsweise Informationen zu einem Marokkaner an den französischen Partnerdienst übermittelt, kann das BAMF nicht mit besonderer Fachkunde zur Würdigung von Betroffenenbelangen am Maßstab von § 55 beitragen. Bereits die geltende Regelung soll besonderer Fachkunde des BAMF bei etwaigen (fernliegenden) Übermittlungen an den Herkunftsstaat Rechnung tragen. Dies kommt nunmehr in der Regelung auch zum Ausdruck.

Zu Absatz 7

Die Regelung trägt Schutzbelangen der benannten Behörden Rechnung, Der Schutz überwiegender Sicherheitsinteressen in der nachrichtendienstlichen Zusammenarbeit mit dem BND (Nummer 1) entspricht dem spiegelbildlichen Übermittlungsausschluss des BfV in § 52 Absatz 1 Nummer 2. Operative Maßnahmen im Sinne der Nummer 2 sind nicht auf Ermittlungsmaßnahmen beschränkt, sondern beziehen auch Maßnahmen beispielsweise des Zeugenschutzes ein.

Soweit die Übermittlungspflicht entfällt, verbleibt es im Ermessen der jeweiligen Stelle, ob sie von der Übermittlungsbefugnis in Absatz 4 Satz 1 (Spontanübermittlung) bzw. § 9 Absatz 2 (Übermittlung auf Ersuchen) Gebrauch macht, wobei naturgemäß die Gründe des Pflichtenausschlusses auch besonders bei der Ermessensausübung zu berücksichtigen sind.

Die speziellen Pflichtenschranken des Absatz 7 gelten unabhängig von besonderen Regelungen in den Fachgesetzen der übermittlungspflichtigen Stellen. Daneben sind bereits nach Absatz 1 Satz 1 entgegenstehende Regelungen dieser Fachgesetze verpflichtungsbeschränkend zu beachten.

Zu Nummer 1

[…]

Zu Nummer 2

[…]

Zu § 11 (Verpflichtende Ersuchen an geschäftsmäßige Diensteanbieter)

Mit dem neuen § 11 werden bisher in §§ 8a, 8b und § 8d enthaltene Vorgaben zu Unternehmensauskünften zusammengeführt und in das neue Schwellensystem der Verfassungsrechtsprechung eingefügt. Ergänzende bereichsspezifische Vorschriften zu besonderen Diensten werden der Übersichtlichkeit halber in §§ 12, 13 und 14 aufgeführt. Die unabhängige Anordnungskontrolle ist künftig in § 34 geregelt. Sie bleibt für Eingriffe in das Post- und Fernmeldegeheimnis (§ 14 i.V.m. § 12 Absatz 3, § 22) beibehalten. Die sonstigen Auskunftspflichten erschließen zwar teils breite Informationen, ohne dass jedoch zur Informationstiefe auch mit höchstprivaten Informationen zu rechnen wäre, so dass insoweit die Vorabprüfung nicht geboten ist (BVerfGE 162 1, - Rn. 214, 217; speziell zu Finanzauskünften BVerfGE 120, 274 - Rn. 330).

Die Pflicht bezieht sich auf die für die Geschäftszwecke vorhandenen Informationen. Weder besteht eine Pflicht zur Vorsorgespeicherung noch eine Pflicht, Informationen zur Auskunftserteilung zu beschaffen.

Auf eine spezielle gesetzliche Regelung, dass die Verpflichteten die Auskunft unverzüglich und vollständig (bisher § 8b Absatz 6) zu erteilen haben, wird im Interesse der Gesetzesverschlankung verzichtet. Öffentlich-rechtliche Pflichten sind allgemein unverzüglich und vollständig zu befolgen, so dass es hier keiner besonderen Regelung bedarf.

Wie bereits der geltende § 8a BVerfSchG bildet die Regelung im Interesse der Normenklarheit mit den korrespondierenden Bestimmungen zu Auskunftspflicht und Ersuchen eine Vollregelung (BVerfGE 130, 151 – Rn. 123) zum Lebensvorgang der Informationsbeschaffung und ist dadurch zugleich für Ersuchen des BfV lex specialis beispielsweise gegenüber dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz, so dass sich dort verortete Abgrenzungsfragen zwischen Nutzungs- und Inhaltsdaten (siehe noch Erläuterung zu Absatz 3) hier nicht stellen.

Zu Absatz 1

Die Regelung ergänzt die Erhebungsbefugnis nach § 9 um eine komplementäre Verpflichtung bestimmter Unternehmen. Der Lebensvorgang der Informationsbeschaffung unterliegt zusätzlich also den Voraussetzungen nach § 9 sowie den ergänzenden Anforderungen nach den Absätzen 2 bis 4. Da diese Voraussetzungen jedoch ausschließlich in der Verantwortung des BfV liegen, werden sie in Absatz 1 nicht wiederholt. Für die Unternehmen besteht Rechtssicherheit, dass sie auf Ersuchen übermitteln. Die Ersuchensvoraussetzungen sind allein vom BfV zu prüfen (so bereits der allgemeine Grundsatz in § 9 Absatz 2.

Satz 2 begrenzt die Auskunft auf die benannten Datenkategorien. Bestandsdaten werden dabei im Näheren mit Absatz 2 Satz 2 definiert. Satz 2 und 3 stellen zudem klar, dass eine Vorratsdatenspeicherung ins Blaue nicht erfolgt. Unbeschadet dessen bleiben konkret veranlasste Ersuchen weiterhin auch zukunftsgerichtet zulässig (Absatz 4 Satz 1).

In Satz 4 knüpft die Verpflichtung zur Übermittlung der verlangten Daten wie in der Vorgängerregelung nach dem Marktortprinzip an. Zwischenzeitlich ist dies auch in § 1 Absatz 2 TKG und § 1 Absatz 3 TDDDG verankert.

Zu Nummer 1

Zu Buchstabe a

Mit Buchstabe a werden gegenüber dem bisherigen § 8a Absatz 1 Nummer 1 (Luftverkehr) nunmehr allgemein entgeltliche oder geschäftsmäßige Anbieter von Leistungen zum Transport von Personen (Personenverkehr) oder Gütern (Güterverkehr) erfasst. Hierzu zählen insbesondere Eisenbahnverkehrsunternehmen im Sinne des § 2 Absatz 3 des Allgemeinen Eisenbahngesetzes, Unternehmen für den Linienverkehr mit Kraftomnibussen im Sinne des § 42a Satz 1 des Personenbeförderungsgesetzes sowie Unternehmen, die entgeltlich oder geschäftsmäßig Mittel für den öffentlichen Personenverkehr bereitstellen wie gewerbliche Anbieter von Mietfahrzeugen für Selbstfahrer im Sinne des § 6 Absatz 1 Nummer 12 des Straßenverkehrsgesetzes und Carsharing-Anbieter im Sinne des § 2 Nummer 2 des Gesetzes zur Bevorrechtigung des Carsharing sowie Güterkraftverkehrsunternehmen (§ 1 Absatz 1 GüKG). Mit der Regelung wird der gestiegenen und perspektivisch weiterwachsenden Bedeutung von Verkehrsträgern alternativ zum Flugverkehr Rechnung getragen. Zudem wird nunmehr auch der Güterverkehr einbezogen, der speziell bei Proliferationssachverhalten bedeutsam sein kann.

Zur Auskunft sind auch diejenigen Dienstleister verpflichtet, die geschäftsmäßig an der Leistungserbringung mitwirken. Für die in Buchstabe a eingeschlossenen Luftverkehrsauskünfte folgt damit, dass auch Betreiber von Computerreservierungssystemen und globalen Distributionssystemen weiterhin verpflichtet werden können (entsprechend der bisherigen Aufzählung im bisherigen § 8a Absatz 1 Nummer 1), ohne dass dies insoweit einer weiteren speziellen Regelung bedarf.

Zu Buchstabe b

Die Regelung entspricht dem bisherigen § 8a Absatz 1 Satz 1 Nummer 5, wobei der Bezug auf Digitale Dienste dem aktuellen Fachrecht folgt, speziell des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz.

Zu Buchstabe c

Hiernach werden technische Dienstleister einbezogen, die zwar zur Erbringung von Zahlungsdiensten beitragen, gleichwohl nach § 2 Absatz 1 Nummer 9 des Zahlungsdiensteaufsichtsgesetzes nicht als Zahlungsdienste gelten, somit nicht zum Verpflichtetenkreis nach Nummer 2 (der Zahlungsdienste umfasst) zählen. Nummer 2 belässt insoweit eine Lücke insbesondere zu Betreibern von Zahlungsverkehrssystemen wie den Kreditkartenunternehmen Mastercard und VISA. Die Auskunftseinholung bei diesen Unternehmen ist jedoch zur Gewinnung relevanter Finanzinformationen insbesondere in den Fällen bedeutsam, in denen die kartenausgebende Bank ihren Sitz in einem Land hat, dessen Tätigkeiten nach § 2 Absatz 1 Nummer 3 womöglich gerade aufklärungsbedürftig sind, so dass die Anfrage an die Bank aus operativen Gründen ausscheidet.

Zu Nummer 2

Einbezogen sind auch Kraftfahrzeughersteller, die telemetrische Daten erheben, sei es für aktive Fahrzeugvernetzungsdienste, die sie anbieten, sei es für eigene Auswertungszwecke. Gerade letzteres ist nicht vollständig von Nummer 1 Buchstabe b abgedeckt, da bestimmte Arten von Informationen in bestimmten Fällen beim Hersteller unabhängig von einem dem Halter verfügbaren Dienst automatisch erhoben werden, darunter Standort, Geschwindigkeit, Kilometerstand, Fahrzeugnutzungsdaten (wie z. B. Zündzyklen, Fahrprofile).

Kraftfahrzeugwerkstätten sind einbezogen, weil dort ebenso solche Daten ausgelesen werden.

Solche Telemetriedaten ermöglichen zwar keineswegs ein der Bewegungsüberwachung vergleichbar verdichtetes Standortbild. Die Übertragung von Sensordaten wie z. B. zur Sitzbelegung im Fahrzeug oder zur Füllstandsanzeige des Fahrzeugtanks (also der Reichweite bis zum nächsten Tanken) kann aber für die operative Arbeit nutzbar sein.

Zu Nummer 3

Mit Nummer 2 werden entsprechend dem bisherigen § 8a Absatz 1 Nummer 2 geschäftsmäßige Dienstleister mit Bezug zu Finanzvorgängen erfasst. Durch den neuen Verweis auf § 2 Absatz 1 Geldwäschegesetz wird der Kreis der mitwirkungspflichtigen Dienstleister mit denjenigen synchronisiert, die auch bereits zu Verdachtsmeldungen nach § 43 Abs. 1 Nr. 2 GwG verpflichtet sind. Vom Anwendungsbereich der Vorschrift ausgenommen ist, wer nach § 30 Absatz 3 Satz 3 und 4 Geldwäschegesetz zur Verweigerung einer Auskunft berechtigt ist. Entsprechendes gilt für Verpflichtete, die durch Rechtsverordnung nach § 2 Absatz 2 Geldwäschegesetz auch vom Anwendungsbereich des Geldwäschegesetzes ausgenommen sind.

Zu Absatz 2

Der Absatz übernimmt das Marktortprinzip aus dem bisherigen § 8a Absatz 4. Ergänzt wird dies mit Satz 3 um eine kollisionsrechtliche Maßgabe zur Anwendung der Verschwiegenheitspflicht in Fällen ohne Niederlassung in Deutschland.

Zu Absatz 3

Der Absatz betrifft den Auskunftsgegenstand. Dies können einerseits bloße Sachinformationen über den Dienst sein (Nummer 1) andererseits aber auch Eingriffe in die informationelle Selbstbestimmung Betroffener (Nummer 2). Für personenbezogene Daten (Nummer 2) wird zwischen bloßen Bestandsdaten (Buchstabe a) und qualifizierten Auskünften (Buchstabe b) unterschieden, da hierfür unterschiedliche Voraussetzungen gelten. Bestandsdatenauskünfte sind ohne besonderen Eingriffsgehalt, so dass hierfür die allgemeinen Voraussetzungen nach § 9 Absatz 1 adäquat sind, eine spezielle Regelung mithin verzichtbar ist. Gleiches gilt für Sachauskünfte nach Nummer 1.

Dagegen gelten für die qualifizierte Auskünfte besondere Anforderungen nach Absatz 5. Gegenständlich bezieht sich dies auch auf Inhalte von Nutzungen. Zu Finanzauskünften unterscheidet bereits das geltende Recht nicht zwischen Verkehrsdaten (wer hat an wen wann überwiesen) und Inhaltsdaten (wieviel hat er überwiesen). Auch für Teledienste ist solche Differenzierung unnötig. Angesichts der Vielfalt digitaler Dienste ist sie trennscharf ohnehin kaum möglich. Hiermit verbindet sich auch keine kategoriale Differenzierung im Eingriffsgewicht. So entstehen etwa beim Online-Kauf keine Informationen, die einem besonderen Geheimbereich, vergleichbar dem Telekommunikationsgeheimnis unterlägen. Dies unterstreicht der realweltliche Vergleich, in dem entsprechende Ermittlungen bei Verkäufern keinen erheblich qualifizierten Voraussetzungen unterliegen. Auch bei der Nutzung sozialer Medien werden, soweit die generierten Inhalte nicht ohnehin allgemein zugänglich sind, nur enge Ausschnitte von Kommunikation erschlossen, was in der Gewichtung keiner Komplettüberwachung der technisch via Telekommunikation übertragenen Kommunikation vergleichbar ist.

Zu Absatz 4

Der Absatz trifft mit Satz 1 und 3 Subsidiaritätsregelungen zur Vermeidung unnötiger Unternehmensbelastungen bzw. unnötiger Belastungsstreuung.

Satz 2 trifft für Digitale Dienste eine Parallelregelung zu der mit § 13 Absatz 2 Satz 2 für TK-Bestandsdaten getroffenen Regelung, um die dies betreffenden Verfassungsrechtsprechung gleichförmig umzusetzen. Die Regelung wird in den Folgeänderungen flankiert von einer entsprechenden Harmonisierung von § 23 TDDDG mit § 174 Absatz 4 TKG.

Zu Absatz 5

Der Absatz trifft ergänzende Sachmaßgaben für eingriffsgewichtigere Ersuchen.

Zu Nummer 1

Die Nummer knüpft solche Ersuchen an die Schwelle erheblicher Beobachtungsbedürftigkeit. Dies dient auch der Praktikabilität. Sachlich könnten einige Ersuchen auch unterhalb dieser Schwelle zugelassen werden. Das Systematisierungsziel der Reform spricht aber dafür, sich möglichst auf eine begrenzte Zahl unterschiedlicher Schwellen zu beschränken, auch um die Anwendbarkeit des Rechts zu verbessern. Praktische Bedarfe stehen dieser hier getroffenen Pauschalierung nicht entgegen.

Zu Nummer 2

Die Regelung orientiert sich an den Vorgaben zur Maßnahmerichtung im bisherigen § 8a Absatz 3 nimmt zugleich aber eine Synchronisierung mit der Maßnahmerichtung beim Einsatz nachrichtendienstlicher Mittel (§ 16 Absatz 5) vor.

Zu Buchstabe a

Der Beteiligtenbegriff erfasst objektiv fördernde Beiträge unabhängig von einem subjektiven Tatbestand. Da nach § 3 Absatz 5 Nummer 2 die Unterstützung grundsätzlich auf nachdrückliche Sachverhalte beschränkt ist, könnte allerdings zweifelhaft sein, ob die bereits bisher erfasste – ggf. einmalige – Leistungsinanspruchnahme für Beteiligte eingeschlossen ist. Dies ist deshalb ausdrücklich klargestellt.

Zu Buchstabe b

Die Regelung entspricht dem § 16 Absatz 5 Satz 1 Nummer 2, einschließlich der Subsidiarität gegenüber Nummer 1.

Zu Buchstabe c

Der Einbezug von verdeckten Hilfspersonen ist neu, korrespondiert aber dem bisherigen § 9 Absatz 1 Satz 1 Nummer 1, der die Aufklärung auch von Quellen ermöglicht (zur Prüfung ihrer Eignung, etwa der Ehrlichkeit von Angaben).

Zu Absatz 6

Absatz 6 regelt gemeinsame Anforderungen, speziell Formerfordernisse für Ersuchen sowohl nach Absatz 2 wie Absatz 3. Satz 1 enthält eine dem bisherigen § 8b Absatz 1 Satz 3 entsprechende Befristung, die mit der Bemessung auf höchstens 1 Jahr der Systematisierung in § 33 Absatz 4 Nummer 1 angepasst wird (siehe Begründung dort). Satz 2 übernimmt den bisherigen § 8b Absatz 4 Satz 1. Satz 3 übernimmt für schriftliche Ersuchen den bisherigen § 8b Absatz 5 Satz 2.

Zu Absatz 7

Die Regelung folgt der nunmehr in § 19 Absatz 6 auch in Verbindung mit § 20 Absatz 3 MAD-Gesetz gewählten Einheitslösung zur Aufwandsentschädigung mit Verweisung auf das Justizvergütungs- und -entschädigungsgesetz (ohne Beschränkung auf den Anwendungsbereich des bisherigen § 8b Absatz 9). Dies sichert angemessene Entschädigung

unter Vermeidung von sachlich nicht gebotenen Ungleichbehandlungen. Besonderheiten von Informationsanforderungen des BfV kann allerdings nach Satz 2 durch eine zusätzliche, flexiblere Vereinbarungsoption Rechnung getragen werden, um angemessenere Ergebnisse auch in Sonderfällen zu gewährleisten. Dies orientiert sich inhaltlich an der bewährten Regelung des bisherigen § 25 Absatz 5 BNDG. Damit wird ein praxisgerechter Handlungsrahmen dafür eröffnet, insbesondere nähere Absprachen zur technischen Durchführung, speziell zu Übermittlungsformaten zu treffen.

Zu § 12 (Verpflichtende Ersuchen bei informationstechnischen Angriffen)

Der Begriff der Hostingdienste ist Artikel 3 Buchstabe g iii des Gesetzes über digitale Dienste (Verordnung (EU) 2022/2065) entlehnt.

Mit der Vorschrift soll insbesondere die Aufklärung von komplexen Angriffen (sog. APT, Advanced Persistent Threats) ermöglicht werden, bei denen einzelne informationstechnische Systeme gezielt als Teil einer komplexeren Angriffsinfrastruktur eingesetzt werden. Die neue Befugnis zur Auskunftsverpflichtung ermöglicht dem BfV eine wirksamere Wahrnehmung seiner Aufklärungsaufgabe. Die Aufgabenwahrnehmung anderer Sicherheitsbehörden bleibt hiervon unberührt.

Angriffe im Sinne der Regelung sind solche, die darauf gerichtet sind, die Integrität, Authentizität, Vertraulichkeit oder Verfügbarkeit von Telekommunikations- und Datenverarbeitungssystemen zu beeinträchtigen, insbesondere mit Programmen und sonstigen informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten zu nutzen oder zu löschen oder die dem Zweck dienen, unbefugt auf sonstige informationstechnische Abläufe einzuwirken (Schadprogramme i.S.d. § 2 Absatz 5 BSIG).

§ 23 flankiert die Auskunftspflicht durch eine kongruente technische Beschaffung für Fälle, in denen der Anbieter nicht vertrauenswürdig ist.

Zu Absatz 1

Die zur Aufklärung solcher Angriffe nötige, spezielle Auskunftspflicht ist beschränkt auf Diensteanbieter, die Telekommunikationsanlagen oder sonstige informationstechnische Systeme Dritten zur Nutzung überlassen. Für einen Angriff werden auch Server genutzt, die in keinem unmittelbaren Bezug zum Angreifer stehen, insbesondere auch Einrichtungen kommerzieller Hostinganbieter. Die vorgesehene Auskunftspflicht soll in diesem Zusammenhang ermöglichen, vorrangig ohne systeminvasive Maßnahmen notwendige Informationen zur weiteren Aufklärung von Angriff und Angriffszielen zu erlangen. Die Auskunftspflicht ist auf die Übermittlung beim Betreiber vorhandener und verfügbarer technischer Informationen begrenzt. Eine Pflicht zur Speicherung wird durch die Vorschrift nicht geschaffen.

In Satz 2 werden die Auskunftspflichten mit den Hauptanwendungsfällen näher konkretisiert. Satz 3 erstreckt die Auskunftspflicht über die nach Satz 1 zu beauskunfteten technischen Informationen hinaus auch auf Beutedaten, die der Angreifer in der genutzten Angriffsstruktur im Rahmen der Angriffsverschleierung womöglich zwischengespeichert hat. Auch diese Informationen sind zur Klärung der Beschaffungsziele des Angreifers wertig.

Zu Nummer 1

Nummer 1 bezieht sich auf Auskünfte zu Verkehrs- und Steuerdaten, die vom Diensteanbieter zur Verkehrsanalyse oder Kapazitätsplanung für die eigene Qualitätssicherung verarbeitet und dokumentiert werden. „Verkehrsfluss“ ist der Fachbegriff der Betreiberpraxis für diese Daten zur betrieblichen Qualitätssicherung. Er wird betreiberseitig mit Standardprodukten, verbreitet beispielsweise im sog. Netflow-Format (proprietärer Standard der Firma Cisco) erhoben. Die gespeicherten Informationen sind abhängig vom jeweiligen Speicherformat und enthalten im Falle von Netflow typischerweise unter ande-rem Quell- und

Ziel-IP-Adressen, Zeitstempel und den jeweiligen Protokolltyp. Damit wer-den auch die im Verkehrsfluss anfallenden Verbindungen von Servern des Hosters zu dem Steuerungsserver eines Angreifers protokolliert.

Anhand von im Netflow protokollierten technischen Parametern kann geprüft werden, ob es sich bei diesen weiteren Verbindungen ebenfalls um solche des Angreifers handelt. So können Infrastrukturnetzwerke von Cyberspionagegruppen aufgeklärt und bisher nicht sichtbare Angriffe gegen deutsche Stellen detektiert werden. Je nach Zeitpunkt des Zugriffs ließen sich auch Ausspähversuche auf bestimmte IP-Adressen identifizieren. So wären potentielle Opfer identifizierbar und könnten durch den Wirtschaftsschutz des BfV sensibilisiert werden.

Die Speicherung von Verkehrsflussdaten bei Providern variiert deutlich, da es keine verpflichtenden Vorgaben gibt. Auch diese gesetzliche Regelung soll ausschließlich auf der betrieblichen Praxis aufsetzen und enthält keinerlei Verpflichtung zu besonderen Vorsorgemaßnahmen speziell für solche Abfragen. Beispielsweise wird in bekannten Implementierungen auf eine vollständige Abdeckung des Verkehrs verzichtet und der Verkehrsfluss mit vorabdefinierten Raten gespeichert (z.B. 1 von 5.000 Verbindungen). Mangels verpflichtender Vorgaben ist auch die Speicherdauer variabel und abhängig vom Bedarf des Betreibers. Regelmäßig wird die betriebliche Speicherung lediglich für einen Zeitraum von wenigen Tagen erfolgen. Die Auskünfte nach Satz 2 Nummer 1 beziehen sich allein auf diese aus betrieblichen Gründen beim Unternehmen vorhandene Dokumentation des Verkehrsflusses.

Parameter zur Bestimmung des relevanten Verkehrsflusses kann beispielsweise eine bestimmte IP-Adresse sein, für die tatsächliche Anhaltspunkte bestehen, dass der Angreifer sie für ihren Angriff nutzt (maliziöse Kennung). Die Auskunftspflicht dient zunächst auch der Klärung des genutzten Providers, wenn - etwa aus der Zusammenarbeit mit anderen Nachrichtendiensten – IP-Adressen bekannt werden, für die tatsächliche Anhaltspunkte dafür bestehen, dass diese zu Angriffskampagnen auch gegen Ziele in Deutschland genutzt werden, ohne dass zunächst bekannt ist, welche IT-Infrastruktur in Deutschland dafür genutzt wird.

Zu Nummer 2

Nummer 2 bezieht sich auf Angriffswerkzeuge, die im System des Diensteanbieters vorliegen. Spuren, die technisch mit dem Angriff verbunden sind, sind eingeschlossen, beispielsweise genutzte Prozesse und Verweisungen auf Speicherorte für erbeutete Informationen. Darüberhinausgehende Inhalte der Kommunikation werden von Satz 2 nicht erfasst. Das Bundesamt für Verfassungsschutz kann den Provider bei der Erfüllung der Auskunftspflicht etwa durch die Bereitstellung notwendiger Hardware unterstützen.

Zu Absatz 2

In Fällen, in denen eine Übermittlung von einzelnen Informationen nach Absatz 1 Satz 2 Nummer 2 technisch nicht möglich oder zumutbar ist, ist ausnahmsweise nach Absatz 2 die Herausgabe von Kopien einzelner Teile eines informationstechnischen Systems geboten. Ausgangspunkt sind dem BfV vorliegende Informationen über den Angriff (etwa eine Angreifer-IP), die dem Provider die Identifikation des vom Angreifer genutzten IT-Bereichs und damit von vornherein die Begrenzung der Erhebung auf den kleinstmöglichen Sektor des genutzten IT-Systems ermöglichen. Die Datenverarbeitung wird in diesen Fällen zusätzlich durch Absatz 3 Satz 2 begrenzt.

Zu Absatz 3

Absatz 3 ist an das BfV adressiert und regelt dessen Ersuchen, dem die Übermittlungspflicht nach Absatz 1 und 2 folgt. Das Herausgabeverlangen zu einer Kopie wird dabei nach Nummer 2 an erhöhte Voraussetzungen gebunden.

Zu Absatz 4

Absatz 4 enthält spezifische Vorgaben, um den Eingriff auf den erforderlichen Umfang begrenzt zu halten. Die nach Satz 2 nötige Auswertung der Kopien einzelner Teile eines informationstechnischen Systems orientiert sich dabei immer an technischen Parametern. Es gilt, in einem ersten Schritt Logdateien und Verzeichnisstrukturen zu analysieren, um beispielsweise die Frage zu klären, was auf dem System geschehen ist. Dabei können verschiedene Werkzeuge des Akteurs, wie Skripte, Exploits und Malware, identifiziert werden. Werden über solche Informationen zudem Daten als Beutegut des Angriffs zuordenbar, können auch diese ausgewertet werden, müssen also nicht sogleich gelöscht werden.

Zu Absatz 5

Absatz 5 stellt klar, dass der Provider seine Vertragspflichten nicht verletzt, wenn er Malware oder mit dem informationstechnischen Angriff erbeutete Daten löscht. Durch eine Sicherungskopie wird die Reversibilität gewährleistet ebenso wie die weitere Aufklärung des Angriffs. Dazu ist die Sicherungskopie an das BfV herauszugeben. Im Übrigen ist tunlich, dass sich der Provider mit dem BfV abstimmt, da mit der Löschung dem Angreifer bekannt werden kann, dass seine Angriffsstruktur entdeckt ist. Unter Umständen kann es zweckmäßiger sein, eine Situation, wenn sie sich unter Kontrolle befindet, weiter zu beobachten, um die Angriffskampagne strukturell weiter aufklären zu können.

Zu Absatz 6

Absatz 6 trifft Folgeregelungen für den Fall, dass der die Maßnahme veranlassende Verdacht entfallen ist. Da bei gefertigtem sektoralem Systemabbild wegen des Datenumfangs Umständen ein besonderes Betroffeneninteresse an nachgängiger Klärung bestehen kann, werden die Daten hier nicht sogleich gelöscht, sondern zunächst nur gesperrt. Satz 3 enthält Löschungsregelungen, die gleichermaßen den Individualinteressen des Betroffenen Rechnung tragen (Nummern 1 und 2) wie auch einem davon unabhängigen Datenschutzkontrollinteresse (letzter Halbsatz in Nummer 1).

Zu Absatz 7

Der Absatz verweist für Formerfordernisse und Kostenfolgen auf die allgemeinen Bestimmungen in § 11. Speziell bei der Durchführung des § 13 wird die Vereinbarungsoption nach § 11 Absatz 7 Satz 2 besondere Praxisrelevanz besitzen.

Zu § 13 (Verpflichtende Ersuchen an Anbieter von Telekommunikationsdiensten)

§ 13 trifft bereichsspezifische Vorschriften, die die allgemeine Regelung von Unternehmenspflichten in § 11 speziell zu Telekommunikationsdiensten ergänzen. Dabei integrieren sie den bisherigen § 8d wie auch Vorgaben des Artikel 10-Gesetzes, das aufgehoben und inhaltlich in die Fachgesetze integriert wird.

Zu Absatz 1

Der Absatz verstärkt einerseits die Übermittlungsregelung des § 9 zur Übermittlungspflicht und beruft dazu als normatives Grundgerüst des § 11 Absatz 2, 3, 6 und 7 zur Anwendung, Hinzutreten bereichsspezifische Regelungen speziell zu TK-Diensten in den nachfolgenden Absätzen.

Sofern Standortdaten aus Diensten mit Zusatznutzen (§ 2 Absatz 2 Nummer 5 TDDDG) GPS-basiert präzise Geodaten enthalten, können zur Auswertung für eine längerfristige Bewegungsüberwachung im Übrigen Einschränkungen aus § 37 Absatz 2 Satz 1 Nummer 3 folgen.

Zu Absatz 2

Die Regelung sieht in Satz 1 zur Aufwandsvermeidung die Subsidiarität der konventionellen Unternehmensabfrage gegenüber der Nutzung eingerichteter Abrufverfahren vor.

Satz 2 entspricht dem bisherigen § 8d Absatz 3. Eine spezielle Verfahrensregelung erübrigt sich, da der allgemeine Verweis auf die gesetzlichen Voraussetzungen auch Verfahrensvoraussetzungen einschließt. Dann, wenn die vorbereitete Anschlussnutzung einer unabhängigen Vorabkontrolle unterliegt, muss diese mithin bereits zur Auskunft über PIN/PUK erfolgen (BVerfGE 130, 151 – Rn. 185). Eine von der vorbereiteten Maßnahme unabhängige Verfahrensregelung ist dagegen nicht erforderlich, vielmehr sollen eben gerade annexe Anforderungen bereits auf die Vorbereitungsmaßnahme gelten.

Satz 3 entspricht dem bisherigen § 8d Absatz 2.

Zu Absatz 3

Die Vorschrift regelt qualifizierte Auskünfte. Der Begriff der Qualifizierten Auskunft ist in § 11 Absatz 3 Satz 1 Nummer 2 Buchstabe b eingeführt. Die Schwelle in Satz 1 Nummer 1 entspricht der in § 11 Absatz 5 Nummer 1, zugleich auch der in § 22 Absatz 1 Satz 2. Diese Schwelle gilt für die Umstände der Kommunikation (Verkehrsdaten). Für Kommunikationsinhalte gilt die höhere Schwelle nach Absatz 4. Ebenso synchronisiert Satz 1 Nummer 2 die Maßnahmerichtung mit den Vorgaben in § 22. Für Einsatzschwelle und Maßnahmerichtung macht es keinen Unterschied, ob die Informationen unter Indienstnahme des Providers beschafft werden.

Satz 2 stellt klar, dass auch eine Funkzellenabfrage möglich ist.

Zu Absatz 4

Der Absatz regelt die Erhebung von Kommunikationsinhalten. Wie bereits zu Verkehrsdaten in Absatz 3 erfolgt hier ebenso die Synchronisierung mit den materiellen Voraussetzungen der entsprechenden Erhebung ohne Indienstnahme des Providers nach § 22. Satz 3 übernimmt die bisherige Regelungen in § 2 Absatz 1a Satz 1 Nummern 2 und 3 G 10.

Zu Absatz 5

Die Regelung greift den bisherigen § 2 Absatz 1a Satz 1 Nummer 4 G 10 auf. Im G 10 war die Unterstützung bei der Einbringung des technischen Tools entsprechend dem Gesetzesanwendungsbereich bezogen auf die Telekommunikationsüberwachung (sog. Quellen-TKÜ) geregelt. Nunmehr wird dies allgemein zur Einbringung in informationstechnische Systeme geregelt. Wie auch in Absatz 3 und 4 ist auch diese Unterstützungshandlung mit den Voraussetzungen der originären Erhebungsbefugnisse synchronisiert, hier indem die jeweilige Anordnung zum Eingriff in das informationstechnische System vorausgesetzt wird. Der Bezug auf eine „vollziehbare“ Anordnung bezieht damit die Verfahrensvoraussetzungen nach § 34 mit ein.

Zu Absatz 6

Der Absatz entspricht dem bisherigen § 2 Absatz 2 Artikel 10-Gesetz. Satz 2 trifft eine organisatorische Vorgabe zur vorsorgenden Gewährleistung der tatsächlichen Durchführbarkeit der Maßnahme. Das BMI kann sich als Aufsichtsbehörde nach § 72 Absatz 1 Satz 2 darüber informieren, ob das Unternehmen seiner Vorsorgepflicht nach Satz 2 genügt. Nötigenfalls kann es zur Erfüllung der Vorsorgepflicht nach Satz 6 Anordnungen treffen, etwa wie viele Beschäftigte sie bis wann zur Einleitung einer Sicherheitsüberprüfung zu veranlassen haben. Die Auskunftspflicht und die durch Anordnung konkretisierte Vorsorgepflicht sind nach § 73 Absatz 1 Nummer 3 und 4 bußgeldbewehrt.

Zu Absatz 7

Die Regelung übernimmt § 13 des Artikel 10-Gesetzes.

Zu § 14 (Verpflichtende Ersuchen an Anbieter von Postdiensten)

Die bereits ursprünglich auch im Bundesverfassungsschutzgesetz enthaltene Postauskunft zu Verkehrsdaten war in der Annahme aufgehoben worden, dass Postverkehre angesichts elektronischer Informationsübertragung nicht mehr praxisbedeutsam seien. Diese Erwartung hat sich nicht bestätigt. So sind auch weiterhin Postinhaltsüberwachungen nach dem Artikel 10-Gesetz erfolgt. Spezieller Bedarf, auch zu Verkehrsdaten, besteht für die Logistikbranche mit Paketdiensten, etwa für die Proliferationsaufklärung und Embargoüberwachung. Unter diesen Erwägungen war zuletzt bei der Neuverkündung des MAD-Gesetzes bereits wieder eine Postauskunft aufgenommen worden.

Zu Absatz 1

Die Regelung erfolgt parallel zur Regelung für TK-Dienste in § 13 (dort in Absatz 1 Satz 2 auch die Verweisung auf § 11). Satz 2 übernimmt den bisherigen § 3 Absatz 2 Satz 4 G 10.

Zu Absatz 2

Der Absatz trifft Spezialregelungen zu Inhaltsauskünften. Satz 1 entspricht § 13 Absatz 3 Satz 3. Satz 2 übernimmt die bisherigen Regelungen aus § 2 Absatz 1 Satz 1. Eine dem bisherigen § 2 Absatz 1 Satz 2 G 10 entsprechende, spezielle Regelung erübrigt sich nach dem neuen Regelungskonzept der Unternehmensauskünfte, das nicht auf einzelne Informationsgegenstände ausgerichtet ist, sondern allgemein Informationsklassen nach Eingriffsgewicht kategorisiert.

Zu § 15 (Verpflichtende Ersuchen an Verfügungsberechtigte von Einrichtungen zur Videoüberwachung)

Die Regelung ist initiiert von einer Empfehlung der Innenministerkonferenz zu harmonisierten Verfassungsschutzgesetzen in Bund und Ländern (207. Sitzung am 8. Dezember 2017, TOP 29). Einige Landesverfassungsschutzgesetze enthalten bereits solche Regelungen (vgl. z.B. § 19a Absatz 1 Satz 4 BayVSG, § 21 LVerfSchG RP). Die Regelung folgt der Systematik dieses Unterabschnitts, die Sachvoraussetzungen der Informationsbeschaffung mit der Zulässigkeit von Ersuchen zu regeln (Absatz 2) und als Folge des zulässigen Ersuchens die Mitwirkungspflicht zu begründen (Absatz 1).

Zu Absatz 1

Der Absatz verpflichtet gleichermaßen öffentliche wie nichtöffentliche Stellen. Erfasst sind dabei allerdings ausschließlich Anlagen zur Überwachung des öffentlich zugänglichen Raums. Neben dem öffentlichen Verkehrsraum sind dies auch öffentlich zugängliche Einrichtungen. Nach Satz 2 entstehen dem Verpflichteten keine Aufwände durch – nicht geforderte – Umrüstung seiner Einrichtung. Sie haben lediglich die Mitbenutzung ihrer Einrichtung zu ermöglichen (Nummer 1) und die Daten in Echtzeitdaten auszuleiten (Nummer 2), dies als Sekundärnutzung im Rahmen des originären Einsatzes der Einrichtung (keine Verpflichtung, den Einsatz an BfV-Anforderungen anzupassen, unbeschadet solcher freiwilligen Kooperation), sowie ohnehin gespeicherte Daten (keine Pflicht zur Vorratsspeicherung) zu übermitteln (Nummer 3).

Zu Absatz 2

Absatz 2 regelt die für das BfV geltenden Voraussetzungen der Ersuchen. Angelehnt an die allgemeine Schwelle für verpflichtende Ersuchen zu Unternehmensauskünften ist dies nach Satz 1 die erhebliche Beobachtungsbedürftigkeit (mit bloßen

Bestandsdatenauskünften ist der Eingriff nicht vergleichbar). Satz 2 trifft eine ergänzende Maßgaben für den Sonderfall, dass trotz der stationären Maßnahme eine § 20 Absatz 2 entsprechende Überwachung resultiert. Satz 3 gibt bei der Erhebung gespeicherter Aufzeichnungen die zeitliche Eingrenzung des Ersuchens vor.

Zu Absatz 3

Absatz 3 enthält Löschungsregelungen zu den nach Absatz 1 Satz 1 Nummer 3 übermittelten Aufzeichnungen.

Zu Unterabschnitt 2 (Nachrichtendienstliche Mittel)

Der Unterabschnitt folgt mit der Neuregelung des Einsatzes nachrichtendienstlicher Mittel den Vorgaben der Verfassungsrechtsprechung. Die neue Regelung ist inhaltlich bestimmter, indem ein Einsatz nachrichtendienstlicher Mittel, der qualifiziert in Grundrechte eingreift, in speziellen Befugnisnormen geregelt wird (§§ 17 ff.), dies geknüpft an näher gesetzlich ausgeformte Voraussetzungen qualifizierter Beobachtungsbedürftigkeit (§ 3 Absatz 6 und 7). Auch die allgemeine Befugnis zum einfachen – nicht derart intensivem – Einsatz nachrichtendienstlicher Mittel wird inhaltlich bestimmter ausgeformt, indem er nunmehr querschnittlich bereits durch Gesetz rechtsstaatlich auf Zielpersonen mit einer individuellen Nähe zum Aufklärungsziel beschränkt wird (§ 16 Absatz 5). Ebenso erfolgen querschnittlich besondere Grundrechtssicherungen zum Schutz des Kernbereichs privater Lebensgestaltung (§ 31) und von Berufsgeheimnissen (§ 32). Flankierend werden in Unterabschnitt 3 besondere Verfahrenssicherungen gesetzlich ausgeprägt, dies bereits zur innerbehördlichen Entscheidung (§ 33). Wenn mit der Gewinnung auch höchstprivater Informationen zu rechnen ist, tritt das Erfordernis unabhängiger Vorabkontrolle (§ 34) hinzu, im Ergebnis wesentlich verbreitert gegenüber dem geltenden Recht. Ebenso verbreitert wird die nachträgliche Mitteilung über die Durchführung der Maßnahme an betroffene Zielpersonen (§ 35).

§ 16 bildet dabei die Grundnorm, die mit §§ 17 ff. für spezielle Sachverhalte durch zusätzliche Anforderungen ergänzt wird. § 16 muss beim Einsatz nachrichtendienstlicher Mittel immer erfüllt sein und zusätzlich weitere Voraussetzungen nach Maßgabe der §§ 17 ff. bei besonderen Sachverhalten. Damit trifft § 16 gewissermaßen vor die Klammer gezogen allgemeine Vorgaben, die auch bei Maßnahmen nach §§ 17 ff zu beachten sind. Dies gilt für die in § 16 Absatz 1 aufgenommene Voraussetzung tatsächlicher Anhaltspunkte im Einzelfall zur Erforderlichkeit der Maßnahme für das Aufklärungsziel (das in §§ 17 ff. begrenzt wird auf qualifizierte Bedrohungen) sowie die Beschränkung der zulässigen Maßnahmerichtung in § 16 Absatz 5. Soweit in §§ 17 ff. hierzu spezielle Maßgaben getroffen werden, gehen diese vor. Dies betrifft die begrenzte Maßnahmerichtung in § 24 (nur kommerzielle Host-Provider) sowie nach § 22 Absatz 3, § 25 Absatz 2 und § 27 Absatz 2.

Die Qualifikationstatbestände in §§ 17 bis 23 und 26 beruhen auf den vom Bundesverfassungsgericht (BVerfGE 162, 1 – Rn. 191) benannten allgemeinen Qualifikationskriterien (§ 25 und §§ 27, 28 sind unter den besonderen Anforderungen aus Artikel 13 Absatz 4 GG und der Verfassungsrechtsprechung gesondert zu betrachten). Diese Schwellenanforderungen werden in §§ 17 ff. für besondere Einsatzmittel in speziellen Einsatztatbeständen spezifiziert. § 29 ergänzt dies durch einen kriteriengestützten Tatbestand für außergewöhnliche Sachverhalte, in denen sonstige nachrichtendienstliche Mittel ungewöhnlicher Weise (daher nicht gesetzlich vertypt) auch qualifiziert eingreifend werden. Neben den benannten Gewichtungskriterien sind dabei auch die vorausgehenden besonderen Tatbestände leitbildhaft zur Gewichtung mit heranzuziehen.

Das geltende Recht enthält bereits rechtspolitische Referenzgrößen der Eingriffsgewichtung. Die besonderen Regelungen zu Vertrauensleute-Einsätzen (ohne Inanspruchnahme einer besonders persönlichen Vertrauensbeziehung) oder der Telekommunikationsverkehrsdatenerhebung beschreiben erhebliche Eingriffe (erste Qualifikationsstufe) und die Befugnis zur Inhaltsüberwachung laufender Telekommunikation besonders erhebliche

Eingriffe (zweite Qualifikationsstufe). Die neuen Befugnistatbestände beziehen diese Referenz bei der Gewichtung im Interesse eines wertungskonsistenten Gesamtsystems ein. Die Wohnraumüberwachung (§ 27) und die Online-Überwachung (§ 25) bilden eigene, nochmals ge-wichtigere Eingriffsklassen. Diese Befugnisse betreffen besondere Schutzsphären und sind nach der Verfassungsrechtsprechung mit polizeilichen Einsatzschwellen verknüpft. Im Übrigen bleibt zur Gewichtung des informationellen Eingriffs einzubeziehen, welche operativen Anschlussfolgen drohen. Insoweit ist auch zu berücksichtigen, dass Nachrichtendienste nicht über eigene operative Anschlussbefugnisse zu außenwirksamen Belastungsakten verfügen. Ein direkter Vergleich zu verdeckten polizeilichen Ermittlungsmaßnahmen wäre mithin fehlleitend (BVerfGE 162, 1 – Rn. 156).

Im Übrigen bedarf auch das Zusammenwirken verschiedener Überwachungsmaßnahmen hinsichtlich etwaiger additiver Eingriffseffekte einer Würdigung am Verhältnismäßigkeitsmaßstab. Das ist im Normvollzug nach der allgemeinen Maßgabe des § 30 Absatz 3 zu beachten und bedarf keiner weiteren gesetzlicher Konkretisierung (BVerfGE 162, 1 – Rn. 287).

Zu § 16 (Datenerhebungen mit nachrichtendienstlichen Mitteln)

Gegenüber der bisherigen Regelung in § 8 Absatz 2 Satz 1 und § 9 Absatz 1 enthält die neue Regelung detailliertere gesetzliche Vorgaben, insbesondere durch eine neue allgemeine Richtung zur Maßnahmerichtung (Absatz 5). Geregelt ist die verdeckte (heimliche) Datenerhebung. Davon zu trennen ist eine Datenerhebung bei Dritten, gegenüber denen das BfV offen als solches auftritt, die aber ihrerseits zur Verschwiegenheit verpflichtet sind (§ 9 Absatz 3). Hiervon abzugrenzen sind ferner Datenerhebungen, die zwar ohne Offenlegung des behördlichen Hintergrundes, aber bereits ohne Grundrechtseingriff erfolgen. Bei Maßnahmen der Informationserhebung ist die nachrichtendienstliche Methodik ein Qualifikationstatbestand, der notwendig als Basis einen Grundrechtseingriff voraussetzt. Der ist beispielsweise nicht bei allgemeinen Internetermittlungen gegeben. Dies gilt auch, wenn die Ermittlungen unter unzutreffender Identitätsangabe erfolgen, denn in deren Wahrhaftigkeit wird im Kommunikationskontext typischerweise kein Vertrauen investiert (vgl. BVerfGE 120, 274 – Rn. 311) und ohne schutzwürdiges Vertrauen fehlt es hier grundsätzlich bereits am Eingriffsgehalt.

Die grundsätzliche Regelungsstruktur des bisherigen Rechts wird beibehalten, wonach § 8 Absatz 2 Satz 1 eine allgemeine Erlaubnis enthält, der Eingriff in die informationelle Selbstbestimmung dazu speziell (bisher in §§ 9 bis 9b) geregelt wird und im Übrigen Kollisionen mit Verbotsnormen durch eine Spezialitätsregelung (allgemein § 8 Absatz 2 Sätze 2 und 3) aufgelöst wird (vgl. Gesetzesbegründung zum bisherigen § 8 Absatz 2, BT-Drs. 18/4654, S. 37 ff). Im neuen Recht enthält § 16 Absatz 1 sowohl die Erlaubnis zum Einsatz nachrichtendienstlicher Mittel wie die allgemeine Befugnis zum Eingriff in die informationelle Selbstbestimmung. Die Abgrenzung des Erlaubnisgehalts im Verhältnis mit kollidieren Verbotsnormen enthält nunmehr § 30. Insbesondere die Regelung zum Eingriff in die informationelle Selbstbestimmung erfolgt nunmehr wesentlich spezifizierender, insbesondere differenzierter nach Eingriffsgewichtung zu einzelnen nachrichtendienstlichen Mitteln und Einsatzumständen (§§ 17 ff.).

Zu Absatz 1

Absatz 1 entspricht in der Substanz dem bisherigen § 9 Absatz 1, wobei dessen Sätze 3 und 4 nunmehr in die normenklarer gesondert getroffene Schrankenregelung des neuen § 30 integriert werden. Eine redaktionelle Verschlankung ergibt sich gegenüber dem bisherigen § 9 Absatz 1 Satz 1 Nummer 2 dadurch, dass die Eigensicherung nunmehr als Aufgabe speziell in § 2 Absatz 4 aufgenommen und die dort definierten funktionsgefährdenden Tätigkeiten nach § 3 Absatz 4 im Begriff der Bedrohung eingeschlossen sind, so dass der bisherige § 9 Absatz 1 Satz 1 Nummer 2 bereits im allgemeinen Bezug auf Bedrohungen eingeschlossen ist, also nicht mehr gesondert aufgeführt zu werden braucht.

Der Einsatz nachrichtendienstlicher Mittel ist nachrichtendiensttypisch und wird – wie bisher – nicht generell an erhöhte situative Schwellen gebunden, es genügt vielmehr das im Einzelfall bestehende Einsatzerfordernis. Das Bundesverfassungsgericht hat dies als verfassungsgemäß bestätigt (BVerfGE 162, 1 - Rn. 186, 206). Die „Vorfeld“-Charakteristik nachrichtendienstlicher Aufklärung ist ein bereits risikobasierter Aufgabenansatz, der grundsätzlich nicht erst bei konkreten bzw. konkretisierten Gefahren einsetzt, sondern deren Entstehen frühzeitig erkennt. Auch dieses Grundverständnis nachrichtendienstlicher Aufgaben hat das Gericht bestätigt (a.a.O. Ls. 1 und Rn. 154, 159).

Die Erkenntnisanforderungen folgen nunmehr einheitlicher Diktion mit dem – auch vom Bundesverfassungsgericht vorgenommenen (a.a.O. Rn. 187 f., 206) – Bezug auf „tatsächliche Anhaltspunkte“. Die bisherige Formulierung „wenn Tatsachen die Annahme rechtfertigen“ war Synonym und bringt mit der Formulierung des Bundesverfassungsgerichts jeweils inhaltlich identisch zum Ausdruck, dass eine konkrete Tatsachengrundlage indizielle Anhaltspunkte für eine Schlussfolgerung bietet (unter interpretatorischer Heranziehung allgemeiner Erkenntnisse, speziell nachrichtendienstlichen Erfahrungswissens). Die unterschiedliche Formulierung desselben Tatbestandes ist missverständlich und wird daher hier im Interesse der Bestimmtheit und Normenklarheit bereinigt. Dabei bildet das Erfordernis der tatsächlichen Anhaltspunkte selbst eine gleitende Anforderungsskala zur Erkenntnisdichte abhängig vom Eingriffsgehalt der hierauf gestützten Maßnahme aus, die unter Verhältnismäßigkeitserwägungen bei schlichten verdeckten Ermittlungen minderen Anforderungen folgt als bei besonders erheblich eingreifenden Maßnahmen wie etwa einer Telekommunikationsüberwachung nach § 3 Absatz 1 Artikel 10-Gesetz (auch dort: „tatsächliche Anhaltspunkte“). Diese Anforderungsregulierung erfolgt sachgerecht über den Verhältnismäßigkeitsgrundsatz (§ 30 Absatz 3), ein gesetzgeberisches „Feintuning“ durch detailliert gestufte Erkenntnisregelungen würde die Leistungsfähigkeit von Gesetzgebung, die einen messbaren Maßstab bilden muss, überdehnen. Allgemein gilt lediglich, dass der nachrichtendienstlichen Aufgabe der Frühaufklärung generell ein spezifisch niederschwelliger Erkenntnisansatz zugrunde liegt. Gerade dem dient die Einrichtung gesonderter Nachrichtendienste mit der Aufgabenbeschränkung auf Gefahrerforschung, behördlich getrennt von polizeilich-intervenierender Aufgabenwahrnehmung (vgl. BVerfGE 162, 1 – Rn. 153 ff.).

Auf eine beispielsweise an § 21 Absatz 3 Satz 3 BPolG orientierte spezielle Regelung verdeckter Umfeldermittlungen kann weiterhin verzichtet werden. Auch beim Verfassungsschutz kann verdecktes Auftreten gegenüber Dritten zum Schutz der betroffenen Person erfolgen (wenn offenes Auftreten bei Fragen zum Betroffenen diesen nachteilig als mutmaßlichen Extremisten etikettieren würde). Die Zulässigkeit folgt unmittelbar aus Absatz 1, da die Datenerhebung solcher Erkenntnisgewinnung dient und die Methodik der verdeckten Ermittlung dabei als für den Betroffenen milderes Mittel zum Einsatz kommt, also erforderlich ist.

In Satz 2 wird die beispielhafte Aufzählung einzelner nachrichtendienstlicher Mittel gegenüber dem bisherigen § 8 Absatz 2 modifiziert. Aufgeführt werden Gruppen von Einsatzmitteln, nämlich eigene Bedienstete (Nummer 1), andere Personen, deren Zusammenarbeit mit dem BfV nicht bekannt ist (Nummer 2), und technische Mittel (Nummer 3). Neu aufgeführt wird die heimliche Inbesitznahme, da der berechtigte Besitz ein Individualrecht ist, es nach § 30 Absatz 1 mithin einer speziellen Befugnis bedarf und eine besondere Regelung hier normenklarer ist, als eine Annexableitung aus der Befugnis zur heimlichen Informationsbeschaffung. Die Inbesitznahme kann etwa Dokumente oder Substanzen betreffen, die einer nachrichtendienstlichen Untersuchung bedürfen. Dieser Folgeeingriff ist hier nicht mitgeregelt, sondern ergibt sich aus der jeweiligen Erhebungs- bzw. Weiterverarbeitungsbefugnis. Die spezielle Befugnis in Nummer 4 hat lediglich die Inbesitznahme als solche zum Gegenstand. Wird also beispielsweise ein Speichermedium zum Auslesen beschafft, ergibt sich die Befugnis zur heimlichen Inbesitznahme aus § 16 Absatz 1 und die Befugnis zum Auslesen aus § 23. Satz 4 verpflichtet zur Rückgabe in Besitz genommener Sachen. Ein entgegenstehende Sicherheitsinteressen ist insbesondere Entdeckungsgefahr.

Die Einsatzmethodik der aufgeführten Mittel wird in den nachfolgenden Paragraphen spezifiziert, soweit sich daran ein qualifiziertes Eingriffsgewicht knüpft. § 16 Absatz 1 lässt als grundrechtswesentliche Entscheidung zwar allgemein die heimliche Informationsbeschaffung zu, dabei aber nicht Eingriffe mit erheblicher Eingriffswirkung. Diese sind abschließend für Maßnahmen mit typisiert qualifiziertem Eingriffsgehalt in §§ 17 ff. geregelt und für atypische Einsatzwirkungen in § 29. Das Maß gesetzlicher Detailschärfe der allgemeinen Regelung – mit begrenztem Eingriffsgewicht, insoweit aber anwendungsflexibler Offenheit - trägt mithin der geregelten Sachmaterie Rechnung (BVerfGE 133, 277 - Rn. 117; BVerfGE 162, 1 - Rn. 213).

Zum beschriebenen Spezialitätsverhältnis der Regelungen ergibt sich etwa zu verdeckt ermittelnden Bediensteten Folgendes: Zu einfachen Befragungen, die verdeckt – ohne Angabe des Zwecks und der erhebenden Stelle – erfolgen, oder zu lediglich zeitlich eng begrenzten Observationen ist wegen des begrenzten Eingriffsgewichts keine besondere Regelung erforderlich. Dagegen werden qualifizierte Formen der Internetermittlung, langfristige Observationen oder der längerfristige Einsatz unter dauerhafter Voll-Legende speziell geregelt (§§ 17 bis 20).

Ebenso werden technische Mittel in § 16 Absatz 1 allgemein aufgeführt (ohne Fokussierung auf die im bisherigen § 8 Absatz 2 Satz 1 benannten Bild- und Tonaufzeichnungen) und ergänzend zu eingriffsintensiven Formen in besonderen Befugnissen spezifiziert (§§ 20 ff.). Gerade der Bereich technischer Einsatzmittel unterstreicht den Bedarf nötiger Entwicklungsoffenheit (und u.U. auch den Bedarf des Geheimschutzes zu Fähigkeiten und Vorgehen, die nicht im Näheren im Bundesgesetzblatt zu publizieren sind). Der Gesetzgebungsfunktion adäquat und zukunftsfest praxistauglich kann hier nur eine technikneutrale Regelung sein, die das Grundrechtswesentliche erfasst (heimliche Erhebung personenbezogener Daten unterhalb der Schwelle erheblichen Eingriffsgewichts) und mit § 16 an adäquate Voraussetzungen bindet. Aktuell fällt darunter etwa die Ermittlung der Geräte- oder Kartennummer eines Mobilfunkgerätes mit einem IMSI-Catcher (als Eingriff der Bestandsdatenerhebung von geringem Gewicht und danach auf die Befugnis nach Absatz 1 zu stützen; der IMSI-Catcher überwacht nicht durch Telekommunikationsdienste übertragene Datenverkehre, sondern simuliert selbst eine Funkzelle, in die sich das Gerät einbucht, d.h. der Staat ist hier – verdeckt – selbst Empfänger der Übertragung).

Zu Absatz 2

Absatz 2 trifft zur Verpflichtung von verdeckten Hilfspersonen eine bereichsspezifische Maßgabe zur Anwendung des Verpflichtungsgesetzes. Die Änderung ermöglicht in besonderen Einzelfällen eine größere Flexibilität in der Zusammenarbeit mit verdeckten Hilfspersonen. Grundlage dieser besonderen Art der Zusammenarbeit ist eine absolute Verschwiegenheitszusage beider Parteien, auf welcher das notwendige Vertrauensverhältnis aufgebaut wird. Wird mit der Verpflichtung von der verdeckten Hilfsperson ein schriftliches Bekenntnis zur Zusammenarbeit eingefordert, kann dies in einzelnen Fällen die Vertrauensbeziehung zwischen Fallführung und verdeckter Hilfsperson so empfindlich stören, dass die Zusammenarbeit von der verdeckten Hilfsperson im Zweifel abgebrochen würde. In diesen Einzelfällen konnte bisher seitens der Behörde lediglich komplett auf eine Verpflichtung verzichtet werden, um die Zusammenarbeit weiterzuführen.

Die Regelung ermöglicht hier zukünftig aus den Gründen, die bereits nach § 1 Absatz 3 Satz 2 Verpflichtungsgesetz den Verzicht auf die Aushändigung einer Abschrift rechtfertigen, eine ausschließlich mündliche Verpflichtung. Maßgeblich ist danach, dass dies im konkreten Fall im Interesse der inneren oder äußeren Sicherheit der Bundesrepublik Deutschland geboten ist. Dies ist insbesondere der Fall, wenn die verdeckte Hilfsperson Zugang zu Informationen über eine aufzuklärende Bestrebung oder Tätigkeit hat, die ohne die Mitwirkung der verdeckten Hilfsperson nicht oder nur mit unverhältnismäßigem Aufwand erlangt werden könnten und im Falle der Aufforderung zur Unterzeichnung einer Niederschrift zu befürchten wäre, dass die verdeckte Hilfsperson die Zusammenarbeit beendet.

Da die verdeckten Hilfspersonen in den dargestellten Fällen keinerlei Vorbehalte gegenüber der von ihnen geforderten Verpflichtung zur gewissenhaften Erfüllung ihrer Obliegenheiten, sondern lediglich gegenüber der schriftlichen Verpflichtung hegen, ist die ausschließlich mündliche Verpflichtung gegenüber einer gänzlichen Unterlassung der Verpflichtung deutlich vorzugswürdig.

Im Falle der mündlichen Verpflichtung wird die Niederschrift über die Verpflichtung durch die Behörde ohne die Unterschrift der zu verpflichtenden Person aufgenommen.

Zu Absatz 3

Die bisher in § 8 Absatz 2 mit aufgeführten Tarnpapiere und Tarnkennzeichen sind selbst nicht operative Maßnahmen, sondern Hilfsmittel der Legendierung, um Aufgaben verdeckt durchführen zu können. Solche Legendierung ist auch ein Grundschutz zur Eigensicherung, etwa von Einrichtungen des BfV. Die Absicherung ist nicht durch konkrete Gefährdungsanhaltspunkte bedingt, sondern dient der allgemeinen Funktionssicherung. Deshalb werden diese Hilfsmittel unabhängig von den nach Absatz 1 zur konkreten Informationsbeschaffung vorausgesetzten Einzelfallanhaltspunkten zugelassen, mit dem Rechtfertigungsgehalt der Amtsbefugnis etwa bei der Herstellung unechter Urkunden oder Identitätstäuschung im allgemein Rechtsverkehr. Die Aufgabenwahrnehmung bezieht im Übrigen auch die Ausbildung ein, so dass Ausbildungszwecke von der Regelung mit umfasst sind.

Die Abtarnung ist dadurch nicht auf Vorsorgemaßnahmen beschränkt, sondern bleibt zugleich im Einzelfall operativ unterstützend. Dies betrifft nicht nur den Einsatz bei Internetermittlungen (§ 17, eventuell nicht mit Voll-Legende, aber Elementen) sowie von verdeckten Bediensteten (§ 19), sondern unter Umständen auch die Forschungsphase vor Anwerbung von Vertrauenspersonen oder auch deren Fallführung. In besonderen Fällen ist Vertrauenspersonen nicht bekannt, dass sie für das BfV tätig sind, beispielsweise bei Personen aus diktatorischen Herkunftsländern, die zur Aufklärung deren Aktivitäten einerseits zusammenarbeitsbereit sind, aufgrund ihrer Herkunftserfahrungen aber ein allgemeines Misstrauen gegenüber „Geheimdiensten“ haben können, dem mit dem Auftritt als Vertreter einer anderen Behörde Rechnung getragen werden kann. Im Übrigen schließt die Finalität (zur verdeckten Aufgabenwahrnehmung) auch Ausbildungsmaßnahmen ein, dies sowohl hinsichtlich der Abdeckung solcher Maßnahmen wie auch die Vermittlung von Fertigkeiten der Herstellung von Tarnmitteln.

Die im Bundesverfassungsschutzgesetz neue Regelung einer speziellen Amtshilfepflicht in Satz 2 findet sich bereits in einigen Landesverfassungsschutzgesetzen (z.B. § 6 Absatz 3, Satz 2 BBVerfSchG, § 14 Abs. 2 Satz 3 NiVerfSchG). Die ausdrückliche Regelung dient der Handlungssicherheit in der Zusammenarbeit bei Behörden, die ansonsten keine Zusammenarbeitsbeziehungen mit dem BfV unterhalten und danach unsicher im Umgang mit solchen Ersuchen sein können.

Zu Absatz 4

Der Absatz behält den besonderen Kontrollmechanismus des bisherigen § 8 Absatz 2 Satz 5 bei, dass die Bestimmung zulässiger nachrichtendienstlicher Mittel untergesetzlich (als Verschlusssache) mit Zustimmungsvorbehalt des Bundesministeriums des Innern erfolgt und unter besonderer parlamentarischer Kontrolle durch das Parlamentarische Kontrollgremium steht (Satz 5). Neu hinzu tritt die unabhängige Rechtskontrolle nach Satz 4 bei untergesetzlicher Regelung neuer Maßnahmetypen.

Im Ergebnis können in der Dienstvorschrift nach Absatz 2 untergesetzlich grundsätzlich nur solche neuen Maßnahmetypen aufgenommen werden, die unterhalb erheblichen Eingriffsgewichts bleiben. Diese rechtliche Beschränkung wird verfahrensmäßig durch den Zustimmungsvorbehalt des Unabhängigen Kontrollrats in Satz 4 gesichert, dessen Rechtskontrolle die Prüfung der Klassifizierung als nicht qualifiziert eingreifend unterliegt.

Gleichzeitig erfolgt aber mit Satz 2 auch eine Forschungs- und Erprobungsöffnung, deren Belastungswirkungen jedoch durch eine Weiterverarbeitungsbeschränkung begrenzt bleiben. Eine solche Erprobungsregelung unterliegt mit der Pflicht zur Unterrichtung des Parlamentarischen Kontrollgremiums (Satz 4) dessen besonderer Kontrolle, in dessen Entscheidung es auch liegt, sich womöglich periodisch berichten zu lassen oder seinem Ständigen Bevollmächtigten (§ 5a PKGrG) einen speziellen Kontrollauftrag zu erteilen. Der Rechtskontrolle des Unabhängigen Kontrollrates unterliegen neben der eingriffsgewichtenden allgemeinen Klassifizierung der Maßnahme auch die konkrete Anordnung (§ 34 Absatz 1 Satz 1 Nummer 10) und die Beachtung der Weiterverarbeitungsschranken, einschließlich der zeitlichen Limitierung der Erprobung nach Satz 3. Die Erprobungsphase ist strikt – nicht verlängerbar – auf 4 Jahre begrenzt. Ein kürzerer Zeitrahmen wäre typischerweise nicht geeignet, zunächst den Erprobungszweck zu erreichen und anschließend ebenfalls noch innerhalb dieses Zeitrahmens eine spezielle Befugnisgrundlage für das erprobungsbewährte Mittel gesetzlich zu ergänzen. Typischerweise benötigt die Erprobung eine gewisse Zeit, da dem Nachrichtendienst regelmäßig nur begrenzte Informationszugänge und begrenzte Steuerungsmöglichkeiten bei der Erfassung informationswertiger Situationen zur Verfügung stehen, beim nachrichtendienstlichen Gegenüber mit Abwehrvorsorge zu rechnen ist und ein Mittel in seiner Konfiguration in einem nachsteuernden Prozess gegebenenfalls angepasst werden muss und womöglich komplementär auch passende Auswertungsmethodiken entwickelt und fortentwickelt werden müssen. Angesichts dieser Umstände wäre auch keine praktikable Alternative, einzelne Erprobungsansätze jeweils bereits vorab speziell gesetzlich zu regeln.

Zu Absatz 5

Absatz 5 trifft erstmals eine allgemeine gesetzliche Regelung zur Maßnahmerichtung einer Personenaufklärung mit nachrichtendienstlichen Mitteln. Geregelt ist dabei nicht die allgemeine Lageaufklärung, etwa der Beobachtung einer extremistischen Szene, die gemäß dem nachrichtendienstlichen Aufgabenprofil zunächst auch einen verdachtsgewinnenden Ansatz verfolgt, insoweit aber auch noch nicht personengerichtet ist. Zielperson nachrichtendienstlicher Maßnahmen hingegen darf künftig nur sein, wer eine spezifische individuelle Nähe zur aufzuklärenden Gefahr besitzt. Regelungsinhalt ist also nicht, den Einsatz nachrichtendienstlicher Mittel auf personengerichtete Informationsbeschaffung zu beschränken, sondern dann, wenn die Informationsbeschaffung personengerichtet erfolgen soll, den zulässigen Betroffenenkreis einzugrenzen.

Spezialregelungen zur Maßnahmerichtung treffen für besondere Einsatzmittel § 22 Absatz 3, § 25 Absatz 2 und § 27 Absatz 2. Eine spezielle Beschränkung, die auch die Maßnahmerichtung betreffen kann, enthält auch § 18 Absatz 2 Satz 2, der den VP-Einsatz unter Ausnutzung einer besonders persönlichen Vertrauensbeziehung auf besonders erheblich beobachtungsbedürftige Bedrohungen beschränkt.

Satz 2 erfasst Fälle eines abstrakten Beteiligungsverdachts. Anders als bei Satz 1 Nummer 1 ist kein konkreter Verdacht tragend, vielmehr folgt hier die Verantwortlichkeit für die Gefahrerforschung bereits aus dem Umstand der Amtswaltereigenschaft, für einen Staat, der gegen Deutschland nach § 2 Absatz 1 Nummer 3 aktiv ist. Nach nachrichtendienstlichen Erfahrungen setzen solche Staaten für solche Tätigkeiten typischerweise auch offen auftretende Amtswalter ein, beispielsweise Botschaftspersonal. Die Erkenntnisgrundlage für die individuelle Verantwortlichkeit einer Zielperson ist hier zwar mit der lediglich abstrakt gegründeten Einschätzung geringer. Andererseits besteht mit dem Bezug zu Hoheitsaufgaben eine Anknüpfung, die schutzwürdige Privatheit tendenziell weniger in den Blick nimmt und andererseits von verstärktem Gefährdungspotenzial geprägt ist. In der Gesamtbetrachtung ist dies wiederum eine angemessene Verantwortlichkeitsgrundlage. Ein Beispiel wäre etwa, wenn ein Staat, der aktiv Spionage gegen Deutschland betreibt, neues Personal an seiner Botschaft beschäftigt, zu dem zwar individuell noch keine Anhaltspunkte für geheimdienstliche Tätigkeiten vorliegen, nach nachrichtendienstlichen Erfahrungen

aber in Betracht zu ziehen und deshalb aufzuklären ist, dass die Person geheimdienstlich eingesetzt wird.

Satz 3 ermöglicht auch, die Eignung verdeckter Hilfspersonen, speziell deren Nachrichtenehrlichkeit von Quellen, zu überprüfen. Dies ist unabhängig vom Stand der Zusammenarbeit, bei Vertrauenspersonen also gerade auch schon vor deren Verpflichtung möglich. Soweit der Einsatz des nachrichtendienstlichen Mittels an das Erfordernis erheblicher oder besonders erheblicher Beobachtungsbedürftigkeit gebunden ist, ist maßgeblich, zur Aufklärung welcher Bedrohungen die Quelle eingesetzt wird oder werden soll, da sich danach das Gemeinwohlinteresse am Quellenzugang und damit die Bedeutung der Quelle bemisst. Satz 4 beschränkt allerdings einen schwer eingreifenden Mitteleinsatz bei Quellen auf Eigensicherungsfälle, wenn also etwa der Verdacht besteht, dass die Quelle ihre Zusammenarbeit mit dem BfV entgegen ihrer Verschwiegenheitspflicht anderen offenbart oder womöglich sogar Beschaffungsaufträge, Einsatzumstände oder -methodiken oder Fallführungen des BfV preisgibt. Der Verdacht funktionsgefährdender Tätigkeiten von Quellen begründet generell besonders erhebliche Beobachtungsbedürftigkeit, denn aus ihrem Insiderwissen, das bei Weitergabe an Beobachtungsobjekte künftige Aufklärungserfolge massiv sabotieren kann, resultiert in solchen Fällen generell besondere Gefährlichkeit (§ 3 Absatz 7 Nummer 3 Buchstabe a).

Zu Nummer 1

Die Regelung greift mit den Begriffen „Bedrohung“ und „beteiligt“ Legaldefinitionen aus § 3 Absatz 4 und 5 auf.

Die Beteiligung ist gefahrenabwehrrechtlich – vergleichbar dem Verantwortlichen - zu verstehen, setzt also keinen Vorsatz voraus. Beteiligt sind auch Personen, deren Sachen als Tatmittel zum Einsatz kommen bzw. kommen sollen (ähnlich einem „Zustandsstörer“). Die Art der Beteiligung ist unmaßgeblich, insbesondere ist auch zum Einsatz von Befugnissen, die auf Straftaten gerichtete Personenzusammenschlüsse voraussetzen (z.B. § 3 Absatz 7 Nummer 1 Buchstabe b)) nicht etwa eine Beteiligung an den Straftaten selbst erforderlich, es genügt die objektive Förderung der Bestrebungen als solcher, etwa auch in der infrastrukturellen Logistik. Auch ein Spendensammelverein kann für eine terroristische Organisation direkt wie auch mittelbar unterstützend tätig sein (z.B. BVerwGE 153, 211).

Zu Nummer 2

Die verfassungsrechtlich vorauszusetzende spezifische individuelle Nähe zur aufzuklärenden Gefahr folgt noch nicht daraus, dass der nicht selbst an der Bedrohung Beteiligte mit einer Zielperson überhaupt in irgendeinem Austausch steht. Darüber hinaus muss aufgrund zusätzlicher Anhaltspunkte anzunehmen sein, dass der Kontakt einen Bezug zum Ermittlungsziel aufweist und so eine nicht unerhebliche Wahrscheinlichkeit besteht, dass die Überwachungsmaßnahme der Aufklärung der Bedrohung dienlich sein wird (BVerfGE 162, 1 - Rn. 212). Für eine solche Abschätzung ist wesentlich auch auf nachrichtendienstliches Erfahrungswissen abzustellen (a.a.O. Rn. 205, 221). Ein Beispiel wäre etwa eine Umfeldperson der Zielperson, wenn deren aktueller Verbleib unbekannt ist, aber aufgrund persönlicher Beziehung erwartbar ist, dass die Zielperson zu diesem Dritten Kontakt aufnehmen wird (ohne dass dieser etwa als Nachrichtenmittler selbst zum Beteiligten werden soll) und hieraus neue Spurenansätze für Anschlussermittlungen zur Zielperson gewonnen werden können. Ein weiteres Beispiel wäre ein Unterstützer, der nicht nachdrücklich unterstützt und somit nicht bereits selbst Beteiligter ist (§ 3 Absatz 5 Nummer 2), über den aber dennoch im Unterstützungszusammenhang bestimmte relevante Erkenntnisse zur Aufklärung der Bedrohung zu gewinnen sind.

Satz 4 trifft insofern allerdings eine einschränkende Regelung zu besonders erheblich eingreifenden Maßnahmen, die Zusammenhangspersonen nach Nummer 2 ausschließt.

Zu Absatz 6

Absatz 6 ermöglicht zur Maßnahmevorbereitung und -durchführung einen heimlichen Zutritt zu Gebäuden und Räumen, was das Überwinden von Zutrittssperren einschließt. Auf der Schrankenebene wird dabei zwischen Wohnungen (Satz 2) und sonstigen Räumen unterschieden. Der annexe Eingriff in die Wohnung unterliegt den in Satz 2 vorgesehenen erhöhten Voraussetzungen (BVerfGE 165, 1 – Ls. 2, Rn. 147 ff., 155). In § 34 Absatz 1 Satz 1 Nummer 1 ist zudem die unabhängige Vorabkontrolle durch den Unabhängigen Kontrollrat vorgesehen. Mit Satz 1 erfolgt eine komplementäre Klarstellung zum annexen Zugang für Räume, die keine Wohnung sind. Für sonstige annexe Zutritte, etwa zu einem befriedeten Besitztum, ist keine annexe Regelung nötig, vielmehr ist dies allgemein in Absatz 1 eingeschlossen.

Der Anwendungsbereich des Satzes 2 entspricht der schrankenbezogenen differenzierenden Rechtsprechung des Bundesverfassungsgerichts zu Artikel 13 GG, die zwischen einerseits der räumlichen Privatsphäre, in der sich das Privatleben im engeren Sinne abspielt, unterscheidet und andererseits Räumen, die ohne Ausrichtung auch auf höchstprivate Kommunikation zur sozialen Begegnung bestimmt sind, wie etwa Betriebs- Geschäfts- oder Vereinsräume. Die Voraussetzung der konkretisierten Gefahr und der unabhängigen Vorabkontrolle bezieht das Gericht auf einen besonderen – räumlichen - Schutz „höchstpersönlicher Lebensgestaltung“ (Rn. 134) und eine Befugnis, die auch „privateste Räume“ einschließt (a.a.O. Rn. 133). Bei weniger eingriffsintensiven Maßnahmen sieht das Gericht dagegen die Verhältnismäßigkeit bereits durch den Schutz besonders gewichtiger Rechtsgüter gewahrt (a.a.O. Rn. 173). Die Verfassungsschutzaufgabe dient insgesamt dem Schutz solcher Rechtsgüter (BVerfGE 155, 119 – Rn. 151).

Zu § 17 (Internetermittlungen auf vertiefter Vertrauensbasis)

Nimmt das BfV im Internet Kommunikationsbeziehungen auf, liegt darin auch dann grundsätzlich noch kein Grundrechtseingriff vor, wenn es verdeckt operiert, selbst wenn dies über einen längeren Zeitraum unter Bildung einer Art „elektronischer Gemeinschaft“ erfolgt, denn ein Vertrauen in die Identität und Wahrhaftigkeit seiner Kommunikation ist angesichts der Eigenart typischer Kommunikationsbeziehungen im Internet nicht schutzwürdig (BVerfGE 120, 274 – Rn. 311). Das Empfinden von Privatheit hat sich bei der Generation der „digital natives“ wesentlich gewandelt. Folge ist in breiten Kreisen der Netzkultur eine typische Unbefangenheit, in diesem Rahmen auch von sich aus private Informationen zu teilen.

Erst eine spezifische personale Beziehung, in der persönliches und damit schutzwürdiges Vertrauen aufgebaut – und zur Informationsgewinnung ausgenutzt – wird, begründet die Eingriffsqualität, dies dann mit einfachem Eingriffsgewicht, insoweit also bereits von § 16 eröffnet. § 17 trägt Sachverhalten Rechnung, in denen solches schutzwürdiges Vertrauen sogar noch vertieft besteht.

Eine solche spezielle Gewichtung ist angezeigt, wenn basierend auf einem aufgebauten persönlichen Vertrauensverhältnis die Internet-Kontakte realweltlich flankiert werden oder wenn eine wiederholte wirtschaftlich Unterstützung erfolgt. Solche Unterstützung kann sowohl Geld- als auch Sachzuwendungen umfassen. Da in den jeweiligen Szenen, Spenden und gegenseitige Hilfeleistungen durchaus üblich sind, wird erfahrungsgemäß erst mit einer mehrfach wiederholten Zuwendung ein Maß an persönlicher Nähe gegenüber einem virtuellen Kommunikationspartner begründet, welches dann wiederum ein vertieftes schutzwürdiges Vertrauen in den Virtuellen Agenten erzeugt. Die Annahme eines vertieften Vertrauens ist daher frühestens ab der dritten relevanten Gewährung von persönlichen Zuwendungen anzunehmen. Den Charakter des Persönlichen gewinnen im Übrigen nicht geschäftsmäßige Routinen wie die Zahlung von Mitgliedbeiträgen oder Spenden für szeneübliche Kampagnen. Solche Zuwendungen erfolgen nicht „zugunsten“ der Zielperson. Das Tatbestandmerkmal setzt vielmehr eine persönliche Zuwendung voraus, die nicht ein

Sachanliegen, sondern gerade die Zielperson persönlich unterstützen soll (und dies eben mehrfach wiederholt, besondere persönliche Nähe aufbauend).

Erst mit solchen Erweiterungen bricht der Vorgang aus den Besonderheiten der Netzkultur signifikant aus und kann damit das persönliche Vertrauensverhältnis spezifisch vertiefen. Im Interesse einer klaren Regelung erfolgt dabei eine Pauschalierung, die mit solcher Flankierung generell die Höherqualifizierung zur erheblich eingreifenden Überwachung verbindet. Dies entspricht auch der Fachlichkeit, die solchen Qualitätssprung typischerweise erst in Sachverhalten spezifischer Vertrauensverdichtung vollzieht.

Der Gesetzentwurf erfasst damit gleichermaßen pauschalierend wie anwendungs- und kontrollfreundlich inhaltlich bestimmt die praxisrelevanten Sachverhalte, die spezifisch bei Internetermittlungen eine vertiefte Vertrauensbasis schaffen. Nicht vollständig auszuschließen ist, dass in sehr besonderen Vorgängen auch andere Umstände zu solcher Vertrauensvertiefung führen. Es liegt aber einerseits in der Gesetzgebungsfunktion, auch Pauschalierungen zu treffen. Andererseits enthält § 29 eine allgemeine Auffangregelung für sehr außergewöhnliche Einsatzfälle. Eine unbestimmte Öffnung unmittelbar in § 17 selbst würde hingegen den Eindruck eines breiteren Anwendungsspektrums vermitteln, Rechtsunsicherheit schaffen, speziell die Gesetzesanwender verunsichern, ohne dass dies bei einer Gesamtbetrachtung für eine angemessene Regelung des Einsatzmittels zwingend ist. Deshalb wird hier von solcher – sachwidrigen – Öffnung abgesehen.

Ein sogar über das erhebliche hinausgehende, nochmals besonders erhebliches Eingriffsgewicht wird mit der Maßnahme allerdings auch nicht bei punktueller realweltlicher Flankierung oder verstetigter wirtschaftlicher Unterstützung erreicht. Denkbar wäre allenfalls, dass sich der Fall in eine Richtung entwickelt, der eine Voll-Legendierung des Bediensteten mit einer auf Dauer angelegten umfassenden biographischen und real-weltlichen Absicherung erfordert. Eine solche Maßnahme wäre dann im Weiteren an § 19 zu messen. Die Abgrenzung in der Qualifikation des Einsatzmittels erfolgt dabei nach dem Schwerpunkt der Ausgestaltung (virtuell mit realweltlicher Flankierung oder realweltlich mit virtueller Ergänzung), wofür ein aussagekräftiger Indikator auch die Ausstattung des Bediensteten mit einer Volllegende (und deren umfassende Unterlegung mit Tarnpapieren) ist.

Die Qualifikation der erheblichen Beobachtungsbedürftigkeit bezieht sich auf das Beobachtungsobjekt. Dies kann auch ein Verdachtsfall sein, also ein Sachverhalt, in dem die Erkenntnislage noch nicht gesichert ist, auch hinsichtlich der Qualifikation der Bestrebungen. Im Verdachtsfall bezieht sich die Qualifikation darauf, dass der Verdacht der erheblichen Beobachtungsbedürftigkeit begründet ist. Dies kann beispielsweise den Indikator des erheblichen Aktionspotenzials nach § 3 Absatz 6 Satz 3 Nummer 2 betreffen, wenn Anhaltspunkte für solches Potenzial bestehen, die Erkenntnislage aber eben noch nicht gesichert ist, sondern dahingehend womöglich gerade auch unter Einsatz nachrichtendienstlicher Mittel aufgeklärt werden soll.

Vorausgesetzt ist wenigstens erhebliche Beobachtungsbedürftigkeit. Mithin dürfen natürlich – erst recht – sogar besonders erheblich beobachtungsbedürftige Bedrohungen unter solchem Ein-satz von realweltlich flankierten Internetermittlungen aufgeklärt werden.

Die Erlaubnis zum Einsatz nachrichtendienstlicher Mittel dient dem herausragenden Gemeinwohlinteresse an den Verfassungsschutzgütern und hat danach auch einen limitierten Rechtfertigungsgehalt bei Kollision mit anderen rechtlich geschützten Interessen. Dies schließt szenetypische Straftaten wie etwa die Verwendung von Kennzeichen verfassungswidriger Organisationen ein.

Zu § 18 (Vertrauenspersonen)

Die Regelung entspricht dem bisherigen § 9b. Neu sind insbesondere die Absätze 2 bis 4. Der bisherige allgemeine Anwendungsausschluss für die Aufgabe nach dem bisherigen § 3 Absatz 1 Nummer 2 (Spionageabwehr, vgl. dazu noch BT-Drs. 18/4654, S. 26) wird

aufgegeben. Für die personellen Anforderungen nach Absatz 1 muss daran aber festgehalten werden (Anwendung nur auf die Aufklärung von extremistischen Bestrebungen), weil der staatliche Gegner andere Anforderungen an das Einsatzmittel stellt. Setzt er bestimmte Personen für seine Zwecke ein, muss es dem BfV möglich sein, sie zu überwerben. Die Absätze 2 bis 6 gelten aber nunmehr ohne diese Einschränkung auf Extremismusaufklärung.

Zu Absatz 1

Der Absatz übernimmt die VP-Standards des bisherigen § 9b Absatz 2. Mit diesen Qualitätsstandards löst der Gesetzgeber besondere Kollisionslagen zwischen fachlichen Interessen an Informationsgewinnung und widerstreitenden Belangen. Eine solche Kollisionslage tritt nicht auf bei den originären Anforderungen der Fachlichkeit wie der Vertraulichkeitswahrung und Ehrlichkeit sowie der Steuerbarkeit der Vertrauensperson. Dies ist in der Praxis aus den Anforderungen der Fachlichkeit heraus gewährleistet, ohne dass dies eine gesetzgeberische Anleitung erfordert.

Gegenüber der bisherigen Regelung erfolgt nun in Satz 1 eine Klarstellung zur Entscheidungsdelegation. Der bisherige § 9b Absatz 2 Satz 1 sah für die Verpflichtung eine Entscheidung auch durch einen Vertreter vor. Damit war nicht eine Abwesenheitsvertretung gemeint (die auch bei persönlicher Entscheidungszuständigkeit des Behördenleiters gegeben wäre, vgl. BT-Drs. 18/5415, S. 11), sondern Entscheidungsdelegation. Nach dem Normzweck ist dabei allerdings in jedem Fall eine hohe Funktionsebene zu wahren. Eine Delegation auf einen Gruppenleiter/Unterabteilungsleiter würde dem nicht mehr genügen. Im Interesse der Normenklarheit wird die Delegation nunmehr gesetzlich ausdrücklich auf der Abteilungsleiterebene abgeriegelt.

In Satz 3 werden zusätzliche, eng begrenzte Ausnahmemöglichkeiten aufgenommen. Zum einen soll auch die Gewinnung von Vertrauenspersonen ab dem 16. Lebensjahr eröffnet werden, wenn dadurch besonders erheblich beobachtungsbedürftige Bedrohungen aufgeklärt werden. Im Bereich rechtsextremistischer Parteien ist teilweise ein beachtlicher Zulauf von Jugendlichen zu beobachten, etwa bei der Partei „Der III. Weg“ mit der Jugendorganisation „Nationalrevolutionäre Jugend“ auch in eigenen Organisationsstrukturen. In solchen Ausnahmefällen von Sechzehn- oder Siebzehnjährigen ist in besonderer Weise die Verhältnismäßigkeit zu berücksichtigen, was in der Ausnahmeregelung aber auch angelegt und mit dem Leitungsvorbehalt auch besonders gesichert ist. Flankierend wird eine spezielle Fürsorgepflicht gesetzlich hervorgehoben, die mit der Führung minderjähriger Vertrauenspersonen notwendig einhergeht.

Außerdem wird eine Ausnahme auch von Satz 2 Nummer 2 eröffnet. Die Regelung dient einer abstrakten Qualitätssicherung, da vitale Abhängigkeit von Zuwendungen das Risiko bergen könnte, dass zu deren Sicherung auch erfundene Informationen weitergegeben werden, um „im Geschäft“ zu bleiben. Da solches Risiko allerdings deutlich vom Einzelfall abhängt, dabei nötigenfalls auch durch geeignete Maßnahmen beherrschbar bleibt und andererseits in Sonderkonstellationen ein pauschaler Anwerbungsausschluss nicht nur überschießend, sondern auch mit einem gewichtigen Erkenntnisausfall verbunden sein könnte, wird eine verbesserte Flexibilität zur angemessenen Behandlung des jeweiligen Einzelfalls geschaffen. Dabei gibt das Gesetz bindend eine zeitliche Begrenzung vor, bleibt aber bei der zeitlichen Bemessung wiederum flexibel. Regelmäßig wird auch eine solche VP-Führung mehrjährig erfolgen.

Zur Prüfung der rechtlichen Voraussetzung der Unerlässlichkeit muss auch im Verfahren der Vorabkontrolle gegenüber dem Unabhängigen Kontrollrat in allgemeiner Form auf die tragenden Erwägungen eingegangen werden. Das Verfahren der Vorabkontrolle dient dabei der Freigabe des Einsatzmittels, ist also nicht auf die individuell eingesetzte Person bezogen und vermeidet Angaben, die die Feststellung deren Identität ermöglichen (§ 13 Absatz 4 UKRat-Gesetz). Dem könnte dadurch Rechnung getragen werden, dass in einem

Anordnungsverfahren bezogen auf ein (besonders erheblich beobachtungsbedürftiges) Beobachtungsobjekt eine Einsatzfreigabe auch von minderjährigen Personen erteilt wird, dies unter Darstellung der Unerlässlichkeitsgründe. Angaben zu konkreten Einsätzen oder bestimmten Personen sind auch hier also nicht erforderlich.

Zu Absatz 2

Absatz 2 folgt der neuen Systematisierung durch Stufen der Beobachtungsbedürftigkeit. Der Einsatz wird dabei auf wenigstens erheblich beobachtungsbedürftige Bedrohungen beschränkt. Das Eingriffsgewicht des Einsatzes von Vertrauenspersonen kann allerdings deutlich variieren. Es kommt dafür auf die konkrete Ausgestaltung der Maßnahme an, speziell auch, welche Intensität die Beziehungen erlangen, wobei insbesondere die Dauer des Einsatzes maßgeblich ist (vgl. BVerfGE 162, 1 - Rn. 341, 353). Von Bedeutung sind sowohl die quantitative als auch die qualitative Intensität der Kommunikation, beispielsweise ob Kontakte nur einmal im Monat in einer Sitzung eines größeren Gremiums stattfinden oder der Einsatz nur organisationsbezogen erfolgt.

Wird eine Vertrauensperson zur Aufklärung von erheblich beobachtungsbedürftigen Bestrebungen eingesetzt, ergeben sich dabei aber gelegentlich auch Kontakte zu Beobachtungsobjekten, die diese Schwelle nicht erreichen oder die von der Anordnung nicht erfasst sind, können bei diesen Gelegenheiten auch Informationen zu diesen anderen Beobachtungsobjekten mit gesammelt werden. Das darf aber nicht zu einer Umgehung der Einsatzanforderungen (Schwelle der erheblichen Beobachtungsbedürftigkeit, Erfordernis besonderer Anordnung) führen. Solche Beschaffungsaufträge „bei Gelegenheit“ dürfen mithin nicht gezielt zu einer faktisch dauerhaften Überwachung dieses anderen Beobachtungsobjekts durch VP eingesetzt werden. Dies ist nicht der Fall, wenn das (erheblich beobachtungsbedürftige) Beobachtungsobjekt auch hinsichtlich seiner Beziehung zu anderen (weniger gewichtigen) Beobachtungsobjekten, beispielsweise seine Einflussnahme auf diese, aufgeklärt wird, wozu naturgemäß auch letztere in den Blick zu nehmen sind.

Werden berechtigte Vertraulichkeitserwartungen ganz besonders beeinträchtigt, erreicht der Einsatz besonders erheblich eingreifende Qualität. Deshalb beschränkt Satz 2 den Einsatz bei Gewinnung von Informationen von einer Person, zu der die Vertrauensperson eine besonders persönliche Vertrauensbeziehung unterhält, auf die Aufklärung besonders erheblich beobachtungsbedürftiger Bestrebungen. Abzugrenzen ist dies von den noch intensiveren Intimbeziehungen oder vergleichbar engsten persönlichen Bindungen, die einen Ausschlussgrund nach Absatz 4 bilden.

Die Qualifikation als besonders persönliche Vertrauensbeziehung hebt sich von engen Vertrauenskontakten, die bereits allgemein einsatzprägend sind, ab. Dies kann etwa bei vertrauensvollen Beziehungen in langen, intensiven Freundschaftsbeziehungen der Fall sein oder auch in engen Verwandtschaftsverhältnissen (soweit diese noch nicht die Kernbereichsqualität nach Absatz 4 erreichen, wie etwa bei Geschwistern, wenn sie in engem Kontakt – vor allem im selben Haushalt – leben: BVerfGE 165,1 – Rn. 102). Die konkrete Würdigung kann nur nach Maßgabe der speziellen Umstände des jeweiligen Einzelfalls erfolgen. Beispielsweise kann bei Bestrebungen, die auf abgeschotteten Clanstrukturen aufbauen, auch eine enge Beziehung womöglich auf allgemeinen subkulturellen sozialen Normen und nicht einer besonderen persönlichen Bindung aufbauen. Die Enttäuschung eines solchen subkulturellen Kodex ist kein im Sinne dieser Norm qualifizierender Vertrauensbruch.

Eine besondere persönliche Beziehung ist ferner zu unterscheiden von einer wirtschaftlichen Abhängigkeit, der Unterstützung im Alltag oder sonstigen alltäglichen Beziehungen, etwa der Nachbarschaft (auch in Gemeinschaftsunterkünften), Freizeitaktivitäten oder einem Freundeskreis.

Unmaßgeblich sind auch frühere besondere persönliche Beziehungen, beispielsweise eine vormalige, aber zwischenzeitlich zerrüttete besondere Beziehung.

Die Einsatzregelungen unterscheiden grundsätzlich nicht zwischen der Probephase einer Person, die bei Bewährung als Vertrauensperson verpflichtet werden soll, und dem Einsatz nach Verpflichtung. Dies schließt die Rechtfertigung von einsatzbedingten Handlungen nach Absatz 5 Satz 3 ein, da sie ebenso in der Probephase auf der staatlichen Steuerung beruht. Die Rechtfertigungswirkung lässt die Vertrauensperson an der Rechtmäßigkeit des – einsatzsteuernden – staatlichen Handelns teilhaben. Sie ist danach auch nicht von einem subjektiven Element der Vertrauensperson abhängig. Wenn das BfV seinerseits im Kontakt mit der Vertrauensperson unter Legende tätig ist, bleibt dies für die strafrechtliche Rechtfertigung des VP-Handelns unerheblich.

Zu Nummer 1

Im Praktikabilitätsinteresse wird pauschalierend eine einheitliche Zeitschwelle von 6 Monaten für das Erreichen erheblichen Eingriffsgewichts und korrespondierend das Erfordernis erheblicher Beobachtungsbedürftigkeit festgelegt. Diese Frist berücksichtigt zwei für die Informationsgewinnung und -weitergabe und zugleich für die Eingriffstiefe entscheidende qualitative Faktoren: Die Vertiefung der Beziehung zwischen der VP und Szeneangehörigen und die Vertiefung der Beziehung zwischen der VP und der Behörde. Beide Ebenen müssen qualitativ ausgeformt sein, damit ein VP-Einsatz eine erhöhte Eingriffsschwelle erreicht, was insgesamt typischerweise nach einer Einsatzdauer von 6 Monaten anzunehmen ist. Damit trägt die Regelung dem Umstand Rechnung, dass die erste Phase eines VP-Einsatzes von jeweils sehr unterschiedlich geprägten Ausgangspunkten bzw. Entwicklungen auf beiden Kontaktebenen determiniert ist. Diese erste Phase umfasst sowohl Fälle, in denen eine VP an eine Szene herangespielt wird, als auch solche, in denen eine VP, die bereits in der Szene vernetzt ist, für eine Zusammenarbeit gewonnen werden kann. Die Zeitschwelle bezieht danach beide Aspekte ein, sowohl die systematische Beschaffungszusammenarbeit mit dem BfV (durch dessen Beschaffungsaufträge) wie auch den Vertrauensaufbau im Aufklärungsfeld. Letzteres ist speziell für das aufwändige Anordnungsverfahren mit unabhängiger Vorabkontrolle bedeutsam, wenn eine Quelle als „Springer“ in verschiedenen Aufklärungsfeldern mit jeweils nur punktuellen Aufträgen eingesetzt wird, die dann typischerweise nicht zu vertieften Vertrauensbeziehungen führen. Im Übrigen wird jedoch auf differenziertere Regelungen – etwa gestuft verlängerte Zeitschwellen bei wenigen Kontakten in einem Aufklärungsfeld oder dem Verzicht auf konkret personenbezogene Aufträge – verzichtet. Solche kleinteilige Regelung wäre kaum inhaltlich bestimmt und in praktikabler Weise möglich.

Das Aufklärungsfeld ist der Bereich einer verfassungsfeindlichen Szene der mit dem Einsatz aufgeklärt werden soll und ensprechend die – sicherheits-/funktionsgefährdenden oder geheimdienstlichen – Tätigkeiten, die jeweils von der VP aufgeklärt werden sollen.

Zu Nummer 2

Die Regelung beschränkt den VP-Einsatz gegen Zusammenhangs-Personen unabhängig von der Einsatzdauer auf Fälle erheblicher Beobachtungsbedürftigkeit, weil diese Personen zwar wegen des Aufklärungserfordernisses, dabei aber quasi als „Nicht-Störer“ in Anspruch genommen werden. Dies begründet eine modifizierte Verhältnismäßigkeitsrelation mit höheren Rechtfertigungsanforderungen (vgl. bereits § 16 Absatz 5 Satz 4: grundsätzlicher Ausschluss besonders erheblich eingreifender Maßnahmen).

Zu Absatz 3

Absatz 3 enthält einen Einsatzausschluss komplementär zum Schutz von Berufsgeheimnissen nach § 32. Ein solches, gesetzlich herausragend geschütztes Vertrauensverhältnis darf nicht zur Informationsbeschaffung durch Einsatz des Geheimnisträgers unter Bruch des Vertrauensverhältnisses instrumentalisiert werden.

Zu Absatz 4

Der Absatz ergänzt die allgemeinen Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung in § 31 um spezielle Maßgaben zum besonderen Einsatzmittel einer Vertrauensperson (sowie in Verbindung mit § 18 eines Verdeckten Bediensteten). Die allgemeinen Bestimmungen in § 31 gelten mithin ebenso beim Einsatz von Vertrauenspersonen. Dies gilt zur Maßnahmeunterbrechung, wenn bei ihrer Durchführung Anhaltspunkte für Kernbereichsinformationen anfallen (§ 31 Absatz 2), sowie zur Prüfungs- und Löschungspflicht (§ 31 Absatz 4 und 7).

Bereits allgemein unzulässig ist die gezielte Erhebung von Kernbereichsinformationen (§ 31 Absatz 1 Satz 1). Die Regelung in Absatz 4 Satz 1 konkretisiert den Kernbereichsschutz mit einem vorbeugenden Ausschluss der Instrumentalisierung solcher Vertrauensbeziehungen, in denen geradezu zwangsläufig solche Informationen gewonnen würden (BVerfGE 165, 1 – Rn. 107, 110). Eine solche Vertrauensbeziehung ist nicht zwangsläufig bereits anzunehmen, wenn es zu einer (insbesondere einmaligen) körperlichen Intimität kommt, sondern erst dann, wenn eine schutzwürdige emotionale und höchstpersönliche Bindung vorliegt oder hergestellt werden soll. Die Vertrauensbeziehung besteht zugleich auch nur solange, wie diese besondere Bindung besteht. Eine vormalige, aber nicht fortbestehende Partnerschaft, etwa bei einer zerrütteten Ehe, bedingt keinen Kernbereichsschutz, darf aber auch nicht im instrumentellen Wiederaufleben für Aufklärungszwecke eingesetzt werden.

Das Verbot schützt diese sehr intensive Nähebeziehung und beschränkt sich nach diesem Zweck zugleich auf sie. Besitzt eine Vertrauensperson etwa eine solche Beziehung zu einer Person in einem aufzuklärenden Personenzusammenschluss, dann darf sie nicht zur Gewinnung von Informationen über diese Person, sehr wohl aber zur Aufklärung des Beobachtungsobjekts im Übrigen eingesetzt werden. Allerdings ist im Lichte der grundrechtlichen Garantie der Menschenwürde ausgeschlossen, dass der Staat eine für ihn tätige Person zur Eingehung intimer Beziehungen anhält, um damit staatliche Aufklärungszwecke zu verfolgen, sei es auch mit einer Aufklärungsrichtung, die nicht gegen den Intimpartner gerichtet ist, sondern diese Partnerschaft instrumentell zum Zugang zu einem Beobachtungsobjekt betreibt. Umgekehrt nicht erfasst sind sonstige private Beziehungen jenseits solcher intimen oder vergleichbaren Qualität, einschließlich eines familiären Einschlusses, wie beispielsweise der Einbezug bei der Kinderbetreuung. Dass solche Nähe- und Vertrauensbeziehungen ein erhöhtes Risiko bergen, dass andere Personen von sich aus auch Kernbereichsinformationen offenbaren, begründet keinen grundsätzlichen Einsatzausschluss, sondern stellt Anforderungen an die Einsatzführung (nicht darauf hinsteuernd und solche Situationen möglichst vermeidend) und die Weiterverarbeitung solcher ungezielt anfallender Informationen (die Weiterverarbeitung ist ausgeschlossen).

Bereits allgemein in § 31 Absatz 1 Satz 2 sind Vorgaben zur Einsatzplanung geregelt, besonders kernbereichsgeneigte Einsatzsituationen zu vermeiden. Dies reguliert die staatliche Einsatzsteuerung. Hieraus erwächst kein Erfordernis, Beschaffungsaufträge an Vertrauenspersonen situativ in der Einsatzführung durch das BfV durchzuplanen (was weithin auch unpraktikabel wäre – Aufträge werden grundsätzlich mit Bezeichnung des Erkenntnisziels erteilt). Die Einsatzvorgabe greift auch nicht in die private Lebensgestaltung der Vertrauensperson über, die sich regelmäßig nicht lediglich einsatzgesteuert in einem Lebensumfeld bewegt, sondern dort ebenso ihr – nicht einsatzbestimmtes – Privatleben realisiert.

Erlangt eine Vertrauensperson im Einsatz Kernbereichsinformationen, darf sie sie nicht an das BfV weitergeben, darauf hat das BfV hinzuwirken (Absatz 4 Satz 3). Auch hier ist allerdings die Vertrauens- und Führungssituation zwischen der Vertrauensperson und der fallführenden Person des BfV zu berücksichtigen. Der Einsatz kann für die Vertrauensperson psychisch sehr belastend sein, gerade wenn ihr im Vertrauen ganz besonders persönliche Informationen anvertraut werden. Es ist für die Zusammenarbeitsbeziehung wichtig,

dass sich die Vertrauensperson auch über solche Belastungen mitteilen kann und ein solches Gespräch nicht etwa von der Fallführung einseitig beendet wird.

Erlangt das BfV Kernbereichsinformationen, hat es sie nach § 31 Absatz 7 zu löschen. Dies betrifft physisch gespeicherte Daten. Werden Informationen lediglich mündlich übermittelt, ergibt sich daraus ein Weiterverarbeitungsverbot. Der materiellen Pflicht korrespondiert verfahrensmäßig – wie allgemein bei Verwaltungshandeln – eine entsprechende Prüfungspflicht, ob Informationen kernbereichsrelevant sind (BVerfGE 165, 1 - Rn. 118), ohne dass dies spezieller gesetzlicher Regelung bedürfte.

Zu Absatz 5

Absatz 5 übernimmt den bisherigen § 9a Absatz 2 zu Verdeckten Bediensteten, die bereits nach bisherigem Recht nach § 9b Absatz 1 Satz 1 ebenso für Vertrauensleute anzuwenden waren. Wegen der besonderen Sachnähe bleibt die spezielle Regelung im speziellen Regelungszusammenhang der Vertrauenspersonen und Verdeckten Bediensteten. Inhaltlich handelt es sich um Konkretisierungen der allgemeinen querschnittliche Regelungen in § 15 Absatz 5 und § 27. Dies betrifft nicht nur den Einsatz anderer nachrichtendienstlicher Mittel (etwa den Einsatz von Internetquellen, u.a. nach § 16), sondern ebenso das Einsatzgeschehen von Vertrauenspersonen (oder Verdeckten Bediensteten, § 18) hinsichtlich der hieran im BfV Beteiligten. Das kann die Fallführung betreffen ebenso wie administrative Unterstützung, etwa wenn sich ein Verdeckter Bediensteter an Spendensammlungen im obligaten (begrenzten) Umfang beteiligen muss und dazu von innerbehördlichen Verwaltungsbediensteten Haushaltsmittel einzusetzen sind.

Wenn ein Strafverfahren infolge der Tatrechtfertigung nach Absatz 5 (oder aufgrund Absatz 6) eingestellt wird, liegt in der Natur der Sache, den Zusammenhang mit einem verdeckten Einsatz nicht transparent zu machen. Dazu wird die Bundesregierung eine Klarstellung in Nr. 89 RiStBV bzgl. der Begründung einer Einstellung nach Absatz 6 in einer Einstellungsmitteilung anstreben. In diesen Fällen ist der Hinweis auf fehlendes öffentliches Interesse sachgerecht. Auch zum Akteneinsichtsrecht kann dem Anliegen im Rahmen des geltenden Rechts durch angemessene Verfahrensgestaltung Rechnung getragen werden.

Zu Absatz 6

Die Regelung greift den bisherigen § 9a Absatz 3 (i.V.m. § 9b Absatz 1 Satz 1) auf und passt das Bundesverfassungsschutzgesetz nunmehr zugleich an den neuen § 13 Absatz 5 MAD-Gesetz an, der alle Einsätze erfasst, ohne die Beschränkung des bisherigen § 9a Absatz 3 Satz 1 Nummer 1. Die gebotene Abwägung erfolgt ohnehin nach Absatz 6 Satz 2 (in einer bereichsspezifischen Konkretisierung der allgemeinen Regelung des § 153 Absatz 1 Satz 1 StPO).

Zu Absatz 7

Eine verdeckte Tätigkeit birgt große Risiken für die eingesetzten Personen und ggfs. auch deren enges familiäres Umfeld. Eine Enttarnung kann handgreiflichen Racheaktionen der Szene oder eines fremden Nachrichtendienstes nach sich ziehen, die die eingesetzten Personen an Freiheit, Leib und Leben bedrohen. Weitere Gefahren sind soziale Isolation bis hin zum völligen Abbruch des normalen Lebens bei Aufnahme in ein Schutzprogramm aufgrund massiver Bedrohung. Der eingesetzten Person gegenüber besteht die Verpflichtung, sie bestmöglich vor einer Enttarnung zu schützen.

Die Regelung umfasst auch die Möglichkeit, in gerichtlichen Verfahren die verdeckte Tätigkeit zu leugnen, wenn dies zur Eigensicherung der Person notwendig ist. Eingeschlossen sind auch Informationen, die die Zusammenarbeit offenbaren würden, etwa die Angabe von Geldzuwendungen des BfV im Verfahren der Privatinsolvenz.

In einer Güterabwägung ausgenommen sind jedoch parlamentarische Verfahren und Strafverfahren, wobei in Strafverfahren stattdessen ein Beweisthemaverbot begründet wird. Dies betrifft nicht die Sacherforschung der prozessualen Tat, sondern allenfalls die Beweiswürdigung von Einlassungen einer Person.

Zu § 19 (Verdeckte Bedienstete)

Zu Absatz 1

Der Paragraph behält die bisherige inhaltliche Synchronisierung der Regelungen zu Verdeckten Bediensteten (bisher § 9a) und Vertrauenspersonen bei. Wie beim VP-Einsatz ist die Einsatzanordnung zu unterscheiden von einzelnen im Einsatzrahmen erteilten Beschaffungsaufträgen. Nicht einbezogen sind mithin Beschaffungsmaßnahmen, die nur flankierend zu anderen operativen Maßnahmen in unregelmäßigen Zeitabständen und anlassbezogen, also eben nicht langfristig erfolgen. Ebenso bleiben punktuelle „Springer“-Maßnahmen, die nur zeitlich eng begrenzte, jedenfalls unterhalb der Einsatzschwelle von 6 Monaten bleibende Gelegenheiten zu Kurzkontakten nutzen, außerhalb der materiellen und verfahrensbezogenen Voraussetzungen des § 18.

Satz 2 trägt einer ausdrücklichen Maßgabe des Bundesverfassungsgereichts (BVerfGE 169, 130 – Rn. 191) Rechnung. Das Gericht nimmt dort ein qualifiziertes Eingriffsgewicht auch unabhängig von einer längeren Einsatzdauer (also abgelöst von der Voraussetzung nach § 17 Absatz 2 Nummer 1) an, wenn ein personenbezogener Einsatz auf die Herstellung einer Vertrauensbeziehung angelegt ist. Erfolgt der auf eine Person zielende Einsatz ohne eine vertiefte interpersonale Vertrauensbeziehung, etwa lediglich in einem kollektiven Rahmen, wird das Qualifikationsmerkmal nicht erfüllt.

Im Übrigen sind die vorstehenden Erwägungen des Gerichts zum Einsatz Verdeckter Bediensteter nicht auf Vertrauenspersonen übertragbar. Bei Vertrauensleuten ist zunächst die Verlässlichkeit der Quelle im Einsatz zu erproben und ein wechselseitiges Vertrauensverhältnis als Grundlage staatlicher Einsatzsteuerung aufzubauen. Diese vorlaufenden Besonderheiten des VP-Einsatzes sind sachliche Unterschiede, die auch eine unterschiedliche Gewichtung des Eingriffsgehalts auf der Zeitachse mit einer pauschalierend angesetzten Anlaufphase der Erprobung rechtfertigen,

Im Übrigen formuliert das Gericht Anforderungen zur Eingriffsschwelle und trifft keine Vorgaben zur unabhängigen Vorabkontrolle. Diese ist nicht kurzschlüssig mit der materiellen Schwelle verknüpft, sondern davon abhängig, dass auch höchstprivate Informationen erwartbar sind (siehe nachfolgend zu § 34). Das bloße Angelegt-Sein auf die künftige Herstellung von Vertrauensbeziehungen (materielle Schwelle) lässt jedoch noch nicht sogleich auch mit dem Austausch höchstprivater Informationen rechnen, vielmehr ist Voraussetzung dafür eine tatsächlich hergestellte vertiefte Vertrauensbeziehung, die typischerweise erst über einen geraumen Zeitraum aufzubauen ist. Für das Erfordernis der Vorabkontrolle kann es also bei der 6-Monats-Schwelle bleiben. Neben den angeführten Sacherwägungen sprechen dafür auch praktische und Wirtschaftlichkeitserwägungen. Der hohe Verfahrensaufwand sollte möglichst nicht bereits in einem Stadium anfallen, wenn noch offen ist, ob es überhaupt gelingt, die Quelle erfolgreich im Aufklärungsfeld zu platzieren.

Zu Absatz 2

Die Regelung entspricht § 110c Satz 1 und 2 StPO. Von einer entsprechenden Regeleung zu verdeckt ermittelnden Hilfspersonen kann weiter abgesehen werden, da in ihrem Fall beim geregelten Sachverhalt kein hoheitliches Handeln vorliegt.

Zu § 20 (Längerfristige optische und akustische Überwachung)

Die Regelung trägt dem Umstand Rechnung, dass das Eingriffsgewicht von Observationen sehr unterschiedlich sein kann (BVerfGE 162, 1 - Rn. 357). Die Grundbefugnis zur

Observation ergibt sich bereits unmittelbar aus § 15. § 19 ergänzt diese Grundnorm, indem typischerweise eingriffsqualifizierende Umstände an dazu adäquat angehobene Einsatzschwellen gebunden werden.

Für die Qualifikationskriterien der Maßnahmedauer in Absatz 1 Nummer 1 und Absatz 2 Nummer 1 ist dabei jeweils entscheidend, dass die Maßnahme personengerichtet durchgeführt wird. Wird beispielsweise ein Objekt stationär auch längerfristig überwacht, um festzustellen welche Personen sich dort einfinden, ist die Dauer kein Indikator dafür, dass hierbei jeweils gewichtige Eingriffe in die informationelle Selbstbestimmung dieser Personen erfolgen, die dann eben nur punktuell an diesem Ort, also ohne breite Erkenntnisse zur Persönlichkeit erfasst werden. Gleiches gilt, wenn die stationäre Beobachtung gegen eine bestimmte Person gerichtet ist, da hier eben nur ein sehr enger, lokaler Ausschnitt – auch bei längerfristiger stationärer Beobachtung – im Blick ist. Die Dauer indiziert qualifizierte Gewichtigkeit nur bei ortsunabhängiger, der Person folgender Observation. Dies wird mit dem Begriff „durchgehend“ tatbestandlich erfasst. Durchgehend meint unterbrechungsfrei. Die Schwelle kann aber nicht gezielt durch Unterbrechung umgangen werden. Maßgeblich ist, ob die Unterbrechungen aus fachlich nachvollziehbaren Gründen erfolgt, etwa weil nur bestimmte Zeitfenster überwachungsrelevant sind, weil nur bestimmte Situationen überwacht werden sollen. In solchen Fällen ist die Unterbrechung beachtlich, unabhängig davon, ob hierbei andere Überwachungsmaßnahmen (wie technische Spurfolge oder Ortsüberwachung) fortlaufen, die dann an ihren Voraussetzungen zu messen bleiben. Ergäbe sich – in praxisfernen Szenarien – eine additive Gesamtwirkung, die in Zusammenschau verschiedener Einsatzmittel hinsichtlich des Umfangs der Persönlichkeitserfassung wiederum einer durchgehenden Observation gleichkäme, wäre Folge, dass am Maßstab des § 27 Absatz 3 unter konkretisierender Berücksichtigung der Wertentscheidungen in § 19 dessen Schwelle erreicht sein muss.

Bei der Eingriffsgewichtung der Observation ist jeweils bereits der eingriffserschwerende Umstand einbezogen, dass zur wirksamen Beobachtung technische Hilfsmittel wie Kamera oder Richtmikrofon eingesetzt werden und zur erleichterten Auswertung hiermit ggf. Aufzeichnungen gefertigt werden. Dies entspricht der Einsatztypik. Eine differenzierende Regelung, die Observationen erleichtert ohne solche Mittel zulässt oder einen unterschiedlichen Unterstützungseinsatz solcher Mittel differenzierend regelt, ginge an Praxisanforderungen vorbei und wäre mithin unnötig kompliziert. Klargestellt wird dabei lediglich, dass in den Befugnisvoraussetzungen bereits berücksichtigt ist, dass die menschliche Wahrnehmung der observierenden Bediensteten auch technisch geschärft und konserviert werden kann. Dagegen bleibt gesondert an den jeweiligen Voraussetzungen zu würdigen, wenn ohne Observation - auch während einer Observationspause – Technik zur Erfassung bestimmter Informationen eingesetzt wird (z.B. eine stationäre Videoüberwachung bestimmter Orte, an denen der Betroffene erwartet wird, oder eine bloße Bewegungsüberwachung). Dies verlängert nicht die Observation, sondern ist eine eigene, andere Maßnahme. Hier steht allenfalls in Rede, dass additive Effekte in einer Gesamtschau unter Anwendung des § 27 Absatz 3 das Maßnahmebündel aus kürzerer Observation und anschließender partikulärer technischer Überwachung ausnahmsweise nur im Falle besonders erheblicher Beobachtungsbedürftigkeit als gerechtfertigt erscheinen lassen. Derlei Gesamtbetrachtungen können angesichts der Vielgestaltigkeit möglicher Faktoren nicht gesetzgeberisch adäquat kategorisiert werden, sondern müssen im Verwaltungsvollzug gewürdigt werden (BVerfGE 162, 1 – Rn. 287).

Zu Absatz 1

Zu Nummer 1

Zu Buchstabe a

Die Dauer von 48 Stunden greift die Frist des früheren Art. 19a BayVSG auf. Die Regelung ist vom Bundesverfassungsgericht (BVerfGE 161, 1) geprüft worden, ohne dass die Dauer

auf Kritik gestoßen ist. Die Frist betrifft eine durchgängige Observation über diese Dauer, also nicht die zeitliche Summe verschiedener Observation.

Zu Buchstabe b

Mit Buchstabe b werden jedoch eine Mehrzahl von lediglich punktuellen Observationen erfasst, wenn etwa die Zielperson regelmäßig bestimmte Orte aufsucht, etwa Szeneeinrichtungen an bestimmten Tagen zu bestimmten Zeiten, und angenommen wird, dass dort relevantes Geschehen zu beobachten ist.

Die Schwelle der 7 Tage per Monat soll solche punktuellen Überwachungen erfassen. Daneben sind auch weitere atypischen Konstellationen konstruierbar, die in der Zusammenschau einzelner Maßnahmen ein erhebliches Eingriffsgewicht erreichen, ohne dass dies sich solche Atypik in messbare Tatbestandsmerkmale fassen ließe. Solchem atypischen Sachverhalt muss dann unter Anwendung des § 27 Absatz 3 ebenso durch Beschränkung auf erheblich beobachtungsbedürftige Bedrohungen Rechnung getragen werden. Eine zusätzliche allgemeine Auffangregelung, vergleichbar § 21 Absatz 1 Nummer 1 Buchstabe c, ist bei der Observationsbefugnis dagegen im Interesse inhaltlich bestimmter Ausgestaltung verzichtbar, weil hier Buchstabe b) bereits nicht auf eine täglich durchgehende Observation beschränkt ist und in der Natur des Einsatzmittels Aufwände eingeschlossen sind (bei der Voraufklärung der Situation, in der die Observation aufgenommen wird, wie auch in der Heranführung eines Trupps und dessen Absicherung) nach der der Einsatzflexibilität viel engere Grenzen gesetzt sind, als beim Empfangen technischer Signale eines zur Standortüberwachung platzierten Gerätes. Völlig abseitige Einsatzszenarien sind auch bei einer Observation zwar nicht vollständig auszuschließen, werden insoweit dann aber durch die allgemeine Verhältnismäßigkeitsmaßgabe in § 27 Absatz 3 sachgerecht berücksichtigt.

Auch Buchstabe b setzt eine Observation voraus, die in der Situation dem Verhalten der Zielperson flexibel folgt und dadurch bei kumulierten Einsätzen zu qualifizierter Persönlichkeitserfassung geeignet ist. Auch hier wird eine stationäre Überwachungseinrichtung mit dem hieran angelegten bloß punktuellem Erkenntnispotential nicht erfasst. Solche technische Überwachung kann aber in qualifizierten Situationen wegen solchem qualifizierten Einblick unter Umständen ebenfalls erhöht eingreifend sein (Nummer 2).

Zu Nummer 2

Der Einsatz technischer Mittel schafft mit der optischen und akustischen Aufzeichnung eine erweiterte Möglichkeit, das heimlich beobachtete Verhalten umfassend zu erfassen und auch noch nachgängig vertiefend auszuwerten. Zudem erschließt das technische Einsatzmittel Einsatzmöglichkeiten, die bei persönlicher Anwesenheit einer weiteren Person unter Umständen nicht eröffnet wären, wodurch es womöglich Vertraulichkeitserwartungen vertieft verletzen kann. Deshalb kann solcher Einsatz eingriffsqualifizierend sein. Dies betrifft die Überwachung im nichtöffentlichen Raum, etwa bei Insassen eines Personenkraftwagens. Auch im öffentlichen Raum besteht zwar ein schutzwürdiges Interesse, dass eigenes Verhalten nicht Gegenstand gezielter staatlicher Beobachtung ist. Dies ist aber bereits mit der allgemeinen Befugnis zum Einsatz heimlicher Informationsgewinnung durch Einsatz nachrichtendienstlicher Mittel zulässig, auch insoweit nicht voraussetzungslos, sondern an § 16 Absatz 1 gebunden, also die Einzelfallveranlassung zum Schutz besonders gewichtiger Rechtsgüter.

Zu Absatz 2

Absatz 2 bezeichnet gegenüber Absatz 1 nochmals qualifiziertes, besonderes Eingriffsgewicht, das eine Beschränkung auf besonders erheblich beobachtungsbedürftige Bedrohungen erfor-dert.

Bei besonders erheblich eingreifenden Observationen folgt neben der unabhängigen Vorabkontrolle nach § 34 Absatz 1 Satz 1 Nummer 4 auch eine Mitteilungspflicht an die Zielperson nach § 35 Ab-satz 1 Satz 1.

Zu Nummer 1

Mit einer Observation von einer Wochendauer erfolgt eine Überwachung, die unterschiedliche Lebensabläufe an allen Werktagen und dem Wochenende einschließt.

Zu Nummer 2

Video- oder Tonaufzeichnungen erhalten ebenso eine höhere Eingriffsqualität, wenn mit der Erfassung auch von höchstprivaten Informationen zu rechnen ist. Dies ist noch nicht per se bei einer Überwachung im nichtöffentlichen Raum der Fall, der beispielsweise auch geschäftsmäßige Situationen einschließt oder womöglich gezielt zur Verdeckung eines Kontakts gewählt wird, ohne dass dies auf den Austausch höchstprivater Informationen gerichtet wäre.

Zu Absatz 3

Nach Satz 1 gelten die qualifizierte Voraussetzungen der Absaätze 1 und 2 nicht für Fälle der Eigensicherung. Dies betrifft vornehmlich Maßnahmen nach Absatz 1 Nummer 2, die bei der Vorbereitung von Treffs zu ergreifen sein können. Satz 2 stellt klar, dass § 25 eine abschließende Spezialregelung trifft.

Zu § 21 (Längerfristige Bewegungsüberwachung)

Anders als eine Observation durch visuelle oder akustische Überwachung sind mit Maßnahmen der technischen Standortfeststellung nur begrenztere Informationen, eben zum Standort zu gewinnen (nicht zum sonstigen Verhalten oder konkreter sozialer Interaktion), weshalb solche Maßnahmen grundsätzlich weniger eingreifend bleiben.

Erfolgt die Überwachung allerdings nicht nur punktuell oder fragmentarisch, sondern durchgehend und über einen Zeitraum, der über das Bewegungsprofil weitgehende Einblicke in das Privatleben von hoher Persönlichkeitsrelevanz verschafft, sind auch für die Standortüberwachung qualifizierte Schwellen erforderlich.

Die Befugnis würde auch die Aufenthaltsüberwachung mit einem IMSI-Catcher (bisheriger § 9 Absatz 4) einbeziehen, falls sie den Qualifikationstatbestand des § 21 erreicht. Dies kommt in der Praxis allerdings nicht vor, weil das Einsatzmittel nicht zur längerfristigen Dauerüberwachung geeignet ist (in der Praxis ist danach § 16 Einsatzgrundlage und zwar vornehmlich für die Ermittlung der Geräte- oder Kartenummer eines von der Zielperson genutzten Mobiltelefons). Die Standortermittlung über Verkehrsdaten erfolgt mit deren Erhebung nach § 13 Absatz 1 in Verbindung mit Absatz 3, unabhängig davon, ob die Verkehrsdaten womöglich vom BfV mit sogenannter stiller SMS Standortdaten erzeugt worden sind. In diesem Fall kann allerdings womöglich eine Datenbasis für ein Bewegungsprofil gewonnen werden, dessen Erstellung an § 37 Absatz 2 Nummer 3 zu messen und dadurch in den Voraussetzungen mit § 21 synchronisiert wäre. Zielt der Einsatz stiller SMS auf solches Bewegungsprofil, dann ist die Methode nur geeignet, soweit die entsprechenden Auswertungsvoraussetzungen vorliegen. Dadurch wirken die Auswertungsvoraussetzungen bereits vor auf den Einsatz stiller SMS. Die Generierung von Standortdaten ist nicht erforderlich (und damit unzulässig), wenn sie auf eine Erkenntnis zielt, die eine unzulässige Auswertung bedingen würde (so dass die bezweckte Erkenntnis nicht erzielt werden kann).

Die Qualifikationsstufen der Nummern 1 und 2 erfassen jeweils drei Fallgruppen entsprechenden Eingriffsgewichts. In Buchstabe a ist jeweils eine über den Zeitraum zusammenhängende Überwachung vorausgesetzt, die ein geschlossenes Bewegungsprofil ergibt. Dies setzt kein permanentes Standortsignal, aber doch einen engen Zeittakt voraus.

Allerdings führt eine Lücke im Bewegungsprofil nicht zu einer minderen Eingriffsqualifizierung, wenn über einen langen Zeitraum wiederholt durchgängige, wenn auch kürzere Überwachung erfolgt (BVerfGE 169, 130 -.Rn. 146). Dazu trifft Buchstabe b pauschalierende Vorgaben zu gleichwertiger Persönlichkeitsrelevanz. Damit wird die Falltypik weitgehend erfasst. Da die Gestaltungsbreite beim Einsatz des technischen Mittels aber offen für auch andere gleichwertige Eingriffsszenarien ist, enthält Buchstabe c ergänzend eine allgemeine Auffangregelung, die eine Gesamtbewertung der konkreten Ausgestaltung einbezieht, um auch besondere Ausnahmesachverhalte angemessen zu erfassen (beispielsweise wiederum verkürzte durchgängige Zeiträume in einer Vielzahl und zeitlichen Streuung, die eine gleichwertige Gesamtabdeckung über längeren Zeitraum ergeben). Auf solche erheblich wertungsgebundene Auffangregelung wird in den anderen besonderen Befugnisnormen bewusst durch pauschalierende Regelungen im Interesse inhaltlicher Bestimmtheit und Normenklarheit verzichtet. Speziell bei der Anwendungsflexibilität technischer Einsatzmittel nach § 20 würde jedoch der bloße Rückgriff auf § 27 Absatz 3 der höheren Praxisrelevanz auch außergewöhnlicher Anwendungsausgestaltungen icht angemessen gerecht.

Die Befugnis ist für Grundrechtseingriffe durch Erhebung personenbezogener Daten erforderlich. Die Nachverfolgung von Sachen – etwa von Proliferationsgütern über einen angebrachten GPS-Tracker – bedarf keiner Befugnis und erfolgt auf Grundlage der gesetzlichen Aufgabe.

Zu Absatz 1

Zu Nummer 1

Zu Buchstabe a

Bei durchgehender Überwachung über eine volle Woche können aussagekräftige Bewegungsprofile entstehen, die in erheblich eingreifender Weise Persönlichkeitsrelevanz besitzen.

Zu Buchstabe b

Die Regelung trifft eine § 19 Absatz 1 Satz 1 Nummer 1 Buchstabe b entsprechende Regelung, die Sachverhalte erfasst, bei denen punktuelle Einsätze in der Zusammenschau eines größeren Zeitraums gleichwertiges Eingriffsgewicht wie durchgehende Einsätze über einen kürzeren Zeitraum erreichen.

Zu Buchstabe c

Angesichts der hohen Einsatzflexibilität des technischen Überwachungsmittels lässt die Einsatzschwelle nicht vollständig in vertypten Tatbeständen erfassen. Deshalb ist hier eine flexible Auffangnorm erforderlich, die ihrer Funktion nach notwendig nur weniger bestimmt sein kann.

Zu Nummer 2

Zu Buchstabe a

Aus durchgehend einmonatiger Überwachung können Erkenntnisse gewonnen werden, die über Bewegungsprofile nach Nummer 1 hinaus gehen und womöglich auch validierte Bewegungsmuster erkennen lassen. Dies ermöglicht unter Umständen einerseits Schlüsse auf dauerhafte Beziehungen zu bestimmten Orten und mittelbar womöglich auch auf verfestigte Beziehungen zu bestimmten Personen. Andererseits werden selbst atypische, seltenere örtliche Beziehungen miterfasst. Dies hat insgesamt das Potenzial breite Informationen zur Person unter Einschluss auch höchstprivate Informationen zu gewinnen und dadurch besonders erhebliches Eingriffsgewicht.

Zu Buchstabe b

Die Regelung entspricht der Nummer 1 Buchstabe b, hier für das Niveau eines besonders erheblichen Eingriffs.

Zu Buchstabe c

Die Regelung entspricht der Nummer 1 Buchstabe c.

Zu Absatz 2

Die Voraussetzung der durchgehenden Überwachung bezieht sich auf ein Einsatzmittel, das potenziell eine über den Zeitraum zusammenhängende Überwachung ermöglicht, und ist damit abzugrenzen von Einsatzmitteln, die per se bloß eine fragmentarische Überwachung eröffnen. Dies gilt etwa für nicht laufend mitgeführte Gegenstände (z.B. Laptop) oder ein bestimmtes Verkehrsmittel (z.B. Kfz), weil hieraus erfolgende Standortsignale eben nur Ausschnitte der Bewegung nachverfolgbar machen und nicht typischerweise umfassende Persönlichkeitserforschung eröffnen (BVerfGE 169, 130 - Rn. 166, 168). Wenn es sich hingegen um einen Gegenstand handelt, der – wie beispielsweise in breiten Lebenswelten heute ein Smartphone – typischerweise laufend an der Person geführt wird, und die Standortüberwachung über einen relevanten Zeitraum durchgehend erfolgt, so dass aus den gesammelten Daten objektiv ein persönlichkeitsrelevantes Bewegungsprofil erstellbar ist, ist für die Eingriffsgewichtung unerheblich, ob die Maßnahme auch zu diesem Zweck durchgeführt wird (a.a.O. Rn. 145). Maßgeblich ist in jedem Fall die Informationssammlung, nicht bereits die Platzierung eines Geräts, das Signale abgeben kann (ggfs schon deutlich vorlaufend zur Situation, zu deren Aufklärung Standortdaten später benötigt werden). Entscheidend sind also die Phasen, in denen Standortdaten zur Kenntnisnahme erfasst werden (nicht lediglich zur technischen Verarbeitung ausschließlich zur Funktionsprüfung ohne anschließende Weiterverarbeitung). Wegen dieser Einsatzflexibilität sind jeweils auch die Buchstaben b und c in den Nummern 1 und 2 des Absatzes 1 zur angemessenen Erfassung des konkreten Eingriffsgewichts nötig.

Zu § 22 (Überwachung von Brief-, Post- und Telekommunikationsverkehren)

Die neue Regelung ist Folge der Aufhebung des Artikel 10-Gesetzes unter Integration der bisher dort geregelten Befugnisse in das Bundesverfassungsschutzgesetz. Die notwendig ergänzenden Verfahrensregelungen enthalten §§ 33 bis 35, die besonderen Schutzregelungen der bisherigen §§ 3a, 3b G 10 sind nun in §§ 31, 32 eingegangen. Hinzu tritt die neue – professionalisierte - unabhängige Kontrolle durch den Unabhängigen Kontrollrat (der zugleich Kontrolle ganzheitlich, nicht nur sektoral zum bisherigen G 10-Bereich, ausübt). Komplementäre Auskunfts- und Mitwirkungspflichten der Unternehmen enthält § 13, wobei dies wie bisher (§ 10 Absatz 6 Satz 2 G 10) eine zusätzliche Durchführungsgestaltung neben der nach § 22 ebenso möglichen Eigenerhebung auf dem Übertragungsweg ohne Unternehmensmitwirkung ist.

Wird neben dem Telekommunikationsgeheimnis zugleich auch in das IT-Systemgrundrecht eingegriffen, ist nach neuerer Rechtsprechung des Bundesverfassungsgerichts letzteres nicht durch ersteres konsumiert (BVerfG Beschluss vom 24. Juni 2025 - 1 BvR 2466/19 – [Trojaner I] Ls. 3). Insoweit ist dann nicht § 22 lex specialis gegenüber §§ 23 ff., vielmehr kommen die Voraussetzungen kumulativ zur Anwendung. Im praktischen Ergebnis bedeutet dies, dass die ergänzenden Maßgaben nach § 23 Absatz 4 in Verbindung mit § 26 Absatz 6 zur Anwendung kommen.

Eine besondere Zweckbindung für Übermittlungen an Stellen mit operativen Befugnissen (bisher in § 4 Absatz 4 G10) ist dabei angesichts der allgemein hohen Übermittlungsschwellen unnötig (ebenso wie bei den übrigen nachrichtendienstlichen Erhebungsbefugnissen auch mit besonders erheblichem Eingriffsgewicht). Unter Berücksichtigung der konkreten Übermittlungsinhalte schließt dies auch Folgeverwendungen zum administrativen

Rechtsgüterschutz ein, da nicht die Rohdaten der nachrichtendienstlichen Überwachung übermittelt werden, sondern erforderlichkeitsselektierte Auswertungsergebnisse. Die hohe Schwelle der Überwachungsmaßnahme beruht darauf, dass die Maßnahme notwendig breite Teile von Privatheit einbezieht, deren Kenntnis für die legitimierende Aufgabe sachlich nicht erforderlich ist. Dieser notwendig überschießende Gehalt einer überwachenden Gefahrerforschung fällt bei einer Übermittlung von bereits nach Erforderlichkeit ausgewählten Erkenntnissen fort. Für eine Würdigung des Übermittlungseingriffs im Wege eines hypothetischen Vergleichs mit der Zulässigkeit einer empfängerseitigen Telekommunikationsüberwachung wäre mithin eine Befugnis zu betrachten, die ausschließlich die übermittelten Daten mit diesem Mittel gewinnt. Solche Befugnis zur punktuellen Erhebung ausschließlich der für die Aufgabe relevanten Informationen wäre zwar faktisch unpraktikabel, könnte mit ihrem begrenzten Gehalt aber verhältnismäßigkeitswahrend auch zur Risikoaufklärung in den qualifizierten Fällen des administrativen Rechtsgüterschutzes nach § 47 eingeräumt werden. Wenn also bei einer Telekommunikationsüberwachung des BfV Erkenntnisse anfallen, dass die Zielperson eine geheimdienstliche Agententätigkeit für eine fremde Macht ausübt, kann dies ohne Verstoß gegen Verhältnismäßigkeitsanforderungen der zuständigen Stelle im Rahmen einer Sicherheitsüberprüfung mitgeteilt werden.

Die interne Zweckänderung und Übermittlung an einen anderen nachrichtendienstlichen Empfänger ist bereits bisher uneingeschränkt für alle Verfassungsschutzzwecke zulässig (§ 4 Absatz 2 Satz 3 G 10). Dies entspricht der grundsätzlichen Ausrichtung des Prinzips der hypothetischen Datenneuerhebung auf einen Rechtsgütervergleich zwischen dem erhebungslegitimierenden und dem neuen Zweck (der von entsprechendem Gewicht sein muss). Besondere Erhebngsschwellen (bei Telekommunikationsüberwachung: besonders erhebliche Beobachtungsbedürftigkeit) bleiben dagegen grundsätzlich irrelevant, vielmehr genügt, dass die Übermittlung im Einzelfall als Spurenansatz auch für den neuen Zweck veranlasst ist (BVerfGE 141, 220 – Rn. 288 f.). Eine diesen Grundsatz durchbrechende Relevanz besonderer Erhebungsschwellen für Übermittlungen ergibt sich einerseits maßnahmebezogen für die besonders eingriffsintensive Online-Überwachung und Wohnraumüberwachung (a.a.O. Rn. 291). Andererseits haben Übermittlungen auch empfängerbezogen besondere Schwellenvoraussetzungen, nämlich folgenbetrachtend wenn an eine Gefahrenabwehrbehörde mit „operativen“ / „aktionellen“ Befugnissen (zur „polizeilichen“ Intervention, auch mit Zwangsanwendung gegen Personen) übermittelt wird und damit – anders als im Nachrichtendienstbereich - potenziell auch solche Anschlussmaßnahmen drohen (BVerfGE 162, 1 – Rn. 254, 257f., 270). Im Ergebnis ist eine Weiterverarbeitung, von Informationen aus Post- und Telekommunikationsüberwachung, die innerhalb des nachrichtendienstlichen Bereichs verbleibt, auch bei Zweckänderung mithin nicht an besondere Schwellen gebunden, es bleibt aber auch hier dabei, dass der geänderte Zweck vergleichbar gewichtigen Rechtsgütern dienen muss. Dieses Finalitätskriterium ist im nachrichtendienstlichen Aufgabenspektrum jedoch generell gewährleistet (BVerfGE 155,119 – Rn. 151). Demgemäß sind spezielle Zweckbindungen von Erkenntnissen aus Post- und Telekommunikationsüberwachung für eine nachrichtendienstliche Folgeverarbeitung, wenn sie konkret veranlasst ist, unnötig. Die Daten können dann beispielsweise ohne Weiteres auch zur Aufklärung lediglich erheblich beobachtungsbedürftiger Bedrohungen weiterverwendet werden. Das ist ein nicht nur theoretischer Fall, insbesondere weil verschiedene Beobachtungsobjekte auch untereinander in Beziehung stehen, also bei der Aufklärung des einen auch Erkenntnisse zum anderen mit anfallen können.

Mangels besonderer Folgen der Datenherkunft (aus Telekommunikations- oder Postüberwachung) für die Datenweiterverarbeitung ist eine besondere Kennzeichnung der Daten (bisher: § 4 Absatz 2 und 3) künftig als unnötiger Aufwand verzichtbar. Bisherige Sonderschwellen bei der Übermittlung an Behörden mit operativen Anschlussbefugnissen (bisher § 4 Absatz 4 G 10) entfallen infolge der nunmehr bereits generell hohen Übermittlungsvoraussetzungen. Somit ist allein noch die besondere Wiederholungsüberprüfung zur Speichererforderlichkeit nach Absatz 5 organisatorisch zu sichern, was beispielsweise durch entsprechende Wiedervorlage der Aufzeichnungen erfolgen kann.

Zu Absatz 1

Die Regelung greift die bisherige Begrifflichkeit des Überwachens und Aufzeichnens auf. Im Rahmen einer Erhebungsbefugnis wäre eine begriffliche Beschränkung auf die Überwachung naheliegender, da sich die Befugnis zur Aufzeichnung ohne weiteres aus den Weiterverarbeitungsbefugnissen ergibt. Angesichts etablierter Regelungspraxis wird zur Vermeidung von Missverständnissen dennoch daran festgehalten, auch das Aufzeichnen in der Erhebungsbefugnis anzusprechen.

Der Begriff der Überwachung ist hinreichend allgemein, um auch die Überwachung von Postsendungen mit zu erfassen. Die auf das Öffnen und Einsehen von Sendungen bezogene Formulierung des bisherigen § 1 Absatz 1 G 10 ist weniger präzise, da das Postgeheimnis ebenso die Verkehrsdaten (der näheren Umstände) umfasst (§ 206 Absatz 5 Satz 1 StGB).

Dass Überwachungsgegenstand sowohl die Inhalte wie die Umstände der Verkehre sein kann, verdeutlichen Sätze 2 und 3. Satz 2 regelt zu Verkehrsdaten eine spezielle Erhebungsschwelle, Satz 3 bestimmt die Subsidiarität der Inhaltsüberwachung nach § 21 gegenüber anderen Mitteln der Sacherforschung mit Ausnahme der besonders schweren Eingriffe nach §§ 25, 27.

Insgesamt passt der Absatz die Befugnis in das neue Schwellensystem der verfassungsrechtsprechung ein, wonach die Inhaltsüberwachung als besonders erheblich eingreifend, die Verkehrsdatenerhebung (Satz 2 Nummer 1) als erheblich eingreifend qualifiziert wird (vgl. zur Abstufung BVerfGE 141, 220 – Rn. 107). Gewichtungsbegründend bei der Inhaltsüberwachung ist dabei der Einbezug interpersoneller Telekommunikationsdienste (§ 3 Nummer 61 Buchstabe b TKG), weshalb mit Satz 2 Nummer 2 die Überwachung von Internetzugangsdiensten in der Gewichtung noch der Eingriffsklasse der Verkehrsdatenüberwachung zugeordnet wird. Signale einer Maschine-Maschine-Kommunikation sind insgesamt nicht vom Kommunikationsbegriff des Absatzes 2 Satz 1 erfasst, so dass sich die Zulässigkeit ihrer Mitüberwachung gemäß Absatz 2 Satz 2 nach § 23 bzw. im Privatbereich nach § 26 Absatz 1 richtet, woraus sich jeweils ebenso die Schwelle der erheblichen Beobachtungsbedürftigkeit ergibt.

Satz 4 trifft angesichts des Sachzusammenhangs eine Regelung zur Einbringung technischer Mittel wie insbesondere eines GPS-Trackers zur Sendungsverfolgung, speziell bei versendeten Sachen, auch über die Postzustellung hinaus. Dies kann beispielsweise bei der kontrollierten Lieferung von Proliferationsgütern bedeutsam sein. Darüber hinaus umfasst die Regelung die Manipulation einer Sendung, sofern dies der Vorbereitung weiterer nachrichtendienstlicher Maßnahmen dient. Hier kann es zum Beispiel notwendig werden, dass ein im Handel bestelltes IT-Gerät mit einer Software so manipuliert wird, dass hierüber anschließend eine technische Aufklärungsmaßnahme erfolgen kann. Voraussetzung ist jeweils, dass das BfV zum Einsatz des Mittels befugt ist, im Beispielsfall des Eingriffs in ein informationstechnisches System also die jeweiligen Voraussetzungen nach §§ 23, 25, 26 vorliegen. In der Sache wird mithin nur die mit dem Eingriff in das Postgeheimnis eingetretene Gelegenheit genutzt, eine andere Maßnahme unter Wahrung der diebetreffenden Voraussetzungen mit auszuführen. Im Interesse der Normenklarheit wird dies hier dennoch mit geregelt.

Satz 5 übernimmt die bisherige Regelung des § 3 Absatz 2 Satz 5 G 10.

Zu Absatz 2

Der Absatz trägt der neuen Verfassungsrechtsprechung Rechnung (BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 – [Trojaner I] Leitsatz 1), die den Schutzbereich des Artikel 10 GG über den Lebensvorgang der (Fern-)Kommunikation hinaus auf alle mithilfe von Telekommunikationstechniken über Distanz transportierte Daten erstreckt, also beispielsweise die eigene Datenverarbeitung in eigenen Datenverarbeitungsanlagen

einbezieht, wenn sie über Telekommunikationsdienste vernetzt sind. Dies ist grundsätzlich nicht Gegenstand der Kommunikationsüberwachungsbefugnis des § 22 Absatz 1, was zur Vermeidung von Fehlverständnissen in Absatz 2 klargestellt wird.

Nach Absatz 2 Satz 2 sind auf die Verwendung dieser nicht im Wege eines Kommunikationsvorganges übertragenen Daten §§ 23, 25 und 26 anzuwenden. In der Sache erfolgt kein Eingriff in das IT-System-Grundrecht (solcher Vorgang ist in Satz 4 geregelt), vielmehr regelt Satz 2 allein eine Beschränkung des Telekommunikationsgeheimnisses. Für die inhaltliche Ausgestaltung des seinerseits wiederum potenziell vielfältigen Lebenssachverhalts geben §§ 23, 25, 26 dennoch den angemessenen Maßstab vor. Werden beispielsweise technische Signale eines über Telekommunikationsdienste vernetzten Unternehmens-Systems ausgewertet, bietet § 23 den passenden Maßstab und wäre danach ohne über die Kommunikationsüberwachung hinausgehende Anforderungen zulässig. Ein gegenständlich begrenzter Überwachungseingriff wäre die Telekommunikationsbasierte Synchronisierung von Kontaktelisten in verschiedenen privaten IT-Systemen oder auch die Einbuchung eines Mobiltelefons in das Visitor Location Register einer bestimmten Vermittlungsstelle eines Mobilfunknetzes, über die eine Standortfeststellung möglich ist (entsprechend der Weite des Einzugsgebiets der Vermittlungsstelle allerdings nur sehr grob, also etwa zur Ermittlung eines Auslandsaufenthalts geeignet). Diese Überwachung bliebe unterhalb der Kommunikations-Äquivalenzschwelle des § 26 Absatz 2, wären danach an den Voraussetzungen des § 26 Absatz 1 zu messen. Ein Eingriffsäquivalent zur Kommunikationsüberwachung (§ 26 Absatz 2 Nummer 2) kann sein, wenn ein Cloud-Speicherdienst für Fotos und Videos genutzt wird, und das Nutzerverhalten darauf gerichtet ist, laufend vielfältige private Situationen derart festzuhalten. Erfolgt dagegen eine vollständige Auslagerung der Datenverarbeitung aus einem privaten IT-System, wäre die Weiterverarbeitung insoweit an § 25 zu messen, also nur unter erhöhten Voraussetzungen zulässig. Dabei ist die Überwachungsmaßnahme auch funktional einzuordnen. Wird beispielsweise ein Cyberangriff einer fremden Macht detektiert, der seinerseits ein Schadprogramm in ein privat genutzten Informationstechnischen System eingebracht hat und dadurch Informationen aus diesem System gewinnt, ist dies keine Ausforschung des privat genutzten Informationstechnischen Systems durch das BfV, sondern eine Überwachung der – unbefugten - Ausleitung durch den Angreifer, funktional vergleichbar also der Erfassung eines – befugten – Downloads von einer Webseite, somit Überwachung eines Kommunikationsvorgangs im Sinne des Absatzes 2 Satz 1, mithin eine Maßnahme nach § 22.

Satz 4 verweist für die Quellen-Telekommunikationsüberwachung im Falle eines Eingriffs in private IT-Systeme auf die dies betreffenden Befugnisse. Auch insoweit liegt zugleich zwar ein Eingriff in das Telekommunikationsgeheimnis nach Artikel 10 GG vor (BVerfG, Beschluss vom 24. Juni 2025 - 1 BvR 2466/19 – [Trojaner I] Leitsatz Nummer 3), die inhaltliche Ausgestaltung erfolgt aber angemessen am Maßstab von §§ 25, 26. Ist die Überwachung auf Kommunikationsüberwachung begrenzt, folgt aus § 26 Absatz 2 Nummer 1 und Absatz 3 die sachliche Synchronität mit § 22 Absatz 1 Satz 1, Absatz 3 und 4.

Zu Absatz 3

Der Absatz regelt die Maßnahmerichtung und übernimmt dazu § 3 Absatz 2 Satz 2 bis 4 G 10. Zu Nummer 1 verdeutlicht Satz 2 einen praxisrelevanten Anwendungsfall. Das hat klarstellende Bedeutung für diesen Sachverhalt und verdeutlicht darüber hinaus, dass die tatsächlichen Verdachtsanhaltspunkte nicht bereits selbst individualisiert sein müssen, sondern ebenso Umstände des Verhaltens des Betroffenen – hier die Teilnahme an einem verdächtigen Netzwerk – solchen Aufklärungsbedarf induzieren können.

Zu Absatz 4

Die Regelung greift den bisherigen § 4 Absatz 1 G 10 auf.

Die Erforderlichkeitsselektion ist durch die vorgeschriebene Erstprüfung nach Erhebung und die laufende fachliche Bearbeitung gewährleistet. Gleichwohl wird auch künftig an einer gesetzlichen Vorgabe zur besonderen Routineüberprüfung festgehalten. Diese wird jedoch nunmehr unter Erwägungen wirtschaftlicher Verwaltung auf 2 Jahre (bisher: 6 Monate) festgelegt und auch nicht endlos periodisch fortgeschrieben. Angesichts der erfolgten Erstselektion ist eine wirksam gestaltete nochmalige Routineüberprüfung erst nach 2 Jahren sinnvoll, da laufende Erkenntnisse zur Erforderlichkeit ohnehin in die laufende Bearbeitung eingehen und speziell bei Abschluss einer Maßnahme danach eine generelle Überprüfung der Wertigkeit gewonnener Erkenntnisse erfolgt. Eine spätere Neubewertung, die nicht von einer neuen Information veranlasst ist, sondern im Rahmen neuerlicher Gesamtschau erfolgt, kommt ernstlich erst mit einem wesentlich verbreiterten Bild von Folgeerkenntnissen in Betracht. Das bisher sehr kurze Überprüfungsstakkato ist danach eine Bürokratieroutine ohne relevanten Effekt für den Grundrechtsschutz. Dies gilt ebenso für die dauerhafte Fortführung der Routinen. Bei bereits gesichert als erforderlich eingeschätzten Informationen kommt dem keine weitere Bedeutung zu. Deshalb werden die Sonderprüfungen zugleich nach 2 Jahren abgeschlossen. Dies führt nicht zu einem Wegfall von Prüfroutinen, sondern zur Einbettung in das allgemeine Verfahren nach § 38 Absatz 2. Der Reformansatz der operativen Stärkung soll gerade auch vermeiden, dass operativer Ressourcen für unzweckmäßige Bürokratieroutinen gebunden werden. Wenn sie durch solche Aufwände vom Einsatz zur Gefahrerforschung abgehalten werden, beeinträchtigt dies wirksamen Rechtsgüterschutz.

Ebenso der Vermeidung unnötiger Aufwände dient der Wegfall der bisherigen Verfahrensmaßgabe, dass die Löschung unter Aufsicht eines Volljuristen erfolgt. Diese Verfahrensgestaltung trägt nicht zur Wirksamkeit der Regelung bei und ist danach verzichtbar.

Zu Löschungsprotokollen wird auf eine besondere Zweckbindung verzichtet. Der Fall, dass die Daten noch für Verfassungsschutzaufgaben benötigt werden, ist zwar äußerst unwahrscheinlich. Wenn er dennoch eintritt, besteht indes kein Sachgrund, die erforderliche Nutzung auszuschließen. Diese Daten haben nur sehr begrenzten Informationsgehalt, speziell keinen, der spezifisch Privatheit oder Persönliches beträfe.

Die Vorgaben zur Protokolllöschung sind klarer gefasst. Sie knüpfen eindeutig an die Mitteilung oder dem Absehen hiervon an. Eine vorherige Löschung entfällt im Interesse der Rechtsschutzeffektivität.

Zu Nummer 1

Die Nummer regelt die Löschung als Folge der Mitteilung, wenn der Betroffene nicht binnen angemessener Frist verdeutlicht, dass er aus Rechtsschutzgründen an weiterer Aufbewahrung interessiert ist. Mindestaufbewahrung bleibt das Ende des zweiten Kalenderjahres, das dem Jahr der Protokollierung folgt, um in jedem Fall und unabhängig vom Individualrechtsschutz die Möglichkeit einer Datenschutzkontrolle durch den Unabhängigen Kontrollrat zu gewährleisten.

Zu Nummer 2

Nach der Nummer erfolgt die Löschung nach endgültigem Absehen von der Mitteilung. Da dies frühestens 5 Jahre nach Abschluss der Maßnahme erfolgt, ist die bisherige Speicherdauer (bis zum Ende des zweiten Kalenderjahres, das dem Jahr der Protokollierung folgt) in jedem Fall gewahrt, damit auch die Möglichkeit zur zwischenzeitlichen Datenschutzkontrolle durch den Unabhängigen Kontrollrat.

Zu Absatz 5

Die Regelung übernimmt den bisherigen § 13 G 10.

Zu § 23 (Auslesen informationstechnischer Geräte)

Die §§ 23 bis 26 enthalten differenzierte Regelungen zur nachrichtendienstlichen Gewinnung von Daten aus informationstechnischen Geräten, die abhängig vom Eingriffssachverhalt an dazu jeweils angemessene Voraussetzungen gebunden werden. Zur Abstufung von Privatheitsbezügen dient dabei die Grundstruktur, dass auf einer ersten Ebene nach dem Verwendungsprofil des IT-Geräts zu unterscheiden ist, nämlich zwischen allgemeinen Eingriffen (§ 23) und qualifizierten Eingriffen in private IT-Systeme (§§ 25, 26). Auf einer zweiten Ebene ist bei privaten IT-Systemen maßgeblich, welche Daten letztlich im Rahmen der konkreten Maßnahme genutzt werden dürfen (Vollauswertung, § 25; gegenständliche Beschränkung, § 26). Ergänzend konkretisiert § 24 die Bedingungen eines Eingriffs, der gegenständlich auf IT-Angriffsspuren begrenzt in ein IT-System eines kommerziellen Hosting-Anbieters erfolgt.

§ 23 befugt nicht zum Eingriff in das IT-System-Grundrecht (Absatz 4 Satz 1). Erfasst werden IT-Systeme, die nicht privat eigengenutzt sind (mit der hierin angelegten Potenzialität, Einblick in wesentliche Teile der Lebensgestaltung des Nutzers zu gewinnen), vgl. § 25 Absatz 1 Satz 2 und 3. Auch solche IT-Systeme sind jedoch einerseits von der Typizität einer hohen Datenmenge geprägt, andererseits ist vor Einsichtnahme grundsätzlich ungewiss, was im Näheren gespeichert ist. Der gesetzliche Tatbestand greift dies in einem Rechtsfolgenbündel auf. Der generellen Typizität einer hohen Datenmenge trägt die in Absatz 1 angehobene Grundschwelle – der erheblichen Beobachtungsbedürftigkeit – Rechnung. Werden beim Auslesen intensiv eingreifende Sachverhalte aufgefunden, dürfen sie nach Absatz 3 für den Maßnahmezweck nur weiterverarbeitet werden, wenn er auch diesen Eingriff rechtfertigt, weil die Maßnahme der Aufklärung besonders erheblich beobachtungsbedürftiger Bedrohungen dient. Ist bereits vorab erwartbar, dass auch Informationen enthalten sein werden, die nur zur Aufklärung besonders erheblich beobachtungsbedürftiger Bedrohungen erhoben werden dürfen, muss dann, wenn maßnahmeveranlassend lediglich erheblich beobachtungsbedürftige Bedrohungen sind, nach Absatz 2 eine gesonderte Vorselektion dafür sorgen, dass nur die dazu erhebbaren Daten für die nachrichtendienstliche Anschlussverarbeitung verfügbar werden. Für Fälle, in denen der Speicherinhalt in seiner Gesamtheit weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen ermöglicht, darf dieses Potenzial nicht realisiert werden (Absatz 4), d.h. die Auswertung bleibt in jedem Fall einem punktuellen Erkenntnisinteresse folgend, der informationelle Eingriff hierdurch limitiert.

Zu Absatz 1

Die Befugnis regelt die Informationsgewinnung aus nachrichtendienstlich beschafftem Zugang zu elektronischen Speichermedien. Wie auch Absatz 4 Satz 1 verdeutlicht, schließt die Befugnis, nachrichtendienstlich eingreifen zu dürfen, auch ein, Änderungen im System vornehmen zu dürfen (nach Maßgabe des § 25 Absatz 6). Diese Befugnis gilt infolge erst recht, wenn in dem System keine personenbezogenen Daten verarbeitet werden und lediglich Sachinformationen gewonnen werden sollten. Da solche Informationserhebung für sich keinen Grundrechtseingriff darstellt, ist dies nicht in einer besonderen Befugnis geregelt. Die Rechtfertigung eines Integritätseingriffs folgt aber aus § 23 mit auch für diese Datenerhebung aus einem informationstechnischen System.

Für die Anwendung der Vorschrift ist unerheblich, ob das Speichermedium isoliert beschafft wurde (etwa eine Speicherkarte) oder mit einem Gerät, in das es verbaut ist, und ob bei Einsichtnahme noch etwaige Zugriffssicherungen überwunden werden müssen. Dabei darf es sich allerdings nicht um ein privates informationstechnisches System handeln, da hierin ein Eingriff in das IT-System-Grundrecht läge, der besonders engen Voraussetzungen unterliegt (Absatz 4 Satz 1). Im Übrigen ist unerheblich, ob es sich um ein originales Speichermedium handelt oder eine eingesetzte Quelle dieses vollständig kopiert hat. Nicht unter die Regelung fällt allerdings, wenn eine Quelle ihrerseits gesammelte Informationen auf einem von ihr dazu genutzten Speichermedium kompiliert und übergibt.

Tatbestandlich nicht erfasst sind Geräte, die das BfV nicht selbst nachrichtendienstlich beschafft, sondern von anderen Behörden übermittelt erhält. Hier sind die maßgeblichen Zugangsregelungen in den Beschaffungs- und Übermittlungsbefugnissen der anderen Stelle normiert. Nimmt das BfV hier seine originäre Aufklärungsaufgabe wahr, ist dies kein Erhebungs-, sondern ein Auswertungsvorgang, der sich an § 36 bemisst, also speziellen Beschränkungen nach dessen Absatz 3 und 4 für qualifiziert eingreifende Erkenntnisprodukte unterliegt. Gleiches gilt für Geräte, die dem BfV von Dritten, mit denen es nicht zur Informationsbeschaffung in Verbindung steht, zugespielt werden. Einen Sonderfall bildet die Unterstützung in speziell geregelten Verfahren. Dies richtet sich dann nach den für dieses Verfahren geltenden Vorschriften. Beispiel ist die Asservatenauswertung von nach § 4 Absatz 4 Vereinsgesetz beschlagnahmten Speichermedien, wenn das BMI als Verbotsbehörde zur Auswertung das BfV in Anspruch nimmt.

Abweichend vom vorstehenden Grundsatz wird mit Satz 2 der Sachverhalt, dass das BfV ein informationstechnisches Gerät von einem ausländischen Nachrichtendienst erhalten hat, der eigenen nachrichtendienstlichen Zugangsverschaffung gleichgestellt.

Zu Nummer 1

Einbezogen sind gleichermaßen die Sachverhalte eines elektronischen Fernzugangs wie des Zugangs infolge physischer Inbesitznahme des Speichermediums (etwa einer Speicherkarte). Entscheidend ist, dass sich das BfV selbst und verdeckt operierend Zugang verschafft. Die nachrichtendienstliche Zugangsverschaffung erfolgt mit dem Ziel der Auslesung, so dass der Vorgang wertungsmäßig als funktionale Einheit betrachtet wird und das Auslesen den qualifizierten Voraussetzungen der nachrichtendienstlichen Beschaffung unterliegt. Dies ist zu unterscheiden von sonstigen Sachverhalten, in denen Dritte dem BfV Daten übermitteln. Dieser Vorgang bemisst sich nach den vom Dritten anzuwendenden Erhebungs- und Übermittlungsvorschriften, ohne dass hinzutretend noch besondere Beschränkungen in der Datenverarbeitung des BfV nötig wären, die davon abhingen, ob die Daten etwa durch Telekommunikation oder auf einem physischen Speicher übermittelt werden.

Die Regelung vermittelt einen dem Vertraulichkeitsschutz nach Nummer 2 bereits vorgelagerten Schutz für den nachrichtendienstlichen Informationszugang durch das BfV. Dies entspricht dem Integritätsschutz beim IT-Systemgrundrecht. Ob dessen Anwendungsbereich auch nicht eigengenutzte IT-Systeme umfasst (verneinend Beschluss des BVerfG vom 24. Juni 2025 - 1 BvR 180/23 [Trojaner II] – Rn. 173, 230), kann aus der Ergebnisperspektive mithin dahinstehen, da eine jedenfalls ergebnisgleiche Regelung erfolgt und es dazu nicht darauf ankommt, ob die Fachregelung auch grundrechtlich determiniert ist.

Zu Nummer 2

Zu Buchstabe a

Der Buchstabe erfasst die Datenverarbeitung, auf die die Zugangsverschaffung nach Nummer 1 bereits final angelegt ist.

Zu Buchstabe b

Nummer 2 regelt den Erhalt eines informationstechnischen Geräts von einem ausländischen Nachrichtendienst. Hier erfolgt eine Gleichstellung mit der eigenen nachrichtendienstlichen Zugangsverschaffung.

Zu Absatz 2

Der Absatz trifft eine besondere Verfahrensvorkehrung für Fälle, in denen den Umständen nach damit zu rechnen ist, dass besonders schutzwürdige Informationen erlangt werden. Maßgeblich ist dabei nur der auszulesende Inhalt. Sofern nur ein Teil ausgelesen werden

soll, ist also auch nur dieser Teil maßgeblich. Ist danach mit besonders schutzwürdigen Informationen zu rechnen, erfolgt zunächst eine von der operativen Aufgabenwahrnehmung gesonderte Vorprüfung. Zudem besteht hier die weitere Verfahrenssicherung der unabhängigen Vorabkontrolle nach § 32 Absatz 1 Satz 1 Nummer 6.

Zu Absatz 3

Absatz 3 regelt besondere Verwendungsbeschränkungen zu Sachverhalten besonders erheblichen Eingriffsgewichts, sei es durch den Umfang der Informationen, sei es durch deren Eindringtiefe in die Privatheit. Das Umfangskriterium bezieht sich nicht auf einzelne Sachverhalte, sondern auf Lebensbereiche, wie etwa wirtschaftliche Aktivitäten, die nicht lediglich punktuell, sondern weitestgehend erfasst werden. Ein Beispiel wäre die ordnungsgemäße Buchhaltung eines Gewerbetriebs, wenn ein längerer Zeitraum abgebildet wird. Auch bei der Eindringtiefe vermitteln nicht bereits vereinzelt mitanfallende Informationen aus dem Bereich des Höchstprivaten (vgl. Erläuterung zu § 27) das besonders erhebliche Eingriffsgewicht, das jedoch dann erreicht wird, wenn auf dem Datenträger solche Informationen systematisch gesammelt sind. Liegt ein solcher Qualifikationssachverhalt vor, gelten besondere Voraussetzungen dafür, die gewonnenen Informationen auch für die mit der Maßnahme bezweckte Aufklärung weiterzuverarbeiten. Liegen diese Voraussetzungen nicht vor, sind diese Daten zu löschen. Eine Ausnahme gilt allerdings für die gesetzliche Übermittlungspflicht nach § 46 Absatz 1 zur Abwehr bereits konkretisierter Gefahren für besonders gewichtige Rechtsgüter. Bei den Qualifikationssachverhalt des Absatzes 3 besteht zudem das Erfordernis der unabhängigen Anordnungskontrolle vor Weiterverarbeitung nach § 34 Absatz 1 Satz 1 Nummer 7.

Zu Absatz 4

Die Regelung übernimmt zum Schutz der Integrität des informationstechnischen Systems die Regelung des bisherigen § 11 Absatz 1a G 10 Satz 3 ff. (mit Ausnahme von Satz 3 Nummer 1, die eine spezielle Regelung zu Quellen-TKÜ trifft). In Satz 2 neu hinzugekommen ist – entsprechend anderen Einsatzregelungen – eine Schutzvorschrift, wonach der maßnahmezweck nicht durch die Rückgängigmachung torpetiert werden muss, speziell bei verbundenem Entdeckungsrisiko. Außerdem können die Änderungen nach Satz 3 auch dann belassen werden, wenn sie absehbar wieder benötigt werden.

Im System-Begriff eingeschlossen ist, dass integrierte Komponenten nicht isoliert zu betrachten sind. Es ist also auch eröffnet, unter Eingriff in die Integrität einer Komponente dort Änderungen vorzunehmen, um aus einer anderen Komponenten Informationen gewinnen zu können, wenn die Änderungen dazu unerlässlich sind.

Zu Absatz 5

Absatz 5 stellt die Spezialität für Eingriffe in die Integrität privater informationstechnischer Systeme klar.

Auch mit der jüngsten Verfassungsrechtsprechung (Beschlüsse des BVerfG vom 24. Juni 2025 - 1 BvR 2466/19 [Trojaner I] / 1 BvR 180/23 {Trojaner II] -) ist noch nicht abschließend geklärt, ob auch isolierte Speichermedien – etwa eine Speicherkarte – dem Schutzbereich des IT-System-Grundrechts unterfallen können. Dagegen spricht, dass es begrifflich nicht eröffnet ist, isolierte Systemkomponenten (wie einen Prozessor oder ein Speichermedium), die ohne Systemintegration nicht die Systemfunktionalität erreichen, bereits als IT-System zu bezeichnen. Aus Schutzzweckerwägungen ist zudem relevant, dass das Auslesen einer physisch in Besitz genommenen Speicherkarte ohne Infiltration einer Systemintegrität erfolgt, mithin auch ohne Folgerisiken solcher Infiltration für die Integrität gespeicherter Informationen oder für eine Systemfunktionalität. Die originäre Funktion der Integritätsgewährleistung als vorverlagerter Vertraulichkeitsschutz (Trojaner I, Ls. 2.b) läuft ohne durch Infiltration zu überwindende technische Hürde leer und könnte hier nur als physische Inbesitznahme gedeutet werden. Dagegen würde eine bloße Entgegennahme und Verwahrung

eines Tagesbuchs wohl kaum bereits den Schutz des Kernbereichs privater Lebensgestaltung im Sinne eines eingriffsgleichen Gefährdungstatbestandes vorgelagert berühren.

Andererseits hat das Bundesverfassungsgericht nunmehr eindeutig die Betrachtung von Schutzbereich und Eingriffsgewichtung beim IT-System-Grundrecht entkoppelt (Trojaner I Rn. 124). Leitbild ist mithin nicht mehr ein Eingriffsgewicht, dass die mit den Voraussetzungen der Online-Überwachung bezeichneten Verhältnismäßigkeitsanforderungen stellt, vielmehr weisen solche Eingriffe ein weites Spektrum von Gewichtigkeiten auf (a.a.O.). Dies entkoppelt die Eingriffsbetrachtung zugleich von dem schwersten Eingriffssachverhalt einer Überwachung des Lebens im virtuellen Raum durch längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der entsprechenden Daten (BVerfGE 120, 274 – Rn. 234). Insofern kann auch die einmalige Systemkopie ein, wenn auch minder gewichtiger, Eingriff in das IT-System-Grundrecht sein. Wenn zudem berücksichtigt wird, dass das Gewicht des vorgelagerten Integritätseingriffs aus dem Vertraulichkeitseingriff, auf den die Maßnahme zielt, abzuleiten ist (Trojaner I – Rn. 124: maßgeblich, welche Daten letztlich im Rahmen der konkreten Maßnahme genutzt werden dürfen), spricht einiges dafür, den Sachverhalt eines systemintegrierten Speichermediums nicht von dem Sachverhalt eines systemintegriert beschriebenen, nunmehr aber isolierten Speichermediums zu unterscheiden. Deshalb liegt dem Tatbestandsverständnis des Satzes 1 ebenso dieser Sachverhalt zugrunde. Voraussetzung bleibt damit insoweit jedoch auch, dass das Speichermedium in einem eigengenutzen IT-System zur Speicherung der dort selbst verarbeiteten Daten eingesetzt worden war (oder es sich um eine Kopie eines solchen Speichermediums handelt).

Dieser materiellen Betrachtung folgt auch Satz 2. Die hohe Schwelle des § 24 Absatz 1 ist vom Potenzial umfassender Persönlichkeitsausforschung veranlasst. Um Maßnahmen nach § 22 auch folgenseitig davon klar abzugrenzen, wird die Weiterverarbeitung der ausgelesenen Daten entsprechend beschränkt. Sie dürfen nicht genutzt werden, um aus ihnen Verhaltens- oder Persönlichkeitsprofile zu erstellen. Dies sind Auswertungsprodukte umfassender Persönlichkeitserfassung. Abzugrenzen ist dies etwa von der Auswertung nach Verhaltensmustern bei der Durchführung von Bestrebungen. Der Ausschluss einer umfassenden Persönlichkeitserforschung begrenzt das Eingriffsgewicht der Maßnahme (BVerfGE 162, 1 – Rn. 157).

Zu Absatz 6

Absatz 6 enthält die übliche Regelung, wonach die Löschungspflicht hinter Erfordernissen der Aufgabenerfüllung und wirtschaftlicher Verwaltung zurücktritt, wobei Betroffeneninteressen durch den Nutzungsausschluss dieser Daten gewahrt werden.

Zu § 24 (Auslesen technischer Spuren von informationstechnischen Angriffen)

Zu Absatz 1

Die Befugnis ergänzt § 12 um die Möglichkeit einer Selbstvornahme. Die Befugnis ist auf die Fälle begrenzt, in denen erforderliche Informationen nicht oder nicht ohne Gefährdung des Erhebungszwecks durch Auskunft des Betreibers nach § 12 erlangt werden können. Die Gefährdung des Erhebungszwecks durch die Verpflichtung des Betreibers ist insbesondere dann anzunehmen, wenn Anhaltspunkte dafür vorliegen, dass der Betreiber selbst an dem Angriff mitwirkt oder die Vertraulichkeit nicht gewährleistet ist, also das Risiko besteht, dass der Angreifer davon erfährt, dass sein Angriff im Fokus der Aufklärung ist. Solche Sachverhalte sind die seltene Ausnahme. Eine wirksame Aufklärung muss aber auch für solche Sondersachverhalte das geeignete Aufklärungsmittel erhalten.

Zu Absatz 2

Der Absatz regelt Nothilfemaßnahmen, wenn das BfV gelegentlich seiner Aufklärung von Angriffsspuren im Server des Hosting-Anbieters auch Angriffstools oder dort gepufferte - womöglich noch nicht zum Angreifer weitergeflossene - Beutedaten feststellt. Solche

Intervention in das Störungsgeschehen gehört nicht zum Aufgabenprofil des Nachrichtendienstes. Sie ist als Nothilfe bei Gefahr im Verzug aber auch nicht ausgeschlossen. Stellt das BfV beispielsweise während einer Observation fest, dass die Zielperson eine andere Person angreift, ist legitim, dass die observierenden oder sie absichernde BfV-Bedienstete dem Opfer zu Hilfe eilen. Entsprechend verhält es sich vorliegend, wenn die gegenwärtige Gefahr nicht gleichermaßen wirksam durch polizeiliche Intervention zu beenden ist, was regelmäßig schon allein wegen des Zeitverzugs ausscheidet. In den Fällen des Absatzes 1 scheidet ebenso die Information des Hosting-Anbieter – zur Störungsbeseitigung durch diesen – aus, da die Maßnahme hier gerade verdeckt durchgeführt werden muss, um ihren Zweck nicht zu gefährden.

Zu § 25 (Eingriff in die Integrität privater informationstechnischer Systeme)

Die Befugnis erlaubt Eingriffe in das IT-System-Grundrecht. Sie wird ergänzt durch § 26 für Eingriffe, die durch Eingriffsbegrenzung minderen Gewichts sind (weil hierzu zu berücksichtigen ist, welche Daten letztlich im Rahmen der konkreten Maßnahme zulässig nutzbare Daten sind). Dies folgt der in der jüngsten Verfassungsrechtsprechung klaren Systematisierung einerseits zur Schutzbereichseröffnung und andererseits zur Eingriffsgewichtung (die mithin nicht bereits vom Schutzbereich festgelegt ist - Beschluss des BVerfG vom 24. Juni 2025 - 1 BvR 2466/19 [Trojaner I] – Rn. 124). Mit den verschiedenen Regelungen trägt das Gesetz unterschiedlichen Eingriffssachverhalten Rechnung. Das Potenzial zu gewichtigen Eingriffen in Privatheit und Persönlichkeitsrechte ist heterogen, bereits abhängig von Struktur und Nutzung eines informationstechnischen Systems, ebenso vom punktuellen oder umfassenden Zugriff darauf und schließlich auch von der Möglichkeit zu erkenntnisschöpfender Auswertung. Ein angemessener Ausgleich zwischen Interessen des Grundrechtsschutzes und beschränkenden Gemeinwohlbelangen ist nur möglich, wenn diese reale Heterogenität nicht normativ ignoriert, sondern ihr in angemessen differenzierenden Regelungen Rechnung getragen wird.

Zu Absatz 1

Absatz 1 synchronisiert den Eingriffstatbestand mit dem Schutzbereich des IT-Systemgrundrechts. Dazu hat die jüngste Verfassungsrechtsprechung (Beschlüsse des BVerfG vom 24. Juni 2025 - 1 BvR 2466/19 [Trojaner I] / 1 BvR 180/23 [Trojaner II] -) Präzisierungen vorgenommen. Das Gericht stellt auf die Bedeutung für die persönliche Lebensführung ab (Trojaner I – Rn. 113), folglich die Nutzung des IT-System als eigenes (Trojaner I - Rn. 104, Trojaner II – Rn. 173, 230), sowie die technische Funktionalität, Daten in großem Umfang und einer Vielfalt vorhalten zu können, dies mit dem komplementären Gefährdungspotenzial, hieraus einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen (Trojaner I - Rn. 97). Satz 2 greift dies auf und paraphrasiert dazu die Verfassungsrechtsprechung (speziell Trojaner II – Rn. 173).

Praxisbedeutsame Fälle, in denen das IT-System nicht eigengenutzt zur persönlichen Lebensführung ist, sind insbesondere Sachverhalte, in denen das informationstechnische System nur zur Durchführung der Bedrohung oder für Zwecke oder Tätigkeiten einer Vereinigung betrieben wird. Beispielsweise statten fremde Mächte ihre Agenten oftmals mit spezieller IT für ihre geheimdienstliche Tätigkeit aus, die auch nicht für private Zwecke genutzt werden darf. Ähnliche Methoden der Eigensicherung klandestiner Operationen sind auch in „professionellen“ extremistischen und terroristischen Zusammenhängen realitätsnah. Bei vereinsmäßiger Datenverarbeitung erfolgt ebenfalls lediglich eine auf solche Zwecke begrenzte Informationssammlung, in der weder besonders private Informationen noch eine über das Vereinsleben hinausgreifende Erfassung der privaten Lebensgestaltung angelegt ist. Mit solchem sektoralen Blick ist kein aussagekräftiges Bild der Persönlichkeit einzelner Betroffener zu erhalten. Dies ändert sich nicht dadurch, wenn untergeordnet zugleich eine private Nutzung erfolgt, die aber eben nicht die technische Potenzialität zur Erfassung wesentlicher Teile der Lebensgestaltung durch Einbindung in die persönliche Lebensführung realisiert, sondern peripher bleibt. Umgekehrt verliert das private

informationstechnische System nicht diese Qualität dadurch, dass neben der Einbindung in die persönliche Lebensführung auch die Nutzung für Zwecke der Bedrohung oder für Zwecke erfolgt, die ohne Erkenntniswert für Lebensgestaltung oder Persönlichkeit des Betroffenen sind.

Die in Satz 1 bezeichneten Eingriffsvoraussetzungen beruhen ebenso auf den Vorgaben der Verfassungsrechtsprechung (BVerfGE 162, 1 – Rn. 175 f., 178 f.), zur Einpassung in das Stufensystem des Gesetzes zusätzlich beschränkt auf besonders erheblich beobachtungswürdige Bedrohungen. Für lediglich begrenzte Eingriffe trifft § 26 eine besondere Regelung mit dem Eingriffsgewicht angepassten Differenzierungen in den Voraussetzungen.

Zu Absatz 2

Die Maßnahmerichtung ist gemäß der Verfassungsrechtsprechung (BVerfGE 162, 1 – Rn. 211) speziell begrenzt. Satz 1 Nummer 2 erfasst im Regelungszusammenhang des § 25 nur ein solches Drittsystem, das die Zielperson privat als eigenes nutzt. Dies ist etwa bei Cloud-basierter Datenverarbeitung möglich. Satz 3 trifft eine nach der Verfassungsrechtsprechung (a.a.O. Rn. 285) gebotene Maßgabe zum Kernbereichsschutz bereits auf der Erhebungsebene. Technische Lösungen sind zwar aktuell noch nicht verfügbar, die Regelung muss aber zukunftsfest sein, also auch Vorsorge für den Fall künftiger Verfügbarkeit treffen.

Zu Absatz 3

Der Absatz trifft besondere Löschungsprüfungsmaßgaben entsprechend § 22 Absatz 4.

Zu Absatz 4

Da Informationen, die aus einer Online-Überwachung gewonnen worden sind, wegen des besonders erheblichen Eingriffsgewichts für die Weiterverarbeitung einer speziellen Zweckbindung unterliegen (Absatz 7), sind sie zu deren Sicherung zu kennzeichnen. Die Kennzeichnungsregelung orientiert sich am bisherigen § 4 Absatz 2 und 3 G 10. Ein etwaiger Kennzeichnungsverzicht bleibt zur Sicherung von Betroffeneninteressen unerheblich, da die übermittelten Daten in jedem Fall der allgemeinen Weiterverarbeitungsbindung an den Übermittlungszweck unterliegen (§ 54 Absatz 2 Satz 1 Nummer 1) und eine Zweckänderung der Zustimmung des BfV bedarf (§ 54 Absatz 2 Satz 1 Nummer 2), das damit die Beachtung der Zweckbeschränkung nach Absatz 7 wirksam gewährleisten kann.

Satz 5 und 6 enthalten Maßgaben zur empfängerseitigen Löschungsprüfung. Auf eine Löschungsunterrichtung des BfV (vgl. bisher zu TKÜ-Daten § 4 Absatz 6 Satz 3 G 10) wird zur Bürokratieentlastung verzichtet, da diese Kenntnis für das BfV nicht erforderlich ist.

Zu Absatz 5

Die Regelung folgt der Rechtsprechung des Bundesverfassungsgerichts, das dem von ihm als Verhältnismäßigkeitsanforderung formulierten Prinzip der hypothetischen Datenneuerhebung besondere Vorgaben für die zweckändernde Weiterverarbeitung von personenbezogenen Daten entnimmt, die durch Online-Überwachung gewonnen worden sind (BVerfGE 162, 1 – Rn. 271).

Die Zweckbindung ist auch bei Übermittlungen zu beachten (§ 52 Absatz 1 Nummer 3). Da die Systematik des Gesetzes in gesonderte Abschnitte zu Weiterverarbeitung und Übermittlung gegliedert ist, wird zur Vermeidung von Fehlverständnissen auch hier nicht allein der Oberbegriff der Weiterverarbeitung, sondern auch die spezielle Weiterverarbeitung durch Übermittlung erwähnt.

Zu Nummer 1

Die Nummer überträgt die Erhebungsschwelle auf eine gefahrenabwehrende Anschlussverwendung.

Zu Nummer 2

Die Nummer synchronisiert die Zweckänderung zur Strafverfolgung mit der strafprozessualen Erhebungsbefugnis. Geregelt wird nur eine spezielle Zweckbeschränkung, nicht die Übermittlung, die sich nach § 48 bemisst und danach auch eine gewisse Verdachtsverdichtung voraussetzt, auch bei Übermittlung von Informationen aus Online-Überwachung.

Zu Absatz 6

Nach Absatz 8 gelten die allgemeinen Regelungen zum technischen Systemschutz und zur Dokumentation von Eingriffen in informationstechnische Systeme auch im besonderen Fall eines privaten IT-Systems.

Zu § 26 (Abgegrenzter Eingriff in die Integrität privater informationstechnischer Systeme)

Mit seiner jüngsten Rechtsprechung hat das Bundesverfassungsgericht (Beschlüsse vom 24. Juni 2025 - 1 BvR 2466/19 [Trojaner I] / 1 BvR 180/23 {Trojaner II] -) die Fragen der Schutzbereichseröffnung des IT-System-Grundrechts und der Gewichtung von Eingriffen hierin entkoppelt. Der Integritätsschutz begründet einen vorgelagerten Schutzbereich bereits in Ansehung eines Gefährdungssachverhalts (Trojaner I – Ls. 2.b), wird inhaltlich gewichtend aber am – lediglich bereits vorgelagert zu schützenden - Bezugspunkt des Persönlichkeitsschutzes ausgerichtet. Nicht jeder Eingriff in das IT-System-Grundrecht ist also an den strengen Anforderungen zu messen, die etwa für eine Online-Überwachung nach § 25 gelten; vielmehr ist für das insoweit zu berücksichtigende Eingriffsgewicht insbesondere maßgeblich, welche Daten letztlich im Rahmen der konkreten Maßnahme genutzt werden dürfen (Trojaner I – Rn. 124).

Zu Absatz 1

Demgemäß entkoppelt Absatz 1 gegenständlich beschränkte und dadurch mindergewichtige Eingriffe in das IT-Systemgrundrecht von den besonders strengen Anforderungen nach § 25 Absatz 1 bis 5. Maßgeblich ist dabei, dass die von Absatz 1 eröffnete Maßnahme nicht darauf zielt, dass Informationspotenzial eines privaten IT-Systems durch Erkenntnisse über wesentliche Teile der Lebensgestaltung des Nutzers auszuschöpfen, sie soll dementgegen nur bestimmte Sachverhalte und Lebensvorgänge aufklären und darf dabei auch nur die dazu erforderlichen Daten für diesen Zweck nutzen (Absatz 4 Satz 2). Absatz 1 regelt dabei einen Grundsachverhalt, wohingegen für qualifizierte Eingriffe mit Absatz 2 besonders erhebliche Beobachtungsbedürftigkeit Voraussetzung ist. Für das Begriffsverständnis eines durch bestimmte Arten von Daten abgegrenzten Sachverhalts oder Lebensbereichs ist dabei die im Qualifikationstatbestand des Absatzes 2 Satz 1 Nummer 1 aufgeführte Kommunikation leitbildhaft aussagekräftig. Bezogen auf das Eingriffsgewicht des Absatzes 1 wäre solche Datenartenbegrenzung beispielsweise die Erhebung von im System strukturiert gespeicherten Kontaktpersonen oder Verkehrsdaten zu Kontakten.

Die qualifizierte Schwelle des Absatzes 1 bildet in jedem Fall den Grundsockel für einen Integritätseingriff in private IT-Systeme, also auch für den Fall, dass überhaupt keine personenbezogenen Daten, sondern allein Sachinformationen erhoben werden sollen. Dies trägt dem Umstand Rechnung, dass solche Beschränkung zugleich – rechtfertigungsbedürftig - Missbrauchspotenzial öffnet. Selbst bei der Beschaffung banaler Informationen ist dieser Potenzialsockel einzurechnen. Ein höherer Grundsockel ist dagegen nicht veranlasst. Die rechtsstaatliche Verwaltung ist rechtsgebunden. Von der Beachtung ihrer Rechtsbindung ist grundsätzlich auszugehen. Auch bei der polizeilichen Ausstattung mit

Einsatzmitteln unmittelbaren Zwangs oder mit Schusswaffen ist nicht deren rechtswidriger Einsatz zu unterstellen und in Ausstattungsvoraussetzungen abzubilden.

Die Abkoppelung vom Eingriffsniveau der Online-Überwachung entkoppelt zugleich von polizeilichen Einsatzschwellen (BVerfGE 162, 1 – Rn. 156 ff., 166) und damit auch von der Subsidiarität gegenüber polizeilicher Durchführung (BVerfGE 162, 1 – Rn. 178 f.). Im Ergebnis sind die Maßnahmen – einschließlich der „Quellen-Telekommunikationsüberwachung“ - im Vergleich zu entsprechenden polizeilichen Maßnahmen unter erleichterten Voraussetzungen zulässig (BVerfGE 162, 1 – Rn. 156 ff.).

Zu Absatz 2

Als besonders gewichtigen sektoralen Eingriff, der gleichwohl aber hinter dem Gewicht einer Online-Überwachung zurückbleibt (Trojaner II – Rn. 199), führt Satz 2 leitbildhaft die Inhaltsüberwachung interpersoneller Kommunikation an.

Zu Nummer 1

Die Nummer erfasst gleichermaßen die Überwachung laufender Kommunikation wie die systematische Erhebung ruhender Kommunikation. Eine grundsätzlich mögliche Differenzierung im Eingriffsgewicht der beiden Komponenten wäre ohne relevante Praxisbedeutung, so dass davon im Interesse einer unkomplizierten Regelung abgesehen werden kann. Für die Erfassung ruhender Kommunikation ist in der neuen Regelungssystematik der Anordnungszeitpunkt unerheblich. Die Anordnung erlaubt die Erhebung sämtlicher im Speicher des IT-Systems dokumentierten Kommunikation (auch wenn sie vor dem Anordnungszeitpunkt stattgefunden hatte), da auch dies mit der Beschränkung auf den abgegrenzten Teil der Datenverarbeitung, die in Kommunikation besteht, nicht das Potenzial des persönlichen IT-Systems nutzt, wesentliche Teile der Lebensgestaltung des Nutzers zu erfassen.

Die Qualifikationsstufe des Absatzes 2 wird dabei auch erst erreicht, wenn die Kommunikation umfassend Überwachungsgegenstand ist. Dies ist nicht der Fall, wenn gezielt lediglich einzelne Kommunikationsvorgänge erhoben werden oder interpersonelle Kommunikation insgesamt ausgeschlossen ist (z.B. nur Webserven betrachtet wird). In diesen Fällen bleibt es bei den Eingriffsvoraussetzungen nach Absatz 1.

Zu Nummer 2

Angesichts der Vielgestaltigkeit in Betracht kommender Sachverhalte ist eine angemessene Regelung nicht ohne solche allgemein gehaltene Regelung möglich. Das Beispiel der Nummer 1 gibt dabei aber einen gut heranziehbaren Vergleichsmaßstab. Ein Eingriffsäquivalent zur systematischen Kommunikationsausforschung wäre etwa die Erhebung von Bild- und Videodateien, wenn die Zielperson hierüber systematisch Vorkommnisse seines privaten Lebens festhält. Dieses Beispiel wird mit Satz 2 speziell benannt, um die Norm inhaltlich zusätzlich zu konturieren. Zur Vergleichsbarkeitsbetrachtung am Referenzmaßstab der auf dem Übertragungsweg vom Telekommunikationsgeheimis geschützten Kommunikation ist auch einzubeziehen, inwieweit der Betroffene solche bildliche Dokumentation schon öffentlich gemacht hat und damit die parallele Verarbeitung im eigenen informationstechnischen System keinen Bereich spezifischer Privatheit mehr zum Gegenstand hat.

Zu Absatz 3

Die Regelung verschränkt die Befugnis im Falle der Telekommunikationsüberwachung in der Maßnahmerichtung und den Vorkehrungen zum Kernbereichsschutz mit der Regelung zur Telekommunikationsüberwachung.

Zu Absatz 4

Der Absatz trifft ergänzende Verfahrensmaßgaben.

Satz 1 und 2 gestalten die gegenständliche Befugnisbeschränkung hinsichtlich technischer Anforderungen aus. Die Ausnahmeregelung in Satz 2 lehnt sich an die Regelung zum Kernbereichsschutz an (§ 31 Absatz 1 Satz 4), die sogar für derart sensible Bezüge Standard der Bundesgesetzgebung ist, da auf entsprechender Rechtsprechung des Bundesverfassungsgerichts beruhend (st. Rsp., z.B. BVerfGE 162, 1 – Rn. 284). Danach sind verfügbare informationstechnische Sicherungen einzusetzen. Allerdings eröffnet die Befugnis – erforderlichkeitssichernd und grundrechtsschonend – konzeptionell eine bedarfsangepasste Flexibilität, die sich technisch nicht durchgängig abbilden lässt, da vorhandene Werkzeuge einzusetzen sind und deren technische Anpassung mit den zeitlichen Vorläufen keine praktikable Option ist. Demgemäß enthält Satz 1 ein Prinzip als zu optimierende Grundregel, die aber nach Satz 2 offen für sachbedingte Ausnahmen ist.

Satz 4 trägt der teilweisen gegenständlichen Überlappung mit der Regelung in § 22 Rechnung.

Zu Absatz 5

Angesichts ihrer gegenständlichen Beschränkung besitzt die Maßnahme keine grundsätzliche Potenzialität zur Gewinnung von Daten, die nach Umfang und Vielfalt die Erstellung von Verhaltens- oder Persönlichkeitsprofilen ermöglichen. Absatz 5 trifft daher nurmehr Vorsorge für atypische Fälle, in denen dies im Ergebnis doch möglich wäre. Hierzu synchronisiert der Absatz diese Auswertungsmöglichkeit mit den Voraussetzungen nach § 25. Geregelt ist dabei die Auswertung des aus der Maßnahme angefallenen Informationsaufkommens. Unbenommen bleibt hier – wie bei allen anderen Maßnahmen – die Zusammenführung mit weiteren vorhandenen Informationen auch zu übergeordneten Erkenntniszielen bei Auswertung aller vorhandenen Informationen. Dazu trifft § 36 Absatz 3 Satz 4 eine Regelung. Wie dort, ist die Erstellung von Verhaltens- und Persönlichkeitsprofilen nicht isoliert tatbestandlich, da dies inhaltlich nicht hinreichend bestimmt wäre, sondern die Ausrichtung auf die Gefährdungsbewertung zur Person

Zu Absatz 6

Der Absatz synchronisiert den beschränkten Eingriff in den Vorgaben zu technisch schonendem Eingriff und Dokumentation mit der Regelung in § 25.

Zu § 27 (Wohnraumüberwachung)

Die Regelung gestaltet den bisherigen § 9 Absatz 2 unter Wahrung der verfassungsrechtlichen Anforderungen praxisgerechter aus und passt dessen ungenügende Weiterverarbeitungsbeschränkung den verfassungsrechtlichen Vorgaben an. Da zur Art der technischen Überwachung – speziell: akustisch oder optisch – keine unterscheidenden Voraussetzungen zu treffen sind, kann auf solche Unterscheidung in der Erhebungsbefugnis (Absatz 1) verzichtet werden. Zu differenzieren ist erst für die Weiterverarbeitung (Absatz 4 Satz 1 Nummer 2).

Die Befugnis zur Nutzung technischer Mittel differiert nicht danach, wessen technische Mittel dies sind. Es ist mithin gleichermaßen eröffnet, dazu in die Wohnung eigene Sensorik des BfV einzubringen wie auch vorhandene Sensorik des Wohnungsinhabers zur Informationsgewinnung zu nutzen, etwa einen Smart Speaker. Wenn dazu in die Integrität informationstechnischer Systeme eingegriffen wird, sind allerdings ebenso die diesbetreffenden Anforderungen zu beachten. Die materielle Schwelle ist dabei immer beachtet, da die Schwelle der Wohnraumüberwachung sogar höher ist. Zur unabhängigen Vorabkontrolle trifft § 34 Absatz 4 für den Fall der Wonraumüberwachung eine spezielle Zuständigkeitsregelung, eine parallele Befassung auch des Unabhängigen Kontrollrates zum selben Sachverhalt ist mithin nicht erforderlich, vielmehr können Anordnung und Kontrollentscheidung integral auf den Durchführungsmodus unter Eingriff in ein informationstechnisches System erstreckt werden. Zu beachten sind jedoch die technischen Maßgaben nach § 23 Absatz 4,

wenn kein eigenes technisches Mittel zum Einsatz kommt, sondern dazu in ein in der Wohnung befindliches informationstechnisches System eingegriffen wird.

Zu Absatz 1

Zu Nummer 1

Die Nummer übernimmt die in Artikel 13 Absatz 4 GG vorgegebene Einsatzschwelle der dringenden Gefahr. Diese Gefahrenschwelle setzt eine konkrete Gefahr voraus, die sowohl mit Blick auf das Ausmaß wie auch auf die Wahrscheinlichkeit des zu erwartenden Schadens qualifiziert ist (BVerfGE 141, 220 – Rn. 184). Die Schadensqualifikation ist in Nummer 1 durch den Bezug auf besonders gewichtige Rechtsgüter generell gegeben. Die Wahrscheinlichkeit des Schadenseintritts ist nach den Einzelfallumständen zu würdigen. Ein Indikator kann eine besondere zeitliche Nähe sein. Wenn ein Schaden in allernächster Zukunft zu erwarten ist, ist dies mithin hinreichend, um das Kriterium der Dringlichkeit als erfüllt anzusehen (BVerfGE 162, 1 – Rn. 297). Notwendig ist dies aber nicht, da die verstärkte Schadenswahrscheinlichkeit sich auch aus anderen Umständen ergeben kann. Künftig ist also nicht mehr vorausgesetzt, dass die Gefahr bereits gegenwärtig ist. Die polizeifachliche Begriffsdefinition, die unterschiedlich vorgenommen wird (wie hier z.B. § 2 Nummer 4 NiPOG), ist für die Anwendung des § 25 unmaßgeblich.

Zu Nummer 2

Angesichts des besonders intensiven Grundrechtseingriffs einer Wohnraumüberwachung ist die Maßnahme subsidiär gegenüber den anderen Befugnissen des BfV.

Zu Nummer 3

Die Subsidiarität gegenüber polizeilicher Gefahrerforschung entspricht einer Vorgabe des Bundesverfassungsgerichts (BVerfGE 162, 1 – Rn. 178 ff.)

Zu Nummer 4

Die Nummer konkretisiert zum Schutzbereich des Artikel 13 GG die Erfordernisse des Kernbereichsschutzes der Privatheit mit einer spezifischen Vorgabe bereits auf der Erhebungsebene (BVerfGE 162, 1 – Rn. 280)

Zu Absatz 2

Der Absatz trifft die zum Schutz Dritter gebotene Begrenzung der Maßnahmerichtung (BVerfGE 162, 1 - Rn. 211).

Zu Absatz 3

Der Absatz trifft Verfahrensmaßgaben zur Eingriffsmilderung auf der Auswertungsebene. Die hier besonders wichtigen Regelungen zum Kernbereichsschutz sind in der speziellen regelung des § 31 aufgenommen, dort insbesondere mit Absatz mit Absatz 4 Satz 1 Nummer 2 und Absatz 5 Satz 1 Nummer 1.

Zu Absatz 4

Die Regelung folgt der Rechtsprechung des Bundesverfassungsgerichts, das dem von ihm als Verhältnismäßigkeitsanforderung formulierten Prinzip der hypothetischen Datenneuerhebung besondere Vorgaben für die zweckändernde Weiterverarbeitung von personenbezogenen Daten entnimmt, die durch Wohnraumüberwachung gewonnen worden sind (BVerfGE 162, 1 – Rn. 271).

Zu Nummer 1

Die Nummer überträgt die Erhebungsschwelle auf eine gefahrenabwehrende Anschlussverwendung.

Zu Nummer 2

Die Nummer synchronisiert die Zweckänderung zur Strafverfolgung mit der strafprozessualen Erhebungsbefugnis, die in § 100c Absatz 1 Nummer 1 StPO auf den Straftatenkatalog des § 100b Absatz 2 StPO verweist. Zudem erfolgt im Hinblick auf die entsprechende Beschränkung in Artikel 13 Absatz 3 GG eine Beschränkung auf Informationen aus akustischer Überwachung.

Zu § 28 (Einsatzsicherung)

Die geregelte Maßnahme ist eine einsatzannexe Eigensicherung. Wegen des unmittelbaren Einsatzbezugs und damit der direkten Verknüpfung mit der Aufklärungstätigkeit erfolgt die Regelung in diesem Unterabschnitt und nicht im Abschnitt 4.

Zu Absatz 1

Die Regelung schafft eine spezielle öffentlich-rechtliche Grundlage für bisher auf Nothilfe-Grundlage geführte Sicherungseinsätze. Wenn eingesetzte Personen in besonders gefahrgeneigten Situationen operieren, bedürfen sie einer Absicherung durch im Umfeld verdeckt eingesetzte Sicherungskräfte, die nötigenfalls gefahrenabwehrend einschreiten. Dies ist nicht auf den Einsatz verdeckt geführter Quellen beschränkt, sondern kann gleichermaßen Observationstrupps oder auch die Ansprache von Personen betreffen, die als Vertrauensperson angeworben werden sollen, aber womöglich äußerst aggressiv darauf reagieren.

Geschützt werden können auch Einsatzmittel von bedeutendem Wert wie etwa ein zur Observation eingesetztes Personenkraftfahrzeug.

Solcher Sicherungseinsatz gilt originär der Eigensicherung. In solcher Situation sind aber auch Sachverhalte naheliegend, in denen Nothilfe für Dritte erforderlich wird, wenn beispielsweise eine Zielperson observiert wird, die während der Observation einen Angriff gegen Dritte ausführt. Satz 2 erstreckt hierfür die Befugnis zum gefahrenabwehrenden unmittelbaren Zwang auch auf solche Nothilfe-Konstellation.

Die neue Regelung korrespondiert typischen Einsatzsituationen und schafft dazu eine spezielle Handlungsgrundlage. Hierdurch wird nicht etwa Nothilfe in anderen Situationen ausgeschlossen. Dies betrifft beispielsweise einen Observationstrupp, der nicht von einer speziellen Absicherung begleitet ist. Auch in diesem Fall können die observierenden BfV-Bediensteten, auch wenn sie keine besonderen Vollzugskräfte nach Satz 4 sind, weiterhin einem Dritten, der von der observierten Zielperson unmittelbar angegriffen wird, beistehen und sind dabei durch Nothilfe gerechtfertigt. Gleiches würde auch für den Personenschutz des Präsidenten des BfV gelten, wenn dieser – außerhalb eines Einsatzzusammenhangs – angegriffen wird.

Nähere Maßgaben zur Ausübung unmittelbaren Zwangs trifft das Gesetz über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes. Die dort formulierten Schranken und verhältnismäßigkeitssichernden Maßgaben gelten nach Satz 3 hier entsprechend. Die entsprechende Anwendung bezieht sich nur auf hier sachlich einschlägige Regelungen. Der als ultima ratio eröffnete Schusswaffengebrauch ist dabei in der Maßnahmerichtung beschränkt auf die Störer selbst (§ 10 Absatz 1 Nummern 1 und 2 UZwG), ein Gebrauch gegen eine Menschenmenge (§ 10 Absatz 2 UZwG ist nicht eröffnet).

Die Anwendung unmittelbaren Zwangs ist nach Satz 4 auf dafür besonders geschulte und hierfür von der Amtsleitung speziell ermächtigte Bedienstete beschränkt.

Zu Absatz 2

Der Absatz enthält eine spezielle Eigensicherungsbefugnis, die sich inhaltlich an bestehenden Regelungen orientiert (speziell § 28a BPolG und § 34 BKAG). Die Anordnung liegt – angelehnt an die Vorbildregelungen – bei der Amtsleitung oder einer von ihr bestimmten Abteilungsleitung (§ 33 Absatz 1 Satz 1 Nummer 2 Buchstabe e).

Das Aufklärungsfeld des BfV - terroristische und extremistischen Bestrebungen sowie Operationen fremder Mächte – sind geprägt von einer starken Abschottung und von einem konspirativen Verhalten des nachrichtendienstlichen Gegenübers, verbreitet auch von gewaltsamem Vorgehen. Einsätze erfolgen danach oftmals in hoch gefährlichem Umfeld. Erfolgt der Kontakt zu aufzuklärenden Person erhöht sich die Gefährdung weil eine verdeckt begleitende Absicherung von der Wahrnehmung des Geschehens ausgeschlossen bleibt, also nicht ohne technische Unterstützung erkennen kann, wenn sich eine Gefahrensituation derart zuspitzt, dass ein rettendes Eingreifen nötig wird.

Die Eigensicherungsmaßnahme dient ausschließlich dem Schutz der für das BfV tätigen Person. Sie soll die Möglichkeit einer umgehenden Reaktion (Rettung) eröffnen. Deshalb unterliegt sie nach Artikel 13 Absatz 5 GG nicht den engen Voraussetzungen des Artikel 13 Absatz 4 GG was sich in den gegenüber § 27 erweiterten Voraussetzungen des § 28 abbildet.

Satz 2 enthält die nach Artikel 13 Absatz 5 GG gebotenen Weiterverarbeitungsbeschränkungen. Der Zweck der Gefahrenabwehr bezeichnet eine Finalität (des Rechtsgüterschutzes vor Störungen), dem nicht erst das Einschreiten gegen Gefahren dient, sondern bereits deren Aufklärung. Der Zweck bezeichnet die Finalität allgemein und ist nicht auf situativ qualifizierte Anlässe (wie eine konkrete Gefahr) beschränkt. Die Abwehr drohender Gefahren durch nachrichtendienstliche Aufklärung (vgl. § 1 Absatz 1 Nummer 1 G 10) ist mithin ebenso erfasst.

Ergänzt wird dies zur richterlichen Vorabkontrolle bei Zweckänderung durch § 34 Absatz 3 Satz 2. Da Artikel 13 Absatz 5 GG ebenso wie Artikel 13 Absatz 4 GG eine „richterliche“ Entscheidung voraussetzt, wird hier ebenso wie bei der Wohnraumüberwachung die Zuständigkeit des Bundesverwaltungsgerichts vorgesehen.

Aus der Zweckbegrenzung folgt auch, dass Aufzeichnungen, wenn sie für die zulässigen Zwecke nicht mehr erforderlich sind, zu löschen sind (§ 38 Absatz 1 Satz 1 Nummer 2 Buchstabe b). Soweit eine Weiterverarbeitung für zulässige Zwecke erforderlich ist, sind dazu die hierfür geltenden Bestimmungen zu beachten, also z.B. zur Übermittlung für Strafverfolgungszwecke § 48.

Wie auch § 27 oder § 16 Absatz 6 Satz 2 sind die besonderen Voraussetzungen auf den Fall der Privatwohnung beschränkt, beziehen also Betriebs- oder Geschäftsräume oder sonstigen Wohnungen im weiteren Sinn nicht ein. In diesen Fällen unterliegt die Eigensicherung den allgemeinen Voraussetzungen nachrichtendienstlicher Mittel und die Weiterverarbeitung von Informationen ist auch nicht gemäß Satz 2 beschränkt.

Zu § 29 (Besonderer Einsatz nachrichtendienstlicher Mittel)

§§ 17 bis 27 regeln Einsatzmittel und praxisrelevante qualifizierte Einsatzformen, die qualifiziert eingreifendes Gewicht erlangen und daher mit spezieller Regelung an besondere Voraussetzungen gebunden werden. Neben diesen speziellen Tatbeständen muss aber ergänzend auch berücksichtigt werden, dass Einsatzmittel, die typischerweise kein erhebliches Eingriffsgewicht erlangen, unter außergewöhnlichen Umständen durchaus den in § 16 geregelten Rechtfertigungsrahmen übersteigen. Wenn beispielsweise bei Informationsgewinnung durch einen Informanten, die üblicherweise vollständig von § 16 Absatz 1 getragen ist, nicht nur ungezielt auch höchstprivate Informationen anfallen, sondern auf Grund außergewöhnlicher Umstände einerseits solche Informationen von spezifischem Aufklä-

rungsinteresse sind und andererseits beim Informanten auf Grund einer besonderen Nähebeziehung zur Zielperson solche Informationen systematisch abgeschöpft werden können, kann dies angemessen nicht nach Maßgabe der Voraussetzungen des § 16 erfolgen. Hierzu enthält § 29 einen Qualifikationstatbestand mit qualifizierten Voraussetzungen.

Da es sich um eine Auffangregelung für atypische Sondersachverhalte handelt, sind naturgemäß – anders als bei §§ 17 bis 27 – keine spezifizierten Sachverhalte tatbestandlich bezeichnet, sondern unmittelbar die Kriterien, die nach der Verfassungsrechtsprechung (BVerfGE 162, 1 – Rn. 191) den Vorgang als qualifiziert eingreifend bestimmen. Dauerhaft persönliche Vertrauensbeziehungen beschreibt eine nachhaltig in der Privatheit aufgebaute Vertraulichkeit, in Abgrenzung etwa zu Vertrauensbeziehungen im Geschäftsverkehr oder weniger intensiven privaten Beziehungen, etwa im Vereinsleben. Die Erfassung der Persönlichkeit setzt nicht erst mit der Erstellung eines umfassenden Persönlichkeitsbildes ein, sondern bezieht bereits ein, wenn wesentliche Elemente der Persönlichkeit erfasst werden, wenn etwa private Lebensbereiche nicht nur punktuell, sondern umfassend ausgespäht werden. Nicht gemeint ist der aufklärungsveranlassende Sozialbezug selbst, also die persönliche Disposition zur Beteiligung an der Bedrohung.

Höchstprivate Informationen sind dadurch charakterisiert, dass einerseits die nicht öffentlich zugängliche Privatheit in einer besonders schutzwürdigen Sphäre oder Information berührt ist (eben nicht nur privat, sondern höchstprivat), andererseits aber der – nicht antastbare – Kernbereich der privaten Lebensgestaltung noch nicht erreicht wird, der insbesondere die Intimsphäre oder die Bekundung innerster Gefühle betrifft (vgl. BVerfG, Be-schluss vom 09. Dezember 2022 - 1 BvR 1345/21 – Rn. 102). Dieser – nicht antastbare, einer Überwachung absolut verschlossene - Menschenwürdekern des Höchstpersönlichen wird jedoch nicht bei jedweden höchstprivaten Informationen erreicht. Leitbildhaft ist die Gegenüberstellung in § 18 einerseits der intimen oder vergleichbar engsten persönlichen Bindungen (Absatz 4 – Kernbereich) und andererseits besonders privat geprägter Vertrauensbeziehungen, etwa zwischen langjährigen, engen Freunden.

Umgekehrt abzugrenzen ist der Bereich des Höchstprivaten von solchen Vorgängen, die bereits durch ihren Sozialbezug außerhalb dieses besonderen Privatheitsbereichs liegen (etwa Berufswelt) oder aufgrund ihrer Wahrnehmbarkeit (Gewohnheiten des täglichen Lebens, Aufenthaltsorte, Vereinsaktivitäten) oder einer üblichen oder vom Betroffenen praktizierte Informationsstreuung (z.B. Urlaubsfotos einer Familie) dem Bereich des bloß Privaten (nicht Höchstprivaten) zuzuordnen sind. Für Wahrnehmbarkeit und Streuung ist dabei relevant, ob sie sich im Kreis besonders privat geprägter Vertrauensbeziehungen hält oder eben darüber hinaus geht. Dabei können auch Verkehrsanschauungen und sozial verbreitete Verhaltensweisen zu solchem Informationsverhalten herangezogen werden, weshalb beispielsweise auch Informationen über allgemeine Erkrankungen nicht zwangsläufig als höchstprivat zu qualifizieren wären. Auch im Übrigen kann der Gegenstand der Information für die Einordnung maßgeblich sein. Allgemeine Informationen über Kontakte oder wirtschafliche Verhältnisse sind danach private, aber nicht höchstprivate Informationen. Als Faustformel zur Abgrenzung gegenüber „nur“ Privatem kann herangezogen werden: Was üblicherweise nur engen langjährigen Freunden (oder engen Verwandten) preisgegeben würde und auch sonst nicht erkennbar ist, ist höchstprivat, nicht hingegen, was allgemein oder vom Betroffenen breiter geteilt wird oder anderen erkennbar ist.

Verfahrensmäßig abgesichert wird die Auffangregelung durch die besondere behördeninterne Anordnungszuständigkeit nach § 30 Nummer 2 Buchstabe e (Amtsleitung) sowie die generelle unabhängige Vorabkontrolle nach § 34 Satz 1 Nummer 10, ferner das parlamentarische Berichtswesen nach dem UKRat-Gesetz, in das diese Maßnahmen, die der Vorabkontrolle des Unabhängigen Kontrollrates unterliegen, einbezogen sind.

Zu § 30 (Allgemeine Schranken nachrichtendienstlicher Mittel)

Die Regelung korrespondiert dem allgemeinen Erlaubnisgehalt des Amtsrechts (§ 15 Absatz 5), indem sie diese Erlaubnis mit allgemeinen Schranken begrenzt.

Zu Absatz 1

Absatz 1 greift die Regelung des bisherigen § 8 Absatz 2 Satz 2 auf. Für die Datenerhebung mit dem verbundenen Eingriff in die informationelle Selbstbestimmung oder besondere Privatheitsrechte (wie Artikel 13 GG) begründen bereits die besonderen Erhebungsbefugnisse in §§ 16 ff. solche Befugnis zum Individualrechtseingriff. Zudem enthält § 16 Absatz 1 eine besondere Befugnis in Bezug auf den Sachbesitz. Allgemeine Befugnisse zu sonstigen Grundrechtseingriffen – etwa in Eigentum oder körperliche Unversehrtheit – enthält das Amtsrecht zum Einsatz nachrichtendienstlicher Mittel dagegen gerade nicht. Dies verdeutlicht Absatz 1.

Zu Absatz 2

Absatz 2 übernimmt die bisherigen Regelungen aus § 9 Absatz 1 Satz 2 und 3, wobei die Erforderlichkeitsmaßgabe nicht auf die Beeinträchtigung Betroffener beschränkt bleibt, sondern allgemein auf rechtlich geschützte Interessen bezogen wird.

Zu Absatz 3

Absatz 3 übernimmt den bisherigen § 8 Absatz 2 Satz 3. Die Regelung beschränkt den Anwendungsvorrang nachrichtendienstlicher Befugnisse gegenüber kollidierenden Rechtsvorschriften durch ein Abwägungserfordernis. Dies gilt nicht nur als Verhältnismäßigkeitsmaßgabe gegenüber Individualrechten, sondern auch beispielsweise gegenüber ordnungsrechtlichen Vorschriften (etwa melderechtliche Anforderungen), die bei nachrichtendienstlichen Operationen hinter der speziellen Befugnis zum Einsatz nachrichtendienstlicher Mittel grundsätzlich zurücktreten, auch dies aber nur soweit, wie dies keine außer Verhältnis stehende Nachteile bewirkt. Dies ist angesichts der herausragenden Gemeinwohlinteressen, denen die Aufgabenwahrnehmung des BfV dient (BVerfGE 155, 119 - Rn. 151), regelmäßig nicht der Fall, gleichwohl ist eine allgemeine Schranke auch insoweit sachgerecht.

Zu Absatz 4

Absatz 4 entspricht dem bisherigen § 9 Absatz 1 Satz 4. Nach dem 2. Fall ist die Maßnahme einzustellen, wenn sie ersichtlich ungeeignet ist. Dies kann auch prognostische Elemente einschließen. Die bisherige Formulierung, die auf tatsächliche Anhaltspunkte abstellt, ist dazu aber unpassend, weil hiermit im Verfassungsschutzrecht ein spezifisch niederschwelliger Erkenntnisstand bezeichnet wird. Eine Einstellungspflicht bereits aufgrund erster, womöglich noch sehr unsicherer Eignungszweifel ist jedoch nicht gemeint. Zur Gewährleistung der inneren Kohärenz der Begrifflichkeiten wird somit auf diesen Zusatz verzichtet.

Zu § 31 (Schutz des Kernbereichs privater Lebensgestaltung)

Der Kernbereichsschutz ist verfassungsrechtlich geboten, erfordert allerdings eine spezielle Regelung nur für Maßnahmen, die typischerweise zur Erhebung kernbereichsrelevanter Daten führen (BVerfGE 162, 1 – Rn. 278). Im Interesse der Normenklarheit erfolgt hier gleichwohl eine allgemeine Regelung. Sie wird spezifisch ergänzt zu Vertrauenspersonen mit § 18 Absatz 4 (der nach § 19 auch für Verdeckte Bedienstete gilt),

Zu Absatz 1

Absatz 1 entzieht intime Gedanken wie auch die nichtöffentliche Kommunikation, wenn sie in höchstpersönlichen Vertrauensbeziehungen unter besonders schutzwürdigen Umständen erfolgt (wie etwa Gespräche unter nahen Angehörigen in der gemeinsamen Wohnung

zu höchstpersönlichen Angelegenheiten), pauschal der Beschaffung und Auswertung durch das BfV (BVerfGE 141, 220 - Rn. 121; BVerfGE 162, 1 - Rn. 275 ff). Er ist nicht gleichbedeutend mit höchstprivaten Informationen (die kein Ausschlussgrund der Maßnahme sind, allerdings bei nachrichtendienstlichen Mitteln, die solche Informationen typisch einschließen, eine unabhängige Vorabkontrollen nach § 34 erfordern), vielmehr bezieht er sich auf intime oder vergleichbar engste Beziehungen oder Informationen dieser absoluten Schutzwürdigkeit.

Nach Satz 2 sind bereits bei einer Einsatzplanung besonders kernbereichsgeneigte Situationen möglichst zu vermeiden. Dazu ist bereits vorab zu prüfen, ob Anhaltspunkte bestehen, dass der geplante Einsatz seinem Gesamtcharakter nach kernbereichsrelevante Informationen erfassen wird. Das Bundesverfassungsgericht (BVerfGE 165, 1 – Rn. 111) hat dies zur Einsatzplanung bei Vertrauenspersonen und Verdeckten Bediensteten vorgegeben, es gilt aber gleichermaßen für andere nachrichtendienstliche Mittel, speziell optische oder akustische Überwachungen mit technischen Mitteln, und wird daher in der allgemeinen Schrankennorm aufgenommen. Je mehr der Einsatz insgesamt von einer Nähe zum Kernbereich privater Lebensgestaltung geprägt ist, desto eher muss er von vornherein unterbleiben. Den Rahmen der Risikovermeidung bilden Belange wirksamer Aufgabenwahrnehmung und wirtschaftlicher Verwaltung, die ebenso zu wahren sind.

Für den Einsatz von Vertrauenspersonen und Verdeckteten Bediensteten enthält § 18 Absatz 4 (auch in Verbindung mit § 19 Absatz 1) eine Konkretisierung mit dem Ausschluss intimer Beziehungen, worauf Satz 3 im Interesse der Normenklarheit verweist. Satz 4 fordert ggf. technische Gewährleistungen, allerdings nur soweit möglich, was gegenwärtig faktisch nicht der Fall ist, so dass es sich im Wesentlichen um eine zukunftsgerichtete Regelung handelt.

Nicht umfasst vom absoluten Schutz sind Informationen mit Sozialbezug. Kommunikation hierüber ist nicht geschützt, selbst wenn sie auch Höchstpersönliches zum Gegenstand hat. Die Besprechung und Planung von Straftaten oder Gefährdungen gehört ihrem Inhalt nach nicht zum Kernbereich privater Lebensgestaltung, sondern hat Sozialbezug (BVerfGE 141, 220 - Rn. 122). Solcher Sozialbezug ist beispielsweise auch gegeben, wenn bei Aufklärungsmaßnahmen durch Verhalten und Äußerungen der Zielperson Erkenntnisse über eine psychische Störung mit resultierenden Gewaltphantasien anfallen. Hierbei sind zwar spezifische Vertraulichkeitsbeziehungen, bei denen der betroffenen Person gerade ermöglicht werden soll, fachliche qualifizierte Hilfe zu erlangen, absolut geschützt, also etwa ein Gespräch mit einem Psychotherapeuten (BVerfG a.a.O.), nicht jedoch allgemeine persönliche Kontakte. Wenn also eine Vertrauensperson solche gefährdungsqualifizierende Eigenschaften bei einer Zielperson feststellt, dürfen diese Erkenntnisse auch dem BfV mitgeteilt und dort zur Gefährdungsbewertung genutzt werden.

Mit den Vorgaben nach Absatz 1 ist nicht sicher auszuschließen, dass nicht doch kernbereichsrelevante Informationen beim BfV anfallen. Deshalb regelt Absatz 4 den Umgang mit solchen Informationen.

Zu Absatz 2

Absatz 2 regelt den besonderen Sachverhalt, dass bereits während laufender Überwachung erkennbar wird, dass kernbereichsrelevante Informationen erlangt werden. In diesem Fall ist die Maßnahme zu unterbrechen. Allerdings kann abhängig vom eingesetzten nachrichtendienstlichen Mittel operativ unter Umständen auch möglich sein, den Geschehensablauf oder den Mitteleinsatz dahingehend zu beeinflussen, dass – weitere – kernbereichsrelevante Informationen nicht anfallen. Dann entfällt der Unterbrechungstatbestand und die Maßnahme kann ohne Unterbrechung fortgeführt werden.

Unter Umständen kann eine gebotene Unterbrechung wegen einer Gefährdung eingesetzter Personen oder ihrer Einsetzbarkeit nicht sogleich erfolgen. Dann kann die Maßnahme

nach Satz 2 zunächst fortgeführt werden, allerdings sind etwaige operative Gestaltungsmöglichkeiten auch dahingehend zu nutzen, die Unterbrechung möglichst schnell zu ermöglichen (BVerfGE 165, 1 - Rn. 114 ff.). Nach der Rechtsprechung des Bundesverfassungsgerichts rechtfertigt der Rechtsgüterschutz einer eingesetzten Person eine Ausnahme vom Abbruchgebot „jedenfalls“, wenn ansonsten Leib oder Leben der Person in Gefahr gerieten (a.a.O. Rn. 115). Die gesetzliche Regelung bezieht auch die Freiheit als ebenso besonders gewichtiges Rechtsgut (BVerfGE 162, 1 – Rn. 243) ein. Ebenso wie beim Rechtsgut Leib muss hier allerdings eine erhebliche Beeinträchtigung drohen, um die Fortsetzung rechtfertigen zu können. Wenn in solcher Einsatzsituation solche Gefährdungen drohen, sind sie jedoch typischerweise erheblich. Der eingesetzten Person ist auch keine Aufopferung bei unübersichtlichen Schadensszenarien, die jedenfalls möglicherweise auch erhebliches Ausmaß annehmen, zuzumuten. Das Tatbestandsmerkmal der weiteren Einsetzbarkeit sichert gleichermaßen die Fortführung des aktuellen Einsatzes wie auch künftige andere Einsätze.

In der Regel muss beim Einsatz aller menschlicher Quellen, so z.B. auch bei Informanten, grundsätzlich ein gewisses Maß an Nähe und Vertrauen zu den jeweiligen Zielpersonen bestehen, um überhaupt Informationen gewinnen zu können. Im Einzelfall kann es vorkommen, dass eine Zielperson diese Beziehung in Anspruch nimmt, um kernbereichsrelevante Informationen mitzuteilen, z.B. wenn sie sich in einer emotionalen Ausnahmesituation befindet. In diesen Ausnahmefällen muss es der eingesetzten Person ermöglicht sein, zu ihrem Schutz aber auch zur Sicherung ihrer weiteren Einsetzbarkeit, unter den obig beschriebenen engen Bedingungen, in der Situation zu verbleiben.

Auch bei anderen Mitteln, wie z.B. bei der Observation kann es im absoluten Ausnahmefall nötig sein, in einer kernbereichsrelevanten Situation zu verbleiben. Hier ist insbesondere auch dem Umstand Rechnung zu tragen, dass seitens der beobachteten Bestrebungen und Tätigkeiten teilweise umfangreiche Gegenmaßnahmen ergriffen werden, um vom BfV eingesetzte Personen und nachrichtendienstliche Mittel, insbesondere Observationen, zu identifizieren bzw. unwirksam zu machen. Bei einer Enttarnung besteht auch regelmäßig die Gefahr, dass die Person mit einem heute üblicherweise jederzeit verfügbaren Smartphone fotografiert und das Foto in breiten Szenekreisen – mit Warnhinweis – geteilt wird. Die eingesetzte Person ist dann weit über den konkreten Einsatz hinaus verbrannt.

Bei den eingesetzten Personen, wie z.B. auch Observanten und Informanten, handelt es sich um professionell ausgebildete und erfahrene Akteure, oder Personen mit besonderen Zugangslagen, die nur unter großem Aufwand ersetzt werden können. Besonders schwierig gestaltet sich die Ad-hoc-Kompensation einer nicht mehr einsetzbaren Person in einer laufenden Maßnahme wie z.B. einer Observation. Insofern muss die Funktionsfähigkeit der nachrichtendienstlichen Aufklärung bzw. die Einsetzbarkeit der handelnden Personen durch die Möglichkeit eines ausnahmsweisen Verbleibens in einer kernbereichsgeschützten Situation gesichert werden. Zu berücksichtigen ist hierbei, dass es einer eingesetzten Person, die nicht als Quelle agiert, wie z.B. einem Observanten, eher möglich ist, die einschlägige Situation ohne Gefährdung seiner Person oder seiner Einsatzfähigkeit zu verlassen bzw. seinen Einsatz innerhalb der Maßnahme abzubrechen. Bei Sachverhalten, bei denen dies dennoch nicht der Fall ist, muss aber eben die beschriebene Abwägung zum geregelten Ergebnis führen.

Die in Absatz 2 geregelte Unterbrechung hält die Option offen, die Maßnahme nach Wegfall der Anhaltspunkte wieder fortzusetzen (wenn sich beispielsweise die Anhaltspunkte an die hinzutretende Anwesenheit einer weiteren Person knüpfen und diese erkennbar die Situation wieder verlässt). Besteht diese Option tatsächlich nicht, folgt nach Satz 2 der Abbruch der Maßnahme.

Zu Absatz 3

Absatz 3 trifft angelehnt an geltendes Recht (vgl. § 3a Absatz 1 Satz 3 G 10) eine Regelung zur automatischen Aufzeichnung, die um Vorlage- und Freigaberegelungen in Folgeabsätzen ergänzt wird.

Zu Absatz 4

Der Absatz regelt die Vorlage zur Vorabprüfung, die mit dem Nutzungsausschluss nach Absatz 6 einhergeht. Die Zuständigkeit zur Vorabprüfung ist in Absatz 5 geregelt.

Zu Nummer 1

Die Nummer ist sachlich ein Spezialfall der Nummer 3.

Zu Nummer 2

Im Fall der Wohnraumüberwachung ist wegen der singulären Eingriffsqualität eine vollständige Vorabvorlage von Aufzeichnungen nötig, um auf der Auswertungsebene Kernbereichsschutz maximal zu gewährleisten (BVerfGE 162, 1 - Rn. 282).

Bei Informationen, die unter Eingriff in die Vertraulichkeit eines privaten informationstechnischen Systems gewonnen worden sind, hat die Rechtsprechung des Bundesverfassungsgerichts zu Umfang und Anlass einer solchen Vorprüfung auf der Auswertungsebene eine Entwicklung genommen. Während es zunächst nicht als geboten erachtet hatte, zusätzlich zu den staatlichen Ermittlungsbehörden eine unabhängige Stelle einzurichten, die über die (Nicht-)Verwendbarkeit der gewonnenen Erkenntnisse im weiteren Ermittlungsverfahren entscheidet (BVerfGE 129, 208 – Rn. 221), hatte es zwischenzeitlich entschieden, dass die tatsächliche Durchführung und Entscheidungsverantwortung maßgeblich in den Händen von unabhängigen Personen liegen muss (BVerfGE 141, 220 – Rn. 224). Dies hat es in seiner Grundlagenentscheidung zum Verfassungsschutzrecht bekräftigt und dabei eine Begrenzung der externen Kontrolle auf bestimmte Daten gerügt (BVer-fGE 162, 1 – Rn. 315). Zuletzt hat das Gericht in nicht tragenden Begründungsausführungen allerdings in einer Weise auf § 100d Absatz 3 Satz 2 StPO Bezug genommen, die dahingehend verstanden werden kann, dass hierin eine verfassungskonforme Ausgestaltung des nachgelagerten Schutzes auf der Aus- und Verwertungsebene liegt (BVerfG, Beschluss vom 24. Juni 2025 – l1 BvR 180/23 – [Trojaner II] Rn. 267). Die Regelung des Absatzes 4 folgt diesem rechtlich unumstrittenen und in der Staatspraxis bewährten Modell der Strafprozessordnung, indem bei solchen Eingriffen nicht bereits der Eingriff anlassgebend ist, sämtliche Informationen vollständig vorab vorzulegen, sondern erst erlangte Erkenntnisse im Zweifelsfall Anlass geben, diese vorzulegen. Demgemäß werden in Nummer 2 nicht auch Aufzeichnungen aus Maßnahmen nach §§ 25, 26 aufgenommen, diese sind vielmehr nach Nummer 3 lediglich vorzulegen, soweit im Einzelfall tatsächliche Anhaltspunkte für Kernbereichsrelevanz vorliegen.

Eine alternative Ausgestaltung nach dem Modell der Regelung zur Wohnraumüberwachung ist bei Maßnahmen nach § 25 - in der Typizität gerade geprägt durch besonderen Datenumfang, unter Einschluss auch fremdsprachiger Informationen - faktisch kaum realisierbar. Insoweit ist es auch Gebot praktischer Konkordanz, den Schutz besonders gewichtiger Rechtsgüter nicht über faktisch paralysierende Verfahrensgestaltung auszuhöhlen. Die vorgesehene Regelung gewährleistet, dass die gewonnenen Informationen, bei denen die Zuordnung zum Kernbereich unsicher und zu denen danach eine nähere Prüfung veranlasst ist, vom Unabhängigen Kontrollrat durchgesehen werden, der auch über die Kernbereichsqualifikation und damit über Löschung oder Verwertbarkeit entscheidet. Eine externe Prüfung gewissermaßen ins Blaue erscheint bei Berücksichtigung einerseits der praktischen Probleme und andererseits des unklaren Mehrwerts zum Grundrechtsschutz nicht zwingend, zumal kernbereichsrelevante Informationen einerseits einer Löschungspflicht, verbunden mit einem Verwertungsverbot, unterliegen und andererseits

auch kein spezifisches operatives Interesse an solchen Informationen, mithin auch kein ernstliches Missbrauchsrisiko besteht. Wäre eine weitergehende Verfahrenssicherung, die im Grundgesetz nicht ausdrücklich vorgesehen ist, nicht lediglich eine Billigkeitsabwägung, sondern evidente Anforderung zur Gewährleistung zwingender Menschenrechtsstandards, wäre zu erwarten, dass sich solche Verfahren vergleichbar in anderen menschenrechtsbasierten Rechtsordnungen finden, was indes nicht der Fall ist. Für den absoluten Schutz der Menschenwürde ist unerheblich, in welchem institutionellen Rahmen der Staat – sei es im BfV, sei es im Unabhängigen Kontrollrat – von solchen Informationen ungewollte Kenntnis erlangt (um sie sogleich zu löschen). Für die Kontrolle der Verwaltungspraxis und ihre Fortentwicklung im Zusammenspiel mit der unabhängigen Kontrolle sind im Übrigen Strukturkontrollen des Unabhängigen Kontrollrates ungleich wirksamer als isolierte Einzelfallbetrachtungen.

Zu Nummer 3

Absatz 3 sieht allgemein in Zweifelsfällen ein besonderes Entscheidungsverfahren vor, das eine Prüfung herausgelöst aus den operativen Aufgabenbereichen gewährleistet.

In jedem Fall ist eine Einzelbetrachtung geboten. Dies betrifft auch die Erhebung aus privaten informationstechnischen Systemen. Eine gesicherte Empirie, dass hierin generell oder immerhin pauschalierend typisch auch kernbereichsrelevante Informationen gespeichert sind, liegt nicht vor. Nach der Alltagserfahrung ist solche durchgängige Typizität auch nicht anzunehmen. Indizieren nicht bereits Verwendungsumstände des privaten IT-Systems aussagekräftig, dass auch mit kernbereichsrelevanten Inhalten zu rechnen ist, kann die Auswertung also zunächst regulär als operative Aufgabe erfolgen. Werden dabei unerwartet Kernbereichsinhalte vorgefunden, sind sie zu löschen. Werden bei der Auswertung Teile des Dateisystems identifiziert, zu denen Anhaltspunkte auf Kernbereichsinhalte hindeuten (z.B. ein Ordner mit darauf hindeutender Bezeichnung), sind diese ohne weitere Auswertung zunächst zur Sichtung vorzulegen (nach Absatz 5 Nummer 1 dem Unabhängigen Kontrollrat). Gleiches gilt für einzelne Informationen, falls ihre Qualifikation als kernbereichsrelevant unsicher ist.

Zu Absatz 5

Zu Nummer 1

Eingriffe in die Vertraulichkeit privater informationstechnischer Systeme und die Wohnraumüberwachung betreffen besonders schutzwüdige Sphären der Privatheit. Deshalb erfolgt die Prüfung hier durch den Unabhängigen Kontrollrat.

Zu Nummer 2

Bei Maßnahmen ohne spezifische Kernbereichstypik (auch unter Berücksichtigung von Möglichkeiten Einsatzsteuerung, vgl. Absatz 1 Satz 2) ist nicht zwingend, eine externe Stelle zur unabhängigen Sichtung zu betrauen (BVerfGE 141, 220 – Rn. 129). In diesen Fällen ist sicherzustellen, dass in Zweifelsfällen eine Klärung der Kernbereichsrelevanz durch den behördlichen Datenschutzbeauftragten erfolgt (BVerfGE 165, 1 - Rn. 119). Dies gewährleistet eine aus der operativen Aufgabenwahrnehmung herausgelöste fachkundige Prüfung, die Zweifelsfragen innerbehördlich unabhängig klärt. Daneben ist eine externe unabhängige Kontrolle durch den unabhängigen Kontrollrat eröffnet, der sich der Verwaltungspraxis etwa im Rahmen einer dies betreffenden administrativen Strukturkontrolle annehmen kann. Die Möglichkeit des Unabhängigen Kontrollrats zu Strukturkontrollen dient einer nachhaltigen Einwirkung auf die Verwaltungspraxis sogar effektiver, als eher punktuelle und unsystematische Wahrnehmung von Individualrechtsschutz in Verwaltungssachen.

Die nach Satz 2 ermöglichte Option, anstelle des behördlichen Datenschutzbeauftragten auch – statusgleich – einen anderen Bediensteten mit der Funktion zu betrauen, ermöglicht eine flexible Praxisgestaltung, die berücksichtigt, dass der behördliche Datenschutzbeauf-

tragte nicht notwendig Volljurist ist, die spezielle Funktion spezielle Fachkunde bedingt und sich das Modell eines aufgabenspezifischen Funktionsträgers im Modell des G 10-Juristen (vgl. § 4 Absatz 1 Satz 2 G 10) in der BfV-Praxis bewährt hat. Der Status nach § 6 Absatz 3 BDSG gewährleistet ein aus den Fachinteressen der durchführenden Organisationseinheiten herausgelöstes, sachlich neutrales Rechts-Controlling. Es steht der Amtsleitung frei, je nach Arbeitsaufkommen erforderlichenfalls auch mehrere Personen als Aufsichtsbedienstete zu bestellen.

Zu Absatz 6

Absatz 6 trifft ein Nutzungsverbot unter Erlaubnisvorbehalt, um das nach Absatz 4 vorgesehene Prüfverfahren wirksam zu gestalten. Satz 2 erlaubt in Abwägung mit gegenläufigen Interessen eine – ebenfalls verfahrensgesicherte – vorläufige Nutzung. Gefahr im Verzug ist dabei gleichermaßen, wenn die Informationen für Anschlussermittlungen benötigt werden, die bei Verzögerung vereitelt würden, wie auch bei Gefahr für andere Rechtsgüter, zu deren Abwendung unverzügliche Nutzung der Informationen zwingend ist.

Zu Absatz 7

Der Absatz trifft Folgeregelungen zur Löschung und deren Dokumentation. Die Löschung der Protokolldaten lehnt sich an die Regelung in § 21 Absatz 5 an.

Zu § 32 (Schutz von zeugnisverweigerungsberichtigten Berufsgeheimnisträgern)

Die Regelung verbreitert den Anwendungsbereich des Berufsgeheimnisschutzes im bisherigen § 3b G 10 (also für die Telekommunikationsüberwachung) auf alle nachrichtendienstlichen Mittel.

Der Anwendungsausschluss in Absatz 4 entspricht der bisherigen Verstrickungsregelung in § 3 Absatz 4 G 10. Der Beteiligtenbegriff ist gefahrenabwehrrechtlich zu verstehen, erfasst also Sachverhalte der objektiven Förderung der Bedrohungen, wobei auch mehrstufige Wirkungsketten einbezogen sind, beispielsweise verschleiernde Transaktionsketten bei Finanzierungssachverhalten oder Nachrichtenmittler. Gefahrenabwehrrechtlich ist eine subjektive Tatseite grundsätzlich unmaßgeblich.

Absatz 5 enthält Folgeregelungen, wenn bei Berufsgeheimnisträgern Informationen erhoben worden sind, die nach Absatz 1 bis 4 schutzwürdig sind (die Schutzwürdigkeit ist in Absatz 2 durch eine Abwägung beschränkt und mit Absatz 4 wegen Verstrickung ausgeschlossen). Die Folgeregelung ist dabei nicht auf den in Absätzen 1 bis 3 geregelten Sachverhalt beschränkt, dass die Informationen durch Maßnahmen gewonnen worden sind, die gegen den Berufsgeheimnisträger gerichtet sind. Einbezogen ist also auch die Informationsgewinnung durch Maßnahmen, die gegen andere Personen gerichtet sind, wenn an dem überwachten Sachverhalt auch Berufsgeheimnisträger beteiligt sind und diese dabei Informationen weitergeben, über die sie das Zeugnis verweigern dürften (vgl. § 3b Absatz 1 Satz 5 G 10, hier schutzerweiternd auch auf die Berufsgeheimnisträger nach Absatz 2 erstreckt).

Zu Absatz 1

Die Regelung entspricht § 3b Absatz 1 G 10.

Zu Absatz 2

Die Regelung entspricht § 3b Absatz 2 G 10. Die Unterscheidung zwischen absolut geschützten Berufsgeheimnissen (Absatz 1) und relativ geschützten (Absatz 2) wird beibehalten. Dem Gesetzgeber steht nicht frei, auch insofern den absoluten Vorrang vor den herausragenden Schutzgütern des Verfassungsschutzes einzuräumen (vgl. BVerfGE 129, 208 – Rn. 268). Die neue Regelung trifft gleichwohl auch insoweit eine inhaltlich bestimmtere

Regelung, indem die bisherige allgemeine Abwägungsformel konkretisiert wird. Zu-sätzlich enthalten § 9m Absatz 1 Nummer 1 und § 9n Absatz 1 Satz 1 Nummer 8 auch neue verfahrensmäßige Sicherungen, einschließlich unabhängiger Vorabkontrolle.

Zu Nummer 1

Dazu knüpft Satz 2 Nummer 1 an die abgestufte Klassifizierung des Gemeinwohlinteresses im neuen § 3 Absatz 6 an und legt fest, dass unterhalb der Schwelle erheblicher Beobachtungsbedürftigkeit generell das Schutzinteresse des Berufsgeheimnisses überwiegt. Einen ähnlichen Ansatz – wenn auch nicht gleichermaßen strikt – enthält bereits § 160a Absatz 2 Satz 1, letzter Halbsatz StPO.

Zu Nummer 2

Die kumulativ hinzutretende Nummer 2 entspricht der Regelung im bisherigen § 3b Absatz 2 G 10.

Zu Absatz 3

Die Regelung entspricht dem bisherigen § 3b Absatz 3 G 10.

Zu Absatz 4

Die Regelung entspricht dem bisherigen § 3b Absatz 3 G 10.

Zu Absatz 5

Der Absatz trifft eine neue Schutzregelung zur wirksamen Ausgestaltung des Berufsgeheimnisschutzes. Erfasst werden Maßnahmen, bei denen beim Berufsgeheimnisträger dem Berufsgeheimnis unterfallende Informationen gewonnen worden sind, ohne dass solcher Informationsfluss vorausgesehen und daher bereits auf der Erhebungsebene steuernd vermieden wurde. Hier muss der gebotene Schutz dann auf der Verwertungsebene erfolgen. Ein Beispiel wäre die Informationsgewinnung bei einem Funktionär einer extremistischen Vereinigung, der beruflich als Rechtsanwalt tätig ist. Die Aufklärung zielt auf Erkenntnisse, die beim Betroffenen bei Gelegenheit der Funktionärstätigkeit anfallen. Wenn er – ohne gezieltes Hinwirken des BfV auf solche Informationsgewinnung – auch Informationen, die dem Berufsgeheimnis unterliegen, offenbart, folgt aus Absatz 5 die Unverwertbarkeit und Löschungspflicht (bisher lediglich begrenzt auf einen Teil der Berufsgeheimnisträger und nur beschränkt auf G 10-Maßnahmen in § 3b Absatz 1 Satz 2 bis 4 G 10 geregelt). Nicht erfasst ist die Informationsgewinnung bei Dritten, die nicht Berufsgeheimnisträger sind, über Angelegenheiten, über der Berufsgeheimnisträger Verschwiegenheit wahren müsste.

Zu Unterabschnitt 3 (Verfahren bei besonderen Maßnahmen)

Zu § 33 (Anordnung von Maßnahmen)

Die Bestimmung regelt die innerbehördliche Anordnungszuständigkeit (Absatz 1) sowie querschnittliche Vorgaben zu Anordnungen (Inhalt und Dokumentation: Absätze 2 und 4). Die Anordnung ist eine innerbehördliche Einsatzfreigabe, wonach die geregelte Maßnahme im Anordnungszeitraum – ggf. auch wiederholt – durchgeführt werden darf, je nach konkretem einsatztaktischem Erfordernis. Bei bestimmten Maßnahmen ist zusätzlich auch noch die vorherige Feststellung der Anordnungsrechtmäßigkeit durch den Unabhängigen Kontrollrat für die Vollziehbarkeit der Anordnung erforderlich (§ 34).

Zu Absatz 1

Absatz 1 verknüpft die innerbehördliche Anordnungszuständigkeit mit dem Eingriffsgewicht der Maßnahme, wobei im Interesse der Rechtsklarheit jedoch auf die komplementären Stufen der Beobachtungsbedürftigkeit abgestellt wird.

Satz 2 ermöglicht technische Vorbereitungen bereits vor der Anordnung, wenn ad hoc eine zeitlich eng begrenzte Realisierungsmöglichkeit eintritt. Die technische Vorbereitung kann auch eine dafür nötige Datenverarbeitung einschließen, die durch ihren Zweck eng begrenzt bleibt. Die Besonderheit des hier geregelten Sachverhalts besteht im Eingriff in die Integrität eines informationstechnischen Systems. Ansonsten sind bloße technische Vorbereitungen auch ohne spezielle gesetzliche Regelung bereits vor Maßnahmeanordnung zulässig.

Zu Nummer 1

Erheblich eingreifende Maßnahmen unterliegen der Anordnung durch eine Abteilungsleitung, die dies allerdings – ggf. für bestimmte Arten von Maßnahmen – delegieren kann und zwar entweder an ihre Regelvertretung – also eine Gruppenleitung – oder einen Volljuristen. Die Delegation ist nicht lediglich Abwesenheitsvertretung, sondern mit der Übertragung (in deren – ggf. begrenzten – Rahmen) Regelzuständigkeit. Auch bei solcher Lösung verbleibt der Abteilungsleitung eine besondere Organisationsverantwortung.

Zu Nummer 2

Die Anordnung wenigstens besonders erheblich eingreifender Maßnahmen ist grundsätzlich der Amtsleitung vorbehalten. Zusätzlich sind ihr die in Buchstabe e aufgeführten außergewöhnlichen Maßnahmen vorbehalten (auch soweit nur erheblich eingreifend). Die Amtsleitung einer Behörde von rund 5.000 Mitarbeitenden ist allerdings eine prinzipiell strategische Führungsebene, deren Ressourcen möglichst nicht in operativen Einzelentscheidungen verzettelt werden sollten. Deshalb eröffnet die Regelung eine Delegation, die jedoch beschränkt bleibt auf Abteilungsleitungsebene. Die Delegation muss nicht an eine Person erfolgen, sondern kann auch die jeweils für den Vorgang zuständige Abteilungsleitung berufen. Mit der grundsätzlichen Anbindung an die Amtsleitung bleibt diese in einer besonderen Organisationsverantwortung zur angemessenen Anordnungspraxis.

Zu Absatz 2

Absatz 2 enthält die nötigen Festlegungen zum Eingriffsrahmen der Maßnahme.

Zu Nummer 1

Nummer 1 orientiert sich an § 10 Absatz 3 Satz 1 G 10. Die Schriftlichkeit (vgl. § 10 Absatz 2 Satz 1 G 10) folgt nunmehr aus Absatz 4 Satz 1. Allerdings kann eine Eilanordnung durch die Amtsleitung nötigenfalls zunächst auch mündlich ergehen, ist im Anschluss dann aber schriftlich zu dokumentieren.

Der festzulegende Aufklärungsgegenstand wird speziell durch die aufzuklärende Bedrohung bezeichnet. Die Präzisierung, dass bei personengerichteten Maßnahmen konkrete Angaben „soweit möglich“ zu machen sind, folgt neuerer Regelungsweise, so etwa in § 45 Absatz 4 Nummer 1 BKAG oder § 100e Abs. 3 Nr. 1 StPO. Die Vorgabe betrifft Maßnahmen, die als solche auf Personen ausgerichtet sind, wie eine Observation oder eine Telekommunikationsüberwachung.

Bei Maßnahmen, die als solche auf Beobachtungsobjekte oder extremistischen Szenen gerichtet sind, ist das betreffende Aufklärungsfeld in der Anordnung anzugeben. Dies stellt Satz 3 klar. Danach ist beim Einsatz menschlicher Quellen Anordnungsgegenstand nicht der individuelle Einsatz einer bestimmten Person, sondern die Freischaltung der mit dem

Aufklärungsfeld bezeichneten Beobachtungsobjekte für das Einsatzmittel. Die tatbestandlichen Voraussetzungen solchen Einsatzes sind grundsätzlich nicht abhängig von der Individualität des personellen Einsatzmittels, sondern der Beobachtungsbedürftigkeit der aufklärungsgegenständlichen Bedrohungen. Soweit tatbestandlich erhöhte Schwellenanforderungen in Ansehung besonderer Vertrauensbeziehungen bestehen (§ 17 Absatz 2 Satz 2) kann dies auch in allgemeiner Form in die Freischaltungsanordnung, die dann auch zu solcher Einsatzsteuerung befugt, aufgenommen werden.

Die Einsatzanordnung dient einer die Einsatzvoraussetzungen gewährleistenden Rahmenvorgabe. Dieser Rahmen ist bei Vertrauenspersonen nicht notwendig auf enumerative Beobachtungsobjekte beschränkt, sondern kann auch bestimmte extremistische Szenen betreffen. Der benannte Aufklärungsgegenstand muss lediglich – kontrollierbar – gewährleisten, dass die Einsatzrichtung Bedrohungen sind, deren Beobachtungsbedürftigkeit den Einsatz des Mittels rechtfertigen. Demzufolge ist allgemein, aber speziell auch beim Einsatz in der Spionageabwehr eine abstrakte Umschreibung des Aufklärungsfeldes hinreichend. Dies gewährleistet Flexibilität in der näheren Einsatzsteuerung und speziell in der Spionageabwehr auch die Absicherung gegen Indiskretionsrisiken, die in diesem Einsatzfeld mit besonders hohen persönlichen Risiken für die die eingesetzte Person verbunden wären.

Ist Aufklärungsgegenstand eine Quelle, beispielsweise im Hinblick auf Nachrichtenehrlichkeit oder einem Verdacht funktionsgefährdender Tätigkeit, ist ebenso keine Individualisierung dieser Person vorgesehen (Satz 4), d.h. als Aufklärungsfeld ist hier abstrakt anzugeben, dass die Maßnahme auf Aufklärung zu einer Quelle zielt.

Vom Aufklärungsgegenstand des Einsatzes sind einzelne Beschaffungsaufträge während des Einsatzes zu unterscheiden, die auch bei Vertrauenspersonen gezielt Personen betreffen können. Solche Beschaffungsaufträge können nicht in der Einsatzanordnung vorstrukturiert werden, sondern folgen aus den während des Einsatzes eintretenden Bedarfen und Möglichkeiten. Wenn in der Einsatzanordnung auch qualifizierte Einsätze nach § 17 Absatz 2 Satz 2 freigegeben werden, kann der Unabhängige Kontrollrat dies aber mit Maßgaben versehen, etwa zum Nachbericht für den Fall, dass von dieser Option Gebrauch gemacht wird. Auch im Übrigen kann der Unabhängige Kontrollrat durch administrative Strukturkontrollen, den Quelleneinsatz in einem Aufklärungsfeld unter Wahrung des Quellenschutzes kontrollieren, um etwa der Frage eines womöglichen übermäßigen Einsatzes nachzugehen. In der Realität ist dies angesichts der typischerweise sehr schwierigen Zugangslagen allerdings ein außerordentlich praxisfernes Szenario.

Kein Gegenstand des Anordnungstenors ist die Identität einer eingesetzten Vertrauensperson. Ebenfalls nicht Gegenstand des Anordnungstenors oder einer Anordnungsbegründung sind Angaben, welche eine Offenbarung der Identität ermöglichen (vgl. auch (§ 13 Absatz 4 UKRat-Gesetz). Nach Satz 4 sind auch bei gegen eine Quelle gerichteten Maßnahmen keine Angaben zur Identität der Person zu machen.

Soweit Angaben zu einer sonstigen Zielperson erfolgen, dienen sie der Individualisierung der Maßnahmerichtung. Dies gilt auch für die Angabe zur Anschrift. Damir erfolgt keine Fixierung der Anordnung auf die Beibehaltung dieser Wohnanschrift. Verzieht die Zielperson während des Anordnungszeitraums, kann die Maßnahme also ohne neue Anordnung fortgesetzt wrden.

Zu Nummer 2

Nummer 2 entspricht § 10 Absatz 2 Satz 2 G 10. Der Anordnungsinhalt muss insoweit insbesondere auch Befugnisanforderungen reflektieren, speziell maßgebliche zeitliche Schwellen (vgl. z.B. § 20) oder besondere Qualifikationen bzw. Begrenzungen (vgl. §26). Einsatzdauer und Anordnungsbefristung sind dabei unterschiedliche Festlegungen. Es kann beispielweise angeordnet werden, in den nächsten 6 Monaten (Befristung)

Observationen auch durchgehend länger als 48 Stunden, die aber keine Woche erreichen dürfen (Dauer), durchzuführen.

Zu Nummer 3

Die bereichsspezifischen Vorgaben sind aus dem bisherigen Artikel 10-Gesetz übernommen, allerdings nicht § 9 Absatz 3 Satz 2, 2. Halbsatz. Die Festlegung eines Zielgeräts bei der sogenannten Quellen-TKÜ war eine aus Regelungen der Online-Überwachung übernommene Vorgabe. Erfolgt die Kommunikationsüberwachung künftig unter Eingriff in ein Informationstechnisches System, trifft Nummer 4 die speziellen Anforderungen an den Anordnungsinhalt. Welche Anschlusskennung überwacht wird, ist dafür grundsätzlich unerheblich. Die Nummern sind also nicht kumulativ anzuwenden, vielmehr ist Nummer 4 insoweit dann lex specialis.

Bei der Überwachung des des Brief- und Postverkehrs erfolgt die Angabe der Zielperson nach Absatz 2 Nummer 1 möglichst unter Angabe der Anschrift. Die Anschriftenangabe dient dabei – wie bei anderen Überwachungsmaßnahmen – zur Indivdualisierung der Person. Verzieht die Person während des Anordnungszeitraums, bleibt die Maßnahme – beispielsweise eine Observation – davon unberührt. Dies gilt auchbei der Postüberwachung. Auch hier gilt die Anschriftenangaben nicht zur Eingrenzung des zu überwachenden Sachverhalts, sondern zur Individualisierung der Zielperson. Auch hier kann nach einem Umzug die Maßnahme fortgesetzt werden, nunmehr unter Einbezug der neuen Zustellanschrift, ohne dass dazu eine neue Anordnung nötig wäre. Dies kann zur Klarstellung in der Tenorierung der Anordnung bei Bezeichnung der zu überwachenden Sendungen klargestellt werden, indem dabei auf die jeweilige Wohnanschrift des Betroffenen abgestellt wird.

Zu Nummer 4

Die Nummer enthält maßnahmespezifisch erforderliche Angaben. Die möglichst genaue Bezeichnung des informationstechnischen Systems dient der Steuerung der Maßnahmerichtung. Danach ist eine konkretisierende Angabe zum informationstechnischen System spezifisch dort nötig, wo die Zielperson das System eines Dritten nutzt (§ 25 Absatz 2 Satz 1 Nummer 2 und § 26 Absatz 3 i.V.m. § 22 Absatz 3 Satz 1 Nummer 3), da hier über die Bezeichnung der Person des Dritten womöglich nicht die nötige Begrenzung des Eingriffsumfangs auf das zur Aufklärung erforderliche zu erreichen ist (wenn die Zielperson nur bestimmte IT-Systeme des Dritten als eigene privat nutzen kann). Bei den der Zielpersonen gehörenden, privat eigengenutzten IT-Systemen kann für die Spezifizierung dagegen regelmäßig der allgemeine Bezug auf die jeweils im Eigentum der Zielperson stehenden Geräte (die im Anordnungszeitraum wechseln können) genügen.

Zu Nummer 5

Die Nummer enthält maßnahmespezifisch erforderliche Angaben.

Zu Absatz 3

Der Absatz ermöglicht eine Flexibilisierung der Durchführung in Fällen, in denen absehbar in der Durchführung mit Anpassungsbedarfen zu rechnen ist. Solche Öffnung unterliegt mit der Anordnung der Vorabkontrolle des Unabhängigen Kontrollrats, der zudem nach § 34 Absatz 2 eine nachgängige Kontrolle zur Wahrnehmung dieses flexibilisierten Durchführungsrahmens vornimmt, die aufwandsreduzierend typischerweise ohne zusätzliches Verfahren mit der Prüfung einer Verlängerungsanordnung verbunden werden kann.

Zu Nummer 1

Unter Umständen kann aufgrund üblicher Vorgehensmethodik des nachrichtendienstlichen Gegenübers bereits im Anordnungszeitpunkt damit zu rechnen sein, dass weitere Personen in den Vorgang verstrickt sein dürften, ohne dass dazu bereits individualisierende Er-

kenntnisse vorliegen. Beispielsweise erfolgen Finanzierungstransaktionen nach nachrichtendienstlichen Erfahrungen unter Umständen zur Verschleierung der Attribution im Wege von Überweisungsketten mit eingebundenen Strohpersonen. Hier wäre sehr aufwändig jeweils ein neues Anordnungs- und Vorabkontrollverfahren durchzuführen. Deshalb wird hierzu die Möglichkeit eingeräumt, bereits in der Anordnung die Durchführungspraxis entsprechend zu öffnen.

Zu Nummer 2

Die Nummer betrifft den Fall, dass eine in die Bedrohung verstrickte Person zur Kommunikation das Telefon eines Unbeteiligten benutzt. Eine solche Anordnung ist dann auf einen bestimmten Anschluss mit einer bestimmten Kennung beschränkt (beispielsweise wenn nur Zugriff auf einen Festnetzanschluss besteht und nicht ohne weiteres davon auszugehen ist, dass die verstrickte Person beispielsweise auch das Mobiltelefon des Unbeteiligten mitbenutzen kann). Wenn aufgrund der konkreten Umstände hingegen anzunehmen ist, dass die verstrickte Person, etwa wegen eines Vertrauensverhältnisses, auch Zugriff auf weitere Telefone des Unbeteiligten hat, kann die Anordung auch künftig bekannt werdende weitere Anschlüsse in die Überwachung einzubeziehen.

Zu Absatz 4

Der Absatz begrenzt den zeitlichen Freigaberahmen differenzierend unter Berücksichtigung der Besonderheiten von Maßnahmen (und abhängig vom Eingriffsgewicht (Nummern 2 bis 4).

Nummer 1 berücksichtigt zum Einsatz von Vertrauenspersonen und Verdeckten Bediensteten (Buchstabe b) den hohen Aufwand zum Erschließen des Informationszugangs mit dem typischerweise einhergeht, dass längerfristig operierende Strukturen aufzuklären sind, so dass die aufklärungsrechtfertigenden Voraussetzungen typischerweise stabil auf längere Zeit vorliegen. Ähnliches gilt für den technischen Informationszugang zu informationstechnischen Systemen (Buchstabe e), wobei allerdings der Vollzugriff auf ein privates IT-System wegen des besonderen Eingriffsgewichts gleichwohl einer engeren Befristung unterliegt (Nummer 2 Buchstabe b). Die weiteren in Nummer 1 aufgeführten Mittel beziehen sich gleichermaßen typischerweise auf längerfristig bestehende Aufklärungslagen und Einsatzmittel, die einem typischerweise dauerhaften Erkenntnisbedarf dienen, etwa bei der Kommunikationsüberwachung nachrichtendienstlicher Zielpersonen, die anders als etwa Observationsbedarf nicht von zeitlich begrenzten Überwachungsbedarfen veranlasst ist. Deshalb ist hier ein gesetzlicher Höchstrahmen der Anordnung von einem Jahr sachgerecht. Weicht ein konkreter Vorgang von der typisiert angenommenen Stabilität der Einsatzrechtfertigenden Voraussetzungen ab und muss daher ausnahmsweise in engerer Periodiziät im Anordnungsverfahren überprüft werden, dann darf der Höchstrahmen in diesem konkreten Fall nicht ausgeschöpft werden. Entsprechendes gilt für die unabhängige Vorabkontrolle in deren Rahmen der Unabhängige Kontrollrat zur Rechtmäßigkeitssicherung auch Maßgaben zur Anordnungsdauer treffen kann, die von der ihm vorgelegten Anordnung abweichen. Im Übrigen ist eine Maßnahmen nach Satz 3 in jedem Fall – und unabhängig von der Anordnungsdauer – einzustellen, wenn die Voraussetzungen entfallen sind.

Nummern 2 bis 4 treffen kürzere Anordnungsvorgaben einerseits für stärker situativ geprägte Maßnahmen, deren Einsatzvoraussetzungen mithin nicht gleichermaßen stabil sind (Nummer 2 Buchstabe a), andererseits aufgrund des hohen Eingriffsgewichts (Nummer 2 Buchstabe und Nummer 4. Die nähere Dauer ist dabei zudem nach Eingriffsgewicht gestuft. Wegen der allgemein für die Fristen zur technischen Aufklärung von IT-Systemen nach Nummer 1 Buchstabe e geltenden Erwägungen – hoher Realisierungsaufwand, Einsatz typischerweise zur Aufklärung längerfristig operierender Strukturen – erscheint die „Online-Durchsuchung“ für die Höchstdauer einer Anordnung in Nummer 2 sachgerecht zugeordnet.

Die Anordnung gibt den erforderlichen Einsatz eines nachrichtendienstlichen Mittels für einen bestimmten Zeitraum frei. Hiervon zu unterscheiden ist die Durchführung der Maßnahme, die einsatztaktischen und situativen Gesichtspunkten folgt, etwa danach, wie eine Maßnahme durchführbar ist und wann sie wertige Erkenntnisse erwarten lässt. Eine Anordnung kann also beispielsweise lauten, dass in den kommenden 6 Monaten Observationen gegen eine bestimmte Person auch länger als 48 Stunden (aber weniger als eine Woche) durchgeführt werden dürfen. Die Einsatzentscheidung wird dann in dem mit der Anordnung eröffneten Einsatzrahmen nach operativen Erfordernissen in den dazu zuständigen Organisationseinheiten getroffen. Dort ist auch über eine vorfristige Beendigung nach Satz 3 zu entscheiden.

Zu Absatz 5

Absatz 4 regelt die Dokumentation von Anordnung und Durchführung. Zur Begründung der Anordnung gehören auch Angaben, die die Erforderlichkeit der Maßnahme erschließen, also einerseits Erkenntnisbedarf und Erkenntnisziele des Einsatzes sowie andererseits Eignung des Einsatzes und ggf. sonstige Zugangslage. Die Durchführungsdokumentation muss nicht gesondert erfolgen, sondern kann sich mit den angefallenen Materialien erschließen. Nach dem Grundsatz der Wirtschaftlichkeit (§ 7 BHO) sind Dokumentationsaufwände möglichst gering zu halten. Bei technischen Maßnahmen sind jedenfalls Beginn und Ende festzuhalten.

Zu § 34 (Unabhängige Vorabkontrolle)

Die Regelung sieht für Maßnahmen, bei denen damit zu rechnen ist, dass sie auch höchstprivate Informationen erfassen, die in diesen Fällen verfassungsrechtlich gebotene (BVerfGE 162, 1 – Rn. 214, 217) Vorabkontrolle der betreffenden Anordnung durch eine unabhängige Stelle vor. Dieser Maßstab ist nicht deckungsgleich mit den Kriterien der Eingriffsgewichtung (dazu vgl. § 26). Beispielsweise bei einer – erheblich eingreifenden – Observation unter Einsatz technischer Mittel ist nicht per se mit höchstprivaten Informationen zu rechnen, dies ist vielmehr situationsbedingt. Wenn etwa ein Treff eines Bediensteten eines fremden Nachrichtendienstes mit seiner in Deutschland geführten Quelle überwacht wird, um Übergaben festzustellen, induziert auch ein Treff im nichtöffentlichen Raum nicht, dass Höchstprivates ausgetauscht werden wird. Die nichtöffentliche Situation spricht für ein verdecktes Vorgehen, nicht für höchstprivate Kommunikationsinhalte.

Auch bei Unternehmensauskünften kann unter Umständen mit einer erheblichen Informationsbreite zu rechnen sein, die eine Beschränkung auf Fälle erheblicher Beobachtungsbedürftigkeit bedingt (§ 11 Absatz 5), ohne dass dies eine Informationstiefe ins Höchstprivate indiziert (dies kann im Einzelfall erreicht werden, die Maßnahmetypik ist davon aber nicht geprägt). So hat das Bundesverfassungsgericht etwa zu Finanzauskünften ausdrücklich herausgestellt, dass eine ex-ante-Kontrolle durch eine neutrale Stelle nicht verfassungsrechtlich geboten ist (BVerfGE 120, 274 - Rn. 330). Für den Schutzbereich des Artikel 10 GG wird angesichts dessen besonderen Vertraulichkeitsschutzes dennoch auch zu bloßen Verkehrsdatenauskünften am Erfordernis unabhängiger Vorabkontrolle festgehalten (Absatz 1 Nummer 5).

Bei der technischen Standortfeststellung wird erst die Langfristüberwachung nach § 20 Satz 1 Nummer 2 vom Erfordernis unabhängiger Vorabkontrolle erfasst, da mit höchstprivaten Informationen erst zu rechnen ist, wenn infolge langer Überwachung verfestigte Verhaltensmuster erkennbar werden, die besondere örtliche Bezüge der Person erschließen, die auch auf persönliche Beziehungen hindeuten können.

Die Maßnahmedauer ist - wie bereits bei der materiellen Gewichtung - auch für das zusätzliche Erfordernis der Verfahrenssicherung durch Vorabkontrolle bedeutsam (a.a.O. Rn. 220). Allgemein induziert die Schwelle des besonders erheblichen Eingriffsgewichts aber zugleich die Erwartbarkeit auch höchstprivater Informationen, weshalb diese Maßnahmen

durchgängig unabhängiger Anordnungskontrolle unterliegen. Diese grundsätzliche Stufenanknüpfung legt auch die Verfassungsrechtsprechung nahe (vgl. BVerfGE 162, 1 – Rn. 361 unter Bezug auf „tief“ eingreifende Maßnahme, wobei das Gericht vorausgegangen abstufend zwischen einerseits „eher geringeren bis mittleren Eingriffen“ und andererseits „tief“ in die Privatsphäre eindringenden Eingriffen unterscheidet, Rn. 357).

Bei Befugnissen, die abhängig von der Durchführungsdauer die Schwelle zur unabhängigen Vorabkontrolle erreichen, muss die Entscheidung des Unabhängigen Kontrollrats grundsätzlich vor Erreichen dieser Zeitschwelle, jedoch nicht zwingend bereits vor Maßnahmebeginn vorliegen. Folglich wäre eine Maßnahme mit Erreichen dieser Zeitschwelle einzustellen, wenn in diesem Zeitpunkt keine Vollziehbarkeit nach § 31 vorliegt. In jedem Fall ist die Entscheidung des Unabhängigen Kontrollrates aber möglichst frühzeitig einzuholen, um seine Prüfungsmöglichkeiten nicht ohne Sachgrund zu verkürzen. Insbesondere darf nicht eine Situation der Gefahr im Verzug – also das Erfordernis einer Eilanordnung – geradezu mutwillig herbeigeführt werden. Es kann allerdings gute Gründe haben, eine Maßnahme zunächst zu beginnen, etwa um die begrenzten Bearbeitungskapazitäten effizient einzusetzen oder um zu testen, inwiefern die Maßnahme überhaupt wertige Erkenntnisse erbringt. Ggf. wird sie dann bereits abgebrochen bevor ein Kontrollverfahren zeitlich nötig würde. Dies entlastet alle Beteiligten von unnötigen Verfahrensaufwänden, auch den Unabhängigen Kontrollrat.

Abgelöst von dieser Schwelle der Eingriffsgewichtung besitzen bestimmte Einsatzmittel unter Umständen bereits maßnahmetypisch die Potenzialität des Zugangs auch zu Höchstprivatem. Hier kommt es dann nicht erst auf ein besonders erhebliches Eingriffsgewicht an. Dies betrifft das heimliche Betreten von Privatwohnungen sowie den länger andauernden Einsatz von Vertrauenspersonen oder Verdeckten Bediensteten ebenso wie Internetermittlungen auf Basis vertieften Vertrauens, für die deshalb das Erfordernis der unabhängigen Anordnungskontrolle auch bei nur erheblich eingreifenden Maßnahmen gilt (Absatz 1 Nummern 1 bis 3). Zudem kommt der unabhängigen Anordnungskontrolle nach Nummer 10 auch dort eine absichernde Funktion zu, wo tatbestandliche Unbestimmtheit ein spezifisches Risiko von Fehlentwicklungen belässt (§ 26) oder qualifiziert eingreifende Mittel sich in der Erprobung befinden (§ 15 Absatz 3 Satz 2).

Im Falle beschaffter informationstechnischer Speicher ist grundsätzlich keine Vorabkontrolle vorgesehen, da hier nicht bereits in der Maßnahmetypik die Gewinnung höchstprivater Informationen angelegt ist, etwa wenn Geschäftsvorgänge in Proliferationssachen oder Organisationsstrukturen von extremistischen Personenzusammenschlüssen erforscht werden. Ergibt sich aus den Umständen des Einzelfalls allerdings die Erwartung besonders erheblich eingreifender Informationsgewinnung, ist die Vorabkontrolle nötig (Nummer 7).

Zur Kontrolle sind die für die Prüfung erforderlichen Informationen vorzulegen. Dies ist in jedem Fall die Anordnung samt – umfassender – Begründung (deren Zweck es gerade ist, zu sämtlichen Anordnungsvoraussetzungen deren Vorliegen überzeugungskräftig darzulegen).

Besondere Zurückhaltung ist nach § 13 Absatz 4 UKRat-Gesetz bei der Identität von Vertrauenspersonen angezeigt, die oftmals als „Verräter“ in militantem Umfeld – verbunden womöglich mit einem Fememordrisiko – eingesetzt werden und hiernach ein außerordentliches Bedürfnis zur Vertraulichkeit haben, auch als Grundlage ihrer Zusammenarbeitsbereitschaft. Entsprechendes gilt ebenso für den verdeckten Einsatz eigener Bediensteter. Dieses Funktionserfordernis zum Schutz der herausragenden Rechtsgüter des Verfassungsschutzes geht selbst parlamentarischer Kontrolle vor (BVerfGE 146, 1). Für das Anordnungskontrollverfahren nach § 31 ist die Art des Einsatzmittels, grundsätzlich jedoch nicht seine Individualisierung bedeutsam. Demgemäß wird die Identität einer Vertrauensperson in Anträgen nach § 45 Absatz 4 BKAG nicht genannt. Dies ist nach § 14 Absatz 4 UKRatG ebenso bei Anwendung des § 32 geboten. Wenn der Unabhängige Kontrollrat in ganz besonderen Ausnahmesachverhalten Informationen zur Person zwingend benötigt,

bleibt im jeweiligen Verfahren zu klären, wie dem Informationsbedarf schonend Rechnung getragen werden kann, ohne die Identität der eingesetzten Person zu offenbaren und auch ohne die Identitätsoffenbarung zu ermöglichen (speziell mit abstrahierten Ergänzungsauskünften).

Kontrollgegenstand ist die jeweilige Anordnung, also auch Verlängerungsanordnungen. Werden Maßnahmen über die in § 30 Absatz 3 Satz 1 geregelten Fristen hinaus verlängert, bedarf es jeweils neuerlicher Anordnung und damit im Anwendungsbereich des § 31 zugleich auch jeweils neuerlicher Rechtmäßigkeitsfeststellung vor Durchführung der (Verlängerungs-)Anordnung.

Neben der Vorabkontrolle bestimmter Maßnahmen nimmt der Unabhängige Kontrollrat im Übrigen ebenso gerichtsähnliche Kontrollfunktionen bei anderen speziellen Sachverhalten wahr (§ 29 Absatz 3 UKRat-Gesetz). Außerdem integriert er in seinem Kompetenzrahmen die Datenschutzkontrolle der operativen Aufgabenwahrnehmung des BfV (§ 69 Absatz 2 Nummer 1), auch mit den verbundenen Spezialaufgaben (Anhörung bei Errichtungsanordnungen gem. § 41 Absatz 2 Satz 1; subsidiäre Auskunftserteilung gem. § 71 Absatz 4).

Zu Absatz 1

Zu Nummer 1

Die Regelung schützt die besondere Privatsphäre der Privatwohnung verfahrensmäßig durch unabhängige Vorabkontrolle. Anders als bei der grundgesetzlich in Art. 13 Abs. 4 GG speziell geregelten Wohnraumüberwachung ist die Vorabkontrolle bei Privaträumen nicht allgemein institutionell nicht auf die Justiz beschränkt und kann hier vom Unabhängigen Kontrollrat ausgeübt werden. Anders als bei Privaträumen ist bei Betriebs- und Geschäftsräumen solche aufwändige Verfahrensvorkehrung nicht notwendig.

Zu Nummer 2

Erfolgt bei verdeckten Internetermittlungen eine Vertrauensvertiefung durch Kontaktnahme in physischer Präsenz oder durch mehrfach wiederholte persönliche Zuwendung und wird die verdeckte Informationsgewinnung gegen diese Zielperson unter Ausnutzung dieses vertieften Vertrauens dauerhaft fortgesetzt, besitzt die Beziehung das Potenzial einer Entwicklung, die höchstprivate Informationen auch abgelöst von der Unbefangenheit der Netzkultur, sondern basierend auf schutzwürdigem Vertrauen einbezieht. Solche Entwicklung ist typischerweise nicht Ziel des Kontaktes, es kann aber nötig sein, dass der Bedienstete sich dem öffnet, um die Beziehung nicht zu stören. Da hiernach maßnahmebedingt mit dem Anfall auch höchstprivater Informationen zu rechnen ist, wird dann eine unabhängige Kontrolle der Maßnahmevoraussetzungen (erhebliche Beobachtungsbedürftigkeit) erforderlich. Die 6-Monats-Schwelle orientiert sich pauschalierend an der Einsatzregelung zu Vertrauenspersonen.

Zu Nummer 3

Zu Buchstabe a

Die unabhängige Vorabkontrolle kommt für eine erste Phase der Erprobung einer Quelle noch nicht zur Anwendung (vgl. BVerfGE 162, 1 – Rn. 351, 353). Zeitlich wird dies auf 6 Monate beschränkt, obgleich die Erprobung vor Verpflichtung regelmäßig deutlich länger dauert. Nach 6 Monaten kann aber auch während der Probephase nicht mehr davon ausgegangen werden, dass der Beschaffungsumfang typischerweise hinter dem einer verpflichteten Vertrauensperson zurückbleibt, so dass bei solcher Dauer auch während der Probephase schon eine unabhängige Anordnungskontrolle nötig wird. Der Sechsmonatszeitraum ist eine gesetzliche Pauschalierung des Stabilitätsaufbaus, die insgesamt vom Verpflichtungszeitpunkt unabhängig gilt, also auch in dem außergewöhnlichen Fall, dass eine Verpflichtung bereits zuvor erfolgen würde. Maßgeblich bei der typisierenden

Eingriffsgewichtung ist dabei nicht allein der Aspekt der Erprobung der Quelle, sondern auch das Ausmaß der Ausnutzung dauerhafter persönlicher Vertrauensbeziehungen im aufzuklärenden Umfeld. Auch insoweit ist ein nicht dauerhafter Einsatz mit Blick auf Vertrauensaufbau noch weniger eingreifend. Der vorausgesetzte Sechsmontszeitraum beginnt mit dem Zugang und Beschaffungsaufträgen zu einem Aufklärungsfeld (vgl. § 17 Absatz 2 Satz 1 Nummer 1). Maßgeblich ist mithin weder ein einzelner Beschaffungsauftrag (über solche Dauer) noch die Summe nacheinander folgender (Springer-)Einsätze in unterschiedlichen Aufklärungsfeldern.

Zu Buchstabe b

Im Falle des § 16 Absatz 5 Satz 1 Nummer 2 wird eine selbst nicht beteiligte Person zur Zielperson der sensiblen Maßnahme. Dies erfordert – unabhängig vom 6-Monats-Zeitraum nach Buchstabe a – eine besondere Verfahrenssicherung

Zu Buchstabe c

Angesichts der besonders persönlichen Vertrauensbeziehung ist ebenso abgelöst von der 6-Monats-Frist des Buchstaben a hier die Vorabkontrolle generell geboten.

Zu Nummer 4

Der absehbare Einbezug höchstprivater Vorgänge bedingt die Vorabkontrolle und bei besonders erheblich eingreifenden Maßnahmen induziert die Eingriffsgewichtung auch die Potenzialität zur Gewinnung höchstprivater Informationen.

Zu Nummer 5

Bei besonders erheblich eingreifenden Maßnahmen induziert die Eingriffsgewichtung auch die Potenzialität zur Gewinnung höchstprivater Informationen

Zu Nummer 6

Das Verfahrenserfordernis knüpft grundsätzlich an den Eingriff in den Schutzbereich des Artikel 10 GG an. Für das Telekommunikationsgeheimnis ist dies allerdings nicht pauschalierend angemessen. So ist unter Beachtung der Verfassungsrechtsprechung bereits im geltenden Recht die Bestandsdatenauskunft anhand dynamischer IP angesichts der geringen Persönlichkeitsrelevanz nicht an eine unabhängige Vorabkontrolle gebunden (vgl. § 8d Absatz 2). Dies wird beibehalten, indem die Vorabkontrolle der Auskunftsfälle auf qualifizierte Ersuchen (§ 11 Absatz 5) beschränkt wird. Nach seiner neueren Rechtsprechung ordnet das Bundesverfassungsgericht auch nicht-kommunikative Datenverkehre, die unter Nutzung von Telekommunikationsdiensten übertragen werden, dem Telekommunikationsgeheimnis zu (s.o. Begründung zu § 22 Absatz 2). Die dazu in § 22 Absatz 2 getroffene Synchronisation der materiellen Überwachungsvoraussetzungen mit §§ 23, 25, 26 wird hier für die Verfahrensvoraussetzungen nachvollzogen, indem die Fälle der Nummern 6 und 8 ebenso der unabhängigen Vorabkontrolle unterliegen.

Zu Nummer 7

Das Verfahrenserfordernis ergibt sich in Bezug auf § 22 Absatz 2 aus der nach den Einzelfallumständen erwarteten Sensitivität des Eingriffs. Die Vorabkontrolle ist im Falle des Absatzes 3 nur nötig, wenn sie nicht bereits zuvor mit Hinblick auf § 22 Absatz 2 erfolgt ist.

Zu Nummer 8

Die Vorabkontrolle erscheint wegen des Datenumfangs - speziell auch im Ergebnis irrelevanter Daten - sachgerecht. Gegenstand ist die Erhebung der Kopie. Im Falle eines Auskunftsverlangens nach § 12 Absatz 1 Satz 2 Nummer 2 sind die Voraussetzungen gegeben,

wenn zu erwarten ist, dass die Auskunft nach § 12 Absatz 1 Satz 3 durch Herausgabe einer Kopie erfolgen wird.

Zu Nummer 9

Die Vorabkontrolle ist nach der Verfassungsrechtsprechung geboten.

Zu Nummer 10

Das Erfordernis der Vorabkontrolle trägt der außergewöhnlichen Art der Maßnahme Rechnung.

Zu Nummer 11

Die Vorabkontrolle dient dem Schutz des Berufsgeheimnisses,

Zu Absatz 2

Absatz 2 trifft eine besondere Regelung zur Kontrolle einer nach § 33 Absatz 2 flexibilisierten Durchführungspraxis. Solche Flexibilisierung unterliegt einerseits bereits mit der Anordnung, also dem Grunde nach, der Vorabkontrolle des Unabhängigen Kontrollrats. Zusätzlich sind nach Absatz 2 auch die in diesem Rahmen erfolgten nachträglichen Erweiterungen zur Rechtmäßigkeitskontrolle vorzulegen. Dies kann aufwandsreduzierend typischerweise ohne zusätzliches Verfahren mit der Prüfung einer Verlängerungsanordnung verbunden werden.

Zu Absatz 3

Der Absatz ermöglicht bei Gefahr im Verzug eine vorläufige Durchführung entsprechend der bisherigen Regelung zur Eilanordnung nach § 15a G 10. Mit Einrichtung des Unabhängigen Kontrollrates als integrale Kontrollinstanz aller Nachrichtendienste des Bundes erfolgt die nähere Regelung des Eilverfahrens querschnittlich im Errichtungsgesetz. Satz 2 trifft eine besonders enge Zweckbegrenzung für Übermittlungen aus Maßnahmen der Online- und Wohnungsüberwachung, die vor unabhängiger Rechtmäßigkeitsfeststellung auf wirklich unabweisbare Fälle beschränkt bleiben.

Zu Absatz 4

Artikel 13 Absatz 4 GG erfordert eine richterliche Anordnung, weshalb hier abweichend von Absatz 1 ein Gericht vorgesehen ist. Angesichts der geringen erwartbaren Fallzahl erscheint sachgerecht hierzu in Angleichung an § 50 Absatz 1 Nummer 4 VwGO die Zuständigkeit des Bundesverwaltungsgerichts vorzusehen.

Angesichts der gegenständlichen Besonderheit dieses gerichtlichen Feststellungsverfahrens wird es in Absatz 4 besonders geregelt, dies orientiert an den etablierten Vorabkontrollverfahren im nachrichtendienstlichen Bereich, dem neuen UKRat-Gesetz sowie den Geheimschutzregelungen des § 99 Absatz 2 VwGO. Dabei steht es im Ermessen des Gerichts, die Verfahrensbeteiligten vor einer Entscheidung über den Feststellungsantrag anzuhören oder ausschließlich auf Grundlage der eingereichten Unterlagen zu entscheiden. Wie in vergleichbaren Verfahren, etwa zu richterlichen Anordnungen im Ermittlungsverfahren nach der Strafprozessordnung, wird auch vorliegend die Entscheidung durch einen einzelnen Richter adäquat, bei Eilanordnungen eventuell auch verfahrenspraktisch geboten sein. Hiergegen kann allerdings die Entscheidung des Senats beantragt werden, auch um gegebenenfalls zu grundsätzlichen Fragen eine vom gesamten Senat getragene Linie herzustellen.

Zur Kontrolle auf der Auswertungsebene (§ 31 Absatz 4 Satz 1 Nummer 2) bleibt es bei der Zuständigkeit des Unabhängigen Kontrollrats wie auch zur allgemeinen

Datenschutzkontrolle in Ansehung der Weiterverarbeitung der mit der Wohnraumüberwachung erlangten Daten. Dies hat Vorteile der breiteren Praxiserfahrung und integralen Würdigung von Kontrollvorgängen auch in ihren Zusammenhängen. Die Sonderzuständigkeit des Bundesverwaltungsgerichts für die Anordnungskontrolle ist allein verfassungsrechtlich bedingt.

Zu Absatz 5

Der Absatz trägt den gegenständlichen Besonderheiten des Feststellungsverfahrens nach Absatz 3 verfahrensmäßig Rechnung. Die Ausgestaltung erfolgt einerseits unter Anlehnung an Geheimschutzregelungen des § 99 Absatz 2 VwGO und andererseits orientiert an vergleichbaren Verfahren, etwa zu richterlichen Anordnungen im Ermittlungsverfahren nach der Strafprozessordnung oder dem Verfahren des unabhängigen Kontrollrates nach dem Gesetz über den Unabhängigen Kontrollrat. Dabei steht es im Ermessen des Gerichts, das BfV vor einer Entscheidung über den Feststellungsantrag anzuhören oder ausschließlich auf Grundlage der eingereichten Unterlagen zu entscheiden. Beteiligt ist allein das BfV, eine Beiladung der Zielperson ist naturgemäß ausgeschlossen. Grundsätzlich ist die Entscheidung durch einen einzelnen Richter adäquat, bei Eilanordnungen eventuell auch verfahrenspraktisch geboten. Hiergegen kann allerdings die Entscheidung des Senats beantragt werden, auch um gegebenenfalls zu grundsätzlichen Fragen eine vom gesamten Senat getragene Linie herzustellen.

Zu § 35 (Mitteilung an betroffene Personen)

Zu Absatz 1

Nachrichtendienste sammeln Daten grundsätzlich geheim. Der Grundsatz der Offenheit der Datenerhebung gilt für sie nicht, und sie sind von Transparenz- und Berichtspflichten gegenüber betroffenen Personen weithin freigestellt, was auch Rechtsschutz faktisch einschränkt. Diese materiespezifischen Besonderheiten sind in der Verfassungsrechtsprechung anerkannt (BVerfGE 133, 277 - Rn. 117; BVerfGE 162, 1 – Rn. 150, 240, 290). Diesen Besonderheiten tragen besondere Kontroll-strukturen Rechnung. Neben der besonderen politischen Kontrolle nach Artikel 45d GG durch das Parlamentarische Kontrollgremium ist auch eine besondere unabhängige Kon-trolle eingerichtet, die verbindlich über die Zulässigkeit qualifizierter Eingriffe (§ 34) entscheidet. Der nachrichtendiensttypischen Aufgabenwahrnehmung ohne Kenntnis betroffener Personen korrespondiert auch eine besonders intensive Wahrnehmung der betreffen-den Kontrollaufgaben, einschließlich Strukturkontrollen durch den Ständigen Bevollmächtigten des Parlamentarischen Kontrollgremiums und der unabhängigen Datenschutzaufsicht des Unabhängigen Kontrollrates, die gewährleisten, dass Durchführungspraktiken und zugrunde liegendes Rechtsverständnis sich nicht abgeschlossen innerbehördlich etablieren, sondern sich im Diskurs mit externer Kontrolle entwickeln.

Das Bundesverfassungsgericht hat in seiner jüngeren Rechtsprechung im Übrigen ausdrücklich darauf hingewiesen, dass auf der Hand liegt, dass Benachrichtigungspflichten Erfordernisse des Quellen- und Methodenschutzes entgegenstehen können (BVerfGE 169, 130 [HessVSG] - Rn. 73). Bereits vorausgegangen (BVerfGE 156, 270 - Rn. 112) hatte es ausgeführt, dass bei menschlichen Quellen bereits der subjektive Eindruck, die Vertraulichkeit sei nicht gesichert, ausreichen kann, Quellen von einer weiteren Zusammenarbeit abzuhalten und die Gewinnung neuer Quellen zu erschweren, was wiederum die Aufgabenerfüllung der Nachrichtendienste gefährden kann, die auf den langfristigen Einsatz von V-Personen im betreffenden Milieu angewiesen sind.

Im Ergebnis der zu berücksichtigenden Erwägungen werden die Mitteilungspflichten mit Absatz 1 erweitert, indem weitere Maßnahmen, einschließlich der Wohnraumüberwachung (§ 27), einbezogen werden, für die das bisher geltende Recht dies nicht vorsah. Die

Maßnahmeauswahl folgt der Eingriffsgewichtung. Erfasst werden besonders erheblich eingreifende Maßnahmen.

Nicht einbezogen wird jedoch der Einsatz menschlicher Quellen. Es wäre weithin ausgeschlossen, solche Quellen zu gewinnen, wenn sie erwarten müssten, dass ihr „Verrat“ der betroffenen Person später mitgeteilt wird. Hier ist das Persönlichkeitsrecht der Quelle und die Funktionsfähigkeit nachrichtendienstlicher Gefahrerforschung – zum Schutz herausragender Rechtsgüter – gewichtiger als das Informationsinteresse der betroffenen Person (vgl. BVerfGE 146, 1 – insbes. Rn. 112 ff.). Dem trägt auch Absatz 2 Nummer 3 Rechnung.

In diesem aufgabenspezifischen Gesamtkonzept bleibt es im Übrigen dabei, dass sich die Mitteilungspflicht ausschließlich auf die Zielperson der Überwachung bezieht und nicht auch auf Dritte, die etwa als Gesprächspartner oder als in der Wohnung mitanwesende Personen erfasst worden sind.

Zu Absatz 2

Absatz 2 regelt Sachverhalte, bei denen Mitteilungen nicht erst zurückgestellt werden, sondern bereits bei Maßnahmebeendigung zu entscheiden ist, dass keine Mitteilung erfolgt. Die Nummern 4 und 5 erfordern dabei wegen der mit unbestimmten Tatbestandmerkmalen ausgeformten Absehensgründe gemäß Absatz 5 Nummer 1 der Zustimmung des Unabhängigen Kontrollrats.

Zu Nummer 1

Die Mitteilungspflicht begründet keine Befugnis zu eingriffsvertiefenden Maßnahmen. Liegt eine zustellungsfähige Anschrift nicht vor, dürfen dazu keine eigenen Ermittlungen erfolgen, so dass hier im Ergebnis eine Mitteilung unmöglich ist. Eine bloße Melderegisterabfrage (§ 34 BMG) hat allerdings keinen die Mitteilung hindernden Eingriffsgehalt, auch wenn dabei personenbezogene Daten verarbeitet werden, aber eben begrenzt auf die direkte Erhebung der Meldeanschrift. Anders ist der Sachverhalt etwa bei einer unbekannt ins Ausland verzogenen Person. Erst recht sind weitergehende Ermittlungen zur Identität der Person von der Mitteilungspflicht nicht eröffnet. Fehlen zur Mitteilung erforderliche Informationen, ist die Mitteilung nicht möglich.

Zu Nummer 2

Bei Maßnahmen der Spionageabwehr scheidet eine Mitteilung aus, es sei denn, es kann nachträglich ausgeschlossen werden, dass eine fremde Macht in dem mit der Maßnahme aufgeklärten Sachverhalt involviert war. Mitteilungen würden ansonsten auf gegnerischer Seite eine Informationsammlung eröffnen, die über den Einzelfall hinaus Methodik des BfV bei der Spionageabwehr offenbart. Zudem könnte eine Mitteilung auch außenpolitische Irritationen im Verhältnis zur fremden Macht hervorrufen, die allgemein eher zu vermeiden sind.

Zu Nummer 3

Die Nummer trägt dem besonderen Bedarf zum Quellenschutz und der Eigensicherung Rechnung. Wenn etwa bei einer Maßnahmen nach § 23 die vorgelagerte Beschaffung des Datenträgers oder der Zugangsinformationen über eingesetzte menschliche Quellen erfolgt war, besteht das Risiko, dass die Zielperson darauf schließen kann, wenn ihr das heimliche Auslesen des Speichermediums mitgeteilt werden würde. Wirksamer Quellenschutz setzt sachnotwendig bereits beim Ausschluss von Risiken an. Dies betrifft gleichermaßen Zusammenarbeitsfälle, in denen das BfV eigene operative Maßnahmen unter Amtshilfe einer anderen Sicherheitsbehörde durch deren verdeckt eingesetzten Bediensteten durchführt.

Zu Nummer 4

Solche Sachverhalte sind eher fernliegend, aber nicht allgemein auszuschließen. Dies kann beispielsweise in Fällen des § 21 Absatz 3 Satz 1 Nummer 1 Buchstabe c gegeben sein, wenn die unbeteiligte Person im Wege der Mitteilung von der ihr bislang unbekannten Verstrickung der eigentlichen Zielperson in Bedrohungen erfährt.

Zu Nummer 5

Wenn verlässlich abzusehen ist, dass eine Mitteilungsfähigkeit dauerhaft nicht gegeben sein wird, wäre unwirtschaftlich, dennoch weitere Bearbeitungsroutinen ins Blaue fortlaufen zu lassen (vgl. BVerfGE 129, 208 – Rn. 241 f.).

Zu Absatz 3

Absatz 3 übernimmt die Regelung des § 12 Absatz 1 Satz 1 bis 3 G10, wobei der dort in Absatz 2 Satz 2 Nummer 2 verwendete Gesetzesbegriff „übergreifender“ durch den in Gesetzen üblicheren Begriff „überwiegender“ ersetzt wird, ohne dass damit eine inhaltliche Änderung verbunden wäre (vgl. Huber in Schenke/Graulich/Ruthig, Sicherheitsrecht, 2. Aufl., § 12 G 10 Rn. 32). Die u.a. auch in § 99 Absatz 1 Satz 2 VwGO verwendete Formulierung „Wohl des Bundes oder eines Landes“ ist eng auszulegen, damit auf wesentliche Interessen beschränkt, was jedoch keine Beschränkung auf die besonders gewichtigen Rechtsgüter nach § 3 Absatz 9 bedeutet. Eingeschlossen sind in jedem Fall Anforderungen der nachrichtendienstlichen Funktionssicherung, speziell der hiernach gebotene Methodenschutz.

Zu Absatz 4

Absatz 4 regelt Sachverhalte, die typischerweise zunächst zurückgestellt worden sind, bei denen nun aber Gründe eingetreten sind, von der Mitteilung endgültig abzusehen.

Zu Nummer 1

Bei Löschungsreife ist bereits nach § 38 Absatz 1 Satz 2 eine Interessenabwägung vorzunehmen, ob die Daten ausnahmsweise zum Schutz von Betroffeneninteressen aufzubewahren sind. Dabei muss bei Mitteilungsfällen auch die ausstehende Mitteilung einbezogen werden. Sind die Daten gleichwohl zu löschen, muss damit auch die Mitteilung entfallen, da sie künftige Prüfung nach Löschung nicht mehr möglich ist. Der Zustimmungsvorbehalt des Unabhängigen Kontrollrates nach Absatz 5 Nummer 1 gewährleistet dabei, dass die Abwägung nach § 38 Absatz 1 Satz 2 auch in Ansehung der offenen Betroffenenmitteilung zutreffend erfolgt.

Zu Nummer 2

Bei langfristigen Mitteilungshindernissen entfällt die Mitteilung künftig nach Ablauf von 5 Jahren. Die Regelung trifft im Interesse der Normpraktikabilität eine Fiktion, dass nach derart langer Zurückstellung und absehbar fortbestehenden Zurückstellungsgründen auch künftig keine Mitteilungsfähigkeit eintreten wird. Eine konkrete Prognose wie nach Absatz 2 Nummer 5, mit der dort noch geforderten hohen Gewissheit, ist also nicht mehr möglich, es reicht nach dem fünfjährigen Vorlauf vielmehr, dass für absehbare Zeit keine Mitteilung realistisch erwartbar ist. In die Interessenabwägung geht auch ein, dass typischerweise das berechtigte Betroffeneninteresse an der Mitteilung mit langem Zeitablauf sinkt.

Zu Absatz 5

Zu Nummer 1

Die Nummer führt die Fälle der Nicht-Mitteilung auf, deren Tatbestand zur Sicherung der grundsätzlichen Mitteilungspflicht des Absatzes 1 einer Überprüfung und Bestätigung durch den Unabhängigen Kontrollrat bedarf.

Zu Nummer 2

Die Regelung entspricht dem bisherigen § 12 Absatz 1 Satz 3 und 4 G 10.

Zu Absatz 6

Absatz 6 regelt die Dokumentation der Gründe von Ausnahmeentscheidungen.

Zu Unterabschnitt 4 (Weiterverarbeitung von Daten)

Die Grundnorm der Weiterverarbeitung (§ 36) wird in dem Unterabschnitt durch spezielle Regelungen zur qualifizierten Auswertung (§ 37), Datenpflege in Dateisystemen (§ 38)re Regelungen zu Akten (§ 39) und organisatorischen Vorkehrungen (§§ 40, 41) ergänzt. Zudem enthält das Gesetz für die Weiterverarbeitung besondere Vorschriften auch zur gemeinsamen Nutzung und Auswertung von Dateisystemen (§§ 42 bis 44; im Verfassungsschutzverbund in § 6 Absatz 2) und im Übrigen im Abschnitt 3 zur Übermittlung in §§ 42 ff.. § 69 behält zudem die Einwilligung als weitere Verarbeitungsgrundlage bei.

Zu § 36 (Weiterverarbeitung)

Zu Absatz 1

Satz 1 greift die allgemeine Verarbeitungsbefugnis des bisherigen § 8 Absatz 1 Satz 1 als Befugnis zur Weiterverarbeitung auf (der neue § 8 Absatz 1 Satz 1 enthält künftig nur noch die Befugnis zur Datenerhebung). Der Aufgabenbezug der Regelung bleibt umfassend beibehalten, bezieht also beispielsweise auch Fortbildungszwecke ein und ist dabei nicht methodenselektiv, erfasst also beispielsweise auch die aus den operativen Aufgaben herausgelöste Behördenforschung.

Satz 2 regelt die zweckändernde Weiterverarbeitung. Erhebungszweck ist jeweils nicht global die allgemeine Verfassungsschutzaufgabe, sondern die im Einzelfall wahrgenommene Aufgabe. Bei der Extremismusaufklärung ist dies die Aufklärung der Beobachtungsobjekte zu deren Aufklärung die Erhebung erfolgt (ggf. eine Mehrzahl verschiedener Beobachtungsobjekte in einer Szene). Bei der Spionageabwehr ist der Zweck auf die tätige fremde Macht bezogen. Eine weitere Ausdifferenzierung, etwa nach gegnerischen Operationen, würde verkennen, dass Erkenntnisziele immer auch darüber hinaus auf Strukturen und Methodiken des Angreifers, der fremden Macht, gerichtet sind.

Satz 5 trifft eine Regelung zum wirtschaftlichen Umgang mit verbundenen Daten, deren Trennung mit unverhältnismäßigem Aufwand verbunden wäre. Deshalb dürfen sie mitgespeichert werden. Der Eingriffsgehalt bleibt begrenzt, da hierzu keine Nutzungsbefugnis besteht, die Daten insbesondere nicht in Auswertungen nach Absatz 3 einbezogen werden dürfen. Die Regelung greift damit den bisherigen § 10 Absatz 2 auf.

Zu Nummer 1

Zu Buchstabe a

Die behördeninterne Zweckänderung für die Verfassungsschutzaufgaben ist umfassend zulässig (BVerfGE 162, 1 – Rn. 258, 270). Dies entspricht der grundsätzlichen Ausrichtung

des Prinzips der hypothetischen Datenneuerhebung auf einen Rechtsgütervergleich zwischen dem erhebungslegitimierenden und dem neuen Zweck (der von entsprechendem Gewicht sein muss und dies innerhalb der Verfassungsschutzaufgaben auch generell bleibt: BVerfGE 155,119 – Rn. 151). Besondere Erhebungsschwellen (wie erhebliche oder besonders erhebliche Beobachtungsbedürftigkeit) bleiben dagegen grundsätzlich irrelevant, vielmehr genügt, dass die Zweckänderung im Einzelfall (also hinreichend spezifisch) veranlasst ist, etwa indem die Informationen – ggf. in Verbindung mit weiteren Kenntnissen der Behörde - einen Spurenansatz auch für den geänderten Aufklärungszweck bieten (BVerfGE 141, 220 – Rn. 288 f.; 165, 363 – Rn. 62).

Die Aufgabenerfüllung bezieht auch Fortbildungs- oder Unterstützungstätigkeiten ein, d.h. auch dazu ist eine Zweckänderung erlaubt. Dies schließt auch technische Aufgaben wie die Entwicklung von Datenverarbeitungsprogrammen ein. Die Zweckänderungsbefugnis ermöglicht damit, auch bereits für andere Zwecke erhobene Daten für ein KI-Training weiterzuverarbeiten (die Weiterverarbeitung originär zum KI-Training beschaffter Daten hat ihre Grundlage bereits in Satz 1). Die Einzelfallveranlassung bezieht sich hier auf die Entwicklung jeweils eines bestimmten Programms, wobei parallele oder nachfolgende weitere Zweckänderungen offen bleiben, also ein Trainingsdatenpool beispielsweise auch für ein ablösendes Folgeprogramm fortgenutzt werden kann. Dabei erfolgt eine rein technische Nutzung ohne spezifisches Folgepotential für Betroffene. Speicherung und Zweckbindung sind in Absatz 2 Satz 1 Nummer 5 und Satz 3 geregelt.

Zu Buchstabe b

Die Regelung öffnet eine Zweckänderung für personalbezogene Innenzwecke des BfV.

Dies sind zum einen dienstrechtliche Anschlussmaßnahmen, auch soweit dazu Zuständigkeiten im Aufsichtsstrang oder zur verwaltungsgerichtlichen Prüfung bestehen (die allgemein nicht als – zweckändernde – Übermittlungen qualifiziert, mithin ebenso nicht in speziellen Übermittlungsregelungen abgebildet werden). Zwar drohen hierbei auch gewichtige aktionelle Anschlussmaßnahmen, die ihrerseits aber verfahrensimmanent an entsprechend gewichtige Pflichtverletzungen anknüpfen. Dieser Konnex muss also nicht bereits vorwirkend in der Zweckänderungsnorm hergestellt werden. Die Zweckänderungsschwelle des Verdachts strafbarer Handlungen korrespondiert der entsprechenden Übermittlungsregelung in § 47 Absatz 1 Nummer 4 Buchstabe b und soll ebenso innerbehördlich vermeiden, dass teils bereits vorsorgend durchgeführte Eingriffshandlungen in übermäßigem Umfang lediglich verdachtsgetragene Anschlussmaßnahmen auslösen. Die verdachtsschöpfende Wirkung der Vorsorgemaßnahme wird somit auf qualifizierte Handlungsbedarfe beschränkt. Dies ist neben strafbaren Handlungen auch bei jedweden funktionsgefährdenden Tätigkeiten oder sonstigen sicherheitserheblichen Erkenntnissen der Fall. Die Tätigkeit in einer Behörde mit besonderen Sicherheitsanforderungen ist mit einen entsprechenden Pflichtenstatus verbunden, der wiederum bedingt, entsprechend umfänglich dienstrechtliche Überprüfungen hinnehmen zu müssen.

Der Begriff der „sicherheitserheblichen Erkenntnis“ ist § 5 Absatz 2 SÜG entlehnt. Solche Erkenntnisse müssen nicht nur für dienstrechtliche Maßnahmen sondern ebenso für Zwecke der Sicherheitsüberprüfung genutzt werden können, sei es zur Sensibilisierung von Dienstvorgesetzten, sei es zur direkten Entziehung der Verschlusssachenermächtigung. Die Zweckänderungsregelung ist das innerbehördliche Pendant zur Übermittlungsbefugnis nach dem geltenden § 20 Absatz 1 Satz 1 Nummer 5 Buchstabe a BVerfSchG bzw. § 47 Absatz 1 Nummer 9 des Gesetzentwurfs. Die strafbaren Handlungen müssen als weitere Alternative neben den sicherheitserheblichen Erkenntnissen aufgenommen werden, weil der Begriff der sicherheitserheblichen Erkenntnis mit dem Bezug zur Sicherheitsüberprüfung der Sache nach auf aktive Beschäftige beschränkt ist, aber auch bei Ruhestandsbeamten ggf. strafbare Handlungen disziplinarisch zu würdigen sein können.

Zu Nummer 2

Eine Durchbrechung des Grundsatzes, dass Erhebungsschwellen für die Zweckänderung irrelevant sind, ergibt sich lediglich für die besonders eingriffsintensive Online-Überwachung und Wohnraumüberwachung (BVerfGE 141, 220 – Rn. 291; 165, 363 – Rn. 59). Dies ist bereits in den Zweckbindungsregelungen der betreffenden Erhebungsbefugnisse umgesetzt, die in Nummer 2 in Bezug genommen werden. Einbezogen ist auch die spezielle Zweckbindung aus Artikel 13 Absatz 5 Satz 2 GG, die in § 28 Absatz 2 aufgegriffen ist.

Zu Nummer 3

Die Nummer stellt klar, dass Übermittlungen speziell in Abschnitt 3 geregelt sind.

Zu Absatz 2

Der Absatz schließt an die bisherige Regelung in § 10 Absatz 1 an, differenziert die Betroffenengruppen bei einer personenbezogen strukturierten Speicherung aber stärker aus und enthält eine spezielle Regelung für Daten, die für eine Zuordnung noch zu prüfen sind.

Zu Nummer 1

Die Nummer bringt deutlicher als der bisherige § 10 Absatz 1 zum Ausdruck, dass der betroffene Personenkreis geregelt – und damit begrenzt – wird. Buchstabe a entspricht der bisherigen Nummer 1. § 3 Absatz 5 enthält die Legaldefinition der Beteiligten. Buchstaben b bis d differenzieren die bisherige Nummer 2 aus und sind dadurch inhaltlich klarer und bestimmter. Buchstabe d betrifft die Unterstützung der Aufklärungsaufgabe sowohl bei der Informationsbeschaffung als auch bei der Auswertung, umfasst also gleichermaßen Hilfspersonen des BfV wie auch sonstige für die Erforschung von Bedrohungen relevante Personen.

Die Speichervoraussetzung der tatsächlichen Anhaltspunkte betrifft im Ergebnis erst die strukturierte Speicherung zur Person (Personendatensätze oder -vorgänge), da Nummer 3 Buchstabe b) auch eine allgemeine Befugnis für die Erforschung von Bedrohungen beibehält, allerdings eben unter Ausschluss der personenbezogen strukturierten Speicherung, die damit den Voraussetzungen der Nummer 1 vorbehalten bleibt. Die strukturierte Speicherung zur Person dient der personenbezogenen Sammlung und Verknüpfung von Daten, die mit dieser Strukturierung auf eine personenbezogene Auswertung zielt, und danach nur spezifisch anlassbegrenzt (bei entsprechenden tatsächlichen Anhaltspunkten) erfolgen soll. Eine sonstige Speicherung in einem Dateisystem, dessen Struktur nicht bereits spezifisch auf die Auffindbarkeit der Daten zu einer bestimmten Person ausgerichtet ist, ist davon nicht erfasst.

Zu Nummer 2

Nummer 2 definiert eine neue Personengruppe, zu der die auswertbare Datenverarbeitung speziellen, verhältnismäßigkeitssichernden Regelungen unterliegen muss und die erstmals normenklar aufgenommen werden. Geregelt wird gewissermaßen der individuelle Prüffall, in dem noch kein Beteiligungsverdacht besteht, dem aber aus Anlass bestimmter Erkenntnisse nach fachlicher Bewertung nachgegangen werden muss.

Ein Beispiel sind Kontakte mit Beteiligten, die weder klar als Alltagskontakte (ohne Bezug zu der Bedrohung), noch als Beteiligungsanhaltspunkt zu bewerten sind. Hier ist einerseits mit dem niederschwelligen Aufklärungsauftrag des nachrichtendienstlichen Verfassungsschutzes geboten, zu erkennen, wenn sich stabile Kontaktmuster und Häufungen – etwa zu verschiedenen Bedrohungsbeteiligten – ergeben, was dann ggfs. als Anhaltspunkt eigener Verstrickung bewerten werden kann. Um solche Häufung zu erkennen, müssen die einzelnen Kontakte dazu aber erfasst und auf solche Muster ausgewertet werden.

Andererseits muss die Verarbeitung solcher lediglich zur Prüfung erfolgenden Informationssammlung auf den Prüfzweck begrenzt bleiben, solange sie keine eigene, in der Zusammenschau verdachtsbegründende Erkenntnis eröffnen. Diese Zweckbindung enthält Satz 2. Zudem enthält § 38 Absatz 3 Satz 2 eine spezifisch verkürzte Höchstspeicherdauer. Folgt aus der Prüfung unter Einbezug nachfolgend anfallender Informationen, dass tatsächliche Anhaltspunkte im Sinne der Nummer 1 bestehen, erfolgt die weitere Speicherung nach dieser Vorschrift, so dass für diese Daten damit die besonderen Regelungen für Prüffalldaten zur Zweckbindung nach Satz 2 und zur Speicherdauer in § 38 Absatz 3 Satz 2 nicht weiter anzuwenden sind.

Zu Nummer 3

Die Nummer flankiert und öffnet die Speicherung nach Nummer 1 für eine erweiterte, allerdings nicht personenbezogen strukturierte Speicherung.

Zu Buchstabe a

Die Eigensicherungsaufgabe ist spezifisch präventiv ausgerichtet und beispielsweise von der Bearbeitung situativer Risikosachverhalte (Liegenschaftszugang, § 64) geprägt. Dies bedingt einerseits spezielle Modifikationen der allgemeinen Verarbeitungsregelungen (vgl. § 67), andererseits auch eine von bestimmten Bedrohungen abgelöste Speicherung, die mit dem Buchstaben fundiert wird.

Zu Buchstabe b

Die Regelung entspricht dem bisherigen § 10 Absatz 1 Nummer 2, allerdings unter Ausschluss personenbezogen strukturierter Speicherung, die indes bei konkreter Veranlassung durch tatsächliche Anhaltspunkte nach Nummer 1 Buchstabe d eröffnet ist.

Zu Nummer 4

Die Regelung entspricht dem bisherigen § 10 Absatz 1 Nummer 3. Für Mitwirkungen nach § 2 Absatz 5 wird das BfV zum Verfassungsschutz einbezogen, d.h. auch hier erfolgt die Speicherung zum Schutz der Verfassungsschutzgüter.

Zu Nummer 5

Speziell Anwendungen Künstlicher Intelligenz werden unter Verarbeitung von Trainingsdaten entwickelt. Die trainierende Verarbeitung hat ihre Grundlage bereits in Absatz 1 (soweit dazu zu anderen Zwecken erhobene Daten einbezogen werden: zweckändernd nach Satz 2 Nummer 1 Buchstabe a). Absatz 2 Nummer 5 ermöglicht auch die weitere Speicherung für diesen Zweck, dies jedoch unter der besonderen Zweckbindung nach Satz 3. Diese Daten müssen auch zur Nachvollziehbarkeit für künftiges Qualitätsmanagement gesichert bleiben, was ebenfalls in Satz 3 berücksichtigt ist. Von der Zweckbindung werden nur die Daten erfasst, die ausschließlich zur Trainingsdokumentation gespeichert sind. Daten, die für die originäre Aufgabenwahrnehmung gespeichert sind, dürfen hierfür auch dann weiter genutzt werden, wenn sie auch zum Training einer KI herangezogen worden sind. Allerdings ist hier der zusätzliche Speicherzweck für die Erforderlichkeit der Weiterspeicherung beachtlich, die danach solange zulässig bleibt, wie das Dokumentationserfordernis fortbesteht, auch wenn die Daten für die originäre Aufgaben nicht mehr erforderlich sind. In diesem Fall tritt dann aber die Zweckbindung der Weiterverarbeitung auf diesen verbliebenen Speicherzweck ein, d.h. die weitere Verarbeitung erfolgt nicht im Personenbezug, sondern rein instrumentell auf den technischen Zweck begrenzt.

Eine Speicherung personenbezogener Daten ist nur nach Maßgabe der Erforderlichkeit zulässig, also wenn eine Realisierung auf Basis anonymisierter Daten nicht oder nicht mit wirtschaftlich vertretbarem Aufwand möglich ist. Allerdings wird oftmals schon keine Personenbeziehbarkeit anzunehmen sein, wenn bei den verwendeten Echtdaten zwar womöglich

theoretisch ein Personenbezug herstellbar wäre, dies aber jedenfalls mit unverhältnismäßigem Aufwand verbunden wäre.

Zu Absatz 3

Mit der Pseudonymisierung verliert die Speicherung wesentlich ihr Gefährdungspotenzial für Betroffeneninteressen, weshalb es insoweit einschränkender Regelungen durch Absatz 2 und 3 nicht bedarf. Der regulativ einzuschränkende Vorgang ist hier die Herstellung des Personenbezugs.

Zu § 37 (Qualifizierte Auswertung)

Zu Absatz 1

Die Regelung ergänzt die allgemeinen Befugnisse zur Datenweiterverarbeitung in § 36 um eine spezielle Regelung qualifizierter Auswertung, um dem besonderen Erkenntnispotenzial automatisierter Auswertung durch angemessene Voraussetzungen Rechnung zu tragen.

Der Vorgang, der die besondere Regelung erfordert, ist die Erlangung besonders grundrechtsrelevanten neuen Wissens, das durch die automatisierte Datenanalyse oder -auswertung geschaffen werden kann (BVerfGE 165, 363 – Rn. 50). Demgemäß ist Regelungsgegenstand der Abruf der Auswertung. Dies ist abzugrenzen von technischen Hintergrundprozessen, die vorhandene Daten in der Datenbank lediglich zur künftigen erleichterten Auswertbarkeit technisch aufbereiten. Es kann dahinstehen, ob solche technischen Prozesse überhaupt Eingriffsgehalt besitzen. Jedenfalls handelt es sich hierbei noch nicht um einen besonderen Intensiveingriff, der nicht mehr von der allgemeinen Verarbeitungsbefugnis in § 36 Absatz 1 gerechtfertigt wäre.

Der Begriff der automatisierten, d.h. maschinengestützten, Auswertung geht über einen einfachen Datenabgleich hinaus (wie einen Abruf mit Suchkriterien aus der Datenbank oder einen Trefferabgleich zwischen mehreren Dateisystemen) und erfasst komplexere Formen automatisierter Datenanalyse zur Gewinnung neuer Erkenntnisse. Satz 2 trifft dazu eine Eingrenzung des Anwendungsbereichs. Weitergehende Eingrenzungen – etwa nach Menge der verarbeitbaren Daten, den Dateiformaten oder der Komplexität der Analysemethodik – wären verfassungsrechtlich möglich, um die Voraussetzungen auf das zwingend gebotene einzuschränken (BVerfGE 165, 363 – Rn. 108, 120 ff., s.a. Rn. 78 ff. und 90 ff.). Aus Praktikabilitätserwägungen wird davon aber abgesehen, da es einerseits kaum möglich erscheint, solche Regelung hinreichend technikneutral und zugleich inhaltlich bestimmt zu treffen, andererseits aber auch kein dringender Bedarf besteht, die Schwelle des Absatzes 1 nicht auch auf Auswertungen begrenzter Komplexität oder Datenmenge anzuwenden.

Auswertungen, die nicht die Voraussetzungen von Satz 2 erfüllen, beispielsweise einfache Datenabgleiche, unterliegen den allgemeine Datenverarbeitungsvoraussetzungen nach § 36 Absatz 1. Im Übrigen erfasst die Regelung eine Weiterverarbeitung von bereits nach § 36 Absatz 2 gespeicherten Daten. Die Datenverarbeitung durch Filterprogramme, die bereits bei Datenerhebungen zur Anwendung kommen, ist an der Erhebungsbefugnis zu messen, sofern hierin ein eigenständiger Grundrechtseingriff zu sehen wäre (tatsächlich reduziert solche Filterung typischerweise den Eingriffsumfang). § 37 kommt allerdings auch im Zusammenhang einer Datenerhebung zur Anwendung, wenn die Erhebungsselektion mit einem Programm erfolgt, das dazu die bereits gespeicherten Daten automatisiert auswertet und die Selektion nicht als einfachen Datenabgleich, sondern mit der Generierung persönlichkeitsrelevanter Erkenntnis ausführt.

Absatz 1 Satz 1 gewährleistet grundsätzlich die zu komplexen Analysen vom Bundesverfassungsgericht (BVerfGE 165, 363) formulierten verfassungsrechtlichen Anforderungen. Das Gericht hat einerseits eine absolute Schranke, andererseits bestimmte Voraussetzungen für solche Analysen, abhängig von deren Eingriffsgewicht, bezeichnet.

Absolut unzulässig ist eine weder im Einzelfall durch einen konkreten Anlass getragene noch durch Vorgaben zur Verarbeitungsmethode inhaltlich eingeschränkte automatisierte Durchsuchung großer Bestände personenbezogener Daten auf bislang unbekannte Gesetzmäßigkeiten und gefahrenabwehrrechtlich bedeutende Zusammenhänge hin (a.a.O. Rn 95). Diese absolute Schranke greift Satz 1 durch die allgemeine Voraussetzung auf, dass die Auswertung im Einzelfall veranlasst ist.

Jenseits dieser absoluten Schranke unterliegt eine automatisierte Auswertung, die einen schwerwiegenden Eingriff in die informationelle Selbstbestimmung der Betroffenen ermöglicht, den Voraussetzungen, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten (Rn. 104). Für solche Auswertung durch die Polizei sieht das Gericht als Voraussetzung, dass sie zum Schutz besonders gewichtiger Rechtsgüter erfolgt (Rn. 105) und zudem die Eingriffsschwelle der hinreichend konkretisierten Gefahr vorliegt (Rn. 106).

Bei der Auswertung durch das BfV ist die Rechtsgutsanforderung bereits vom Aufgabenrahmen des § 2 Absatz 1 generell gewährleistet (BVerfGE 155,119 - Rn. 151; BVerfGE 163, 43 - Rn. 150). Die konkretisierte Gefahr ist dagegen die polizeispezifische Einsatzschwelle für intensivere Gefahrerforschungseingriffe. Die verfassungsgemäße Entsprechung bei der nachrichtendienstlichen Aufklärung ist die Anforderung, dass eine Überwachungsmaßnahme zur Aufklärung bestimmter Bedrohungen im Einzelfall geboten sein muss (BVerfGE 162, 1 - Rn. 153 ff., Rn. 164). Diese Schwelle wird in Satz 1 allgemein übernommen. Zusätzliche, qualifizierte Anforderungen an die Beobachtungsbedürftigkeit treten in Absatz 2 für gegenstands- oder folgenbezogen besonders eingriffsintensive Auswertungsprodukte hinzu.

Das Kriterium der Einzelfallerforderlichkeit bedingt, dass die Auswertung nicht ins Blaue erfolgt, sondern hinreichend spezifisch veranlasst ist. Eine Abgrenzung nach Datenumfang oder zu regelhaften Vorgängen ist damit nicht intendiert und nicht getroffen, vielmehr sind etwa regelhafte Vorgänge ebenso einbezogen, wenn die Regel an einen Anlass anknüpft. Soweit nicht ohnehin bereits als technischer Hintergrundprozess implementiert, wäre also beispielsweise ein manueller Abruf bestimmter Analyseprozesse generell bei allen neu eingehenden Informationen durch den Neueingang hinreichend spezifisch veranlasst. Weiteres Beispiel sind auch Prüffalldaten nach § 36 Absatz 2 Satz 1 Nummer 2, bei denen unter Umständen generell ein laufender Netzwerkabgleich durchzuführen ist, mit dem Muster im Kontakt mit Verdachtspersonen zu überprüfen sind. Diese Abgleichsroutine ist jeweils durch den konkreten Sachverhalt veranlasst, der Anlass zur Qualifikation als Prüffall gegeben hat. Hier wäre also beispielsweise möglich, aus dem Programm heraus bei definierten Verdichtungskriterien als Indikatoren eines Beteiligungsverdachts automatisiert die Neuqualifikation der Daten als solche nach § 36 Absatz 2 Satz 1 Nummer 1 vorzunehmen, u.a. mit der automatisierten Folge, dass die besondere Zweckbindung nach § 36 Absatz 2 Satz 2 und die verkürzten Regelhöchstspeicherdauer nach § 38 Absatz 3 Satz 2 wegfallen.

Neben der allgemeinen Schwelle für die Erkenntnismethode der automatisierten Auswertung bleiben besondere Zweckbindungen einzelner Daten zu beachten. Dies gilt speziell für die Weiterverarbeitung der durch Online- oder Wohnraum-Überwachung gewonnenen Informationen (§ 25 Absatz 7 und § 27 Absatz 4; dazu auch BVerfGE 165, 363 - Rn. 59). Solche Daten dürfen nach § 36 Absatz 1 Satz 3 Nummer 2 nur in Auswertungen einbezogen werden, die solchen Zwecken dienen, für die diese Daten weiterverarbeitet werden dürfen (so auch a.a.O. Rn. 118). Absatz 1 enthält eine Befugnis, bei der Auswertung gespeicherter Daten auch große Datenmengen mit variablen Dateiformaten einzubeziehen und komplexe Analysemethoden anzuwenden. Für besonders eingriffsintensive Auswertungsprodukte und -methoden enthält Absatz 2 allerdings ergänzende Voraussetzungen mit angehobenen Schwellen. Auch dies folgt der vom Bundesverfassungsgericht vorgenommenen Voraussetzungs-Synchronisierung komplexer Erkenntnisschöpfung mit heimlicher Informationsgewinnung (Rn. 104), die ebenso abgestuften Schwellenanforderungen korrespondierend

zum Informationsgegenstand (beispielsweise Höchstprivates) oder zur Persönlichkeitsrelevanz der Informationssammlung (beispielsweise Bewegungsprofil) hat.

Zu Absatz 2

Die Eingriffsintensität einer Datenauswertung folgt aus der Erlangung besonders grundrechtsrelevanten neuen Wissens (BVerfGE 165, 363 - Rn. 50), spezifisch indem persönlichkeitsrelevante Informationen erschlossen werden, etwa mit einem Bewegungs- oder Verhaltensprofil oder sogar einem umfassenden Persönlichkeitsbild (Rn. 77), insbesondere wenn darin eine automatisierte Bewertung eingeht (also nicht lediglich Treffer der Suchkriterien im Datenbestand angezeigt werden), speziell bei Gefährlichkeitsaussagen (Rn. 98). Weitere eingriffsintensive Variante ist eine verdachtsschöpfende Auswertung, mit der zu bislang unverdächtigen Personen tatsächliche Anhaltspunkte für eine Verstrickung in Bedrohungen gewonnen wird, so dass hieran anknüpfend auch eine Informationssammlung zu diesen Personen, u.U. auch spezielle personengerichtete Datenerhebung anschließt (Rn. 77).

Solchen Qualifikationskriterien folgend enthält Absatz 2 besondere Beschränkungen für besonders grundrechtsrelevante Erkenntnisprodukte und -methoden und regelt dabei solche Fälle, die in der Praxis möglicherweise erwartbar sind. Er wird mit Absatz 3 um eine Absicherung für nicht absehbare Sonderfälle ergänzt.

Da die Qualifikation aus der Erlangung qualifiziert eingreifender Erkenntnis folgt, ist solche Erkenntnis Voraussetzung der erhöhten Anforderung. Diese greifen folglich erst für die Weiterverarbeitung des Erkenntnisprodukts. Wenn besipielsweise eine Anwendung zur Erstellung eines Bewegungsprofils aus den vorhandenen Daten eingesetzt wird, ergibt sich erst aus dem Auswertungspodukt, welcher Zeitraum mit welcher Genauigkeit abgebildet ist. Der Abruf meint also die Verfügbarkeit der Erkenntnis zur Weiterverarbeitung. Die Initiierung durch den Bearbeiter muss einzelfallveranlasst sein und die weitere Verfügbarkeit richtet sich dann nach der generierten Erkenntnis.

Zu Nummer 1

Die Nummer regelt Auswertungen, die angesichts ihres erhöhten Eingriffsgewichts auf Bedrohungen von wenigstens erheblicher Beobachtungsbedürftigkeit beschränkt bleiben.

Zu Buchstabe a

Die originäre Verdachtsschöpfung hat besonderes Folgenpotenzial für Personen, die hierdurch überhaupt erst ins nachrichtendienstliche Blickfeld gelangen. Sie generiert mithin Streubreite, da eben keine harten Tatsachenerkenntnisse, sondern lediglich indizielle Aussagen getroffen werden. Der Eröffnung solcher Folgenpotenzialität korrespondiert erhöhter Rechtfertigungsbedarf, weshalb eine Beschränkung auf wenigstens erheblich beobachtungsbedürftige Bestrebungen erfolgt.

Von der Regelung nicht erfasst ist die Auswertung von Prüffällen nach Absatz 2 Satz 1 Nummer 2, da diesem Sachverhalt zugrunde liegt, dass die individuelle Prüfung zur Person spezifisch durch tatsächliche Anhaltspunkte veranlasst ist. Hier werden also nicht Personen verdachtsbelastet, die zuvor nicht im Blick waren, vielmehr ist bereits Klärungsbedarf zur Person erkannt und es erfolgt lediglich die danach nötige Klärung.

Zu Buchstabe b

Gegenstand der Regelung ist eine „Gefährdereinstufung“ der Person, die umfassend angelegt ist. Dies betrifft also nicht die analytische Erschließung einzelner Aspekte, die bedrohungsrelevant sind (wie etwa Zugang zu Tatgelegenheiten oder Tatmitteln) oder Teilaspekte der Persönlichkeit (wie etwa Gewaltorientierung), sondern das Gesamtbild der Persönlichkeit unter dem Blickwinkel der persönlichen Gefährdungsdisposition. Eine solche

Einstufung zur Gefährlichkeit einer Person hat einerseits die methodische Unsicherheit einer prognostischen Verhaltensbeurteilung, andererseits hat sie Qualität eines Persönlichkeits-Labelings, das auch dazu dient, Aufklärungsressourcen rational zu steuern, ist insoweit also allgemein auf informationelle Anschlussmaßnahmen gerichtet. Die nicht auf einzelne Maßnahmen, sondern auf die Person als solche bezogene Verknüpfung von Erkenntnissen inhärenter Unsicherheit mit Anschlusspotenzial ist qualifiziert rechtfertigungsbedürftig, weshalb dies nur zur Aufklärung wenigstens erheblich beobachtungsbedürftiger Bedrohungen zugelassen wird.

Zu Buchstabe c

Auch sonstige prognostische Einschätzungen zur Person sind weiche Erkenntnisse. Sie werden allerdings für sich bereits von den Basisanforderungen nach Absatz 1 getragen, die bereits auf Intensiveingriffe ausgerichtet sind (s.o.). Wird das weiche Erkenntnisprodukt allerdings mit einer Methodik der Erkenntnisgewinnung verknüpft, die von der autonom-anpassungsfähigen Entwicklungsfähigkeit maschinellen Lernens charakterisiert wird, kumuliert dies zu einer Kritikalität, die erhöhter Rechtfertigung durch qualifizierte Beobachtungsbedürftigkeit bedarf. Die EU-Verordnung über künstliche Intelligenz (2024/1689) gilt nach deren Artikel 2 Absatz 3 zwar nicht im Anwendungsbereich des Bundesverfassungsschutzgesetzes (so auch bereits primärrechtlich nach Artikel 4 Absatz 2 satz 3 EUV, vgl. BVerfG, Beschluss vom 8. Oktober 2024 - 1 BvR 1743/16 / 1 BvR 2539/16 [BND – Cybergefahren] Rn. 77, 79) und passt darauf bereichsspezifisch auch nicht. Der Grundüberlegung einer spezifischen Risikoeinschätzung zum Kernbestand von KI-Systemen (Artikel 3 Nummer 1) kann aber auch hier gefolgt werden.

Dies gilt demgemäß auch für autonom-anpassungsfähige Programme, die Entscheidungen über behördliche Folgeakte kriteriengestützt generieren oder jedenfalls empfehlend präjudizieren. Entscheidungen nach sachbezogenen Kriterien zu treffen, ist grundsätzlich kein Problem, sondern umgekehrt regelmäßig geboten. Automatisierte Entscheidungen bergen gleichwohl Risiken verkürzender Pauschalierung und kommen danach nur in begrenzten Anwendungsfeldern und bei überschaubaren Folgen in Betracht (im institutionellen Setting eines Nachrichtendienstes von vornherein allenfalls informationelle Akte, keine darüber hinaus gehende operativ-aktionelle Anschlussmaßnahmen). Auch insoweit sollen KI-generierte Entscheidungen auf Fälle wenigstens erheblicher Beobachtungsbedürftigkeit beschränkt bleiben.

Satz 2 begründet ergänzend eine spezielle Qualitätssicherungsaufgabe. Diskriminierende, also nicht sachlich begründete Auswertungsansätze sind per se ungeeignet, die erforderliche Erkenntnis zu gewinnen und danach gleichermaßen ohne weiteres unzulässig wie auch fachlich absurd. Bei maschinellem Lernen können aber durch nicht vorhersehbare oder steuerbare Effekte, etwa resultierend aus einer genutzten Datenbasis, Fehlentwicklungen auftreten. Solches Risiko muss unter Kontrolle bleiben. Deshalb begründet Satz 2 eine besondere Aufgabe, eingesetzte KI auf Fehlentwicklungen zu prüfen, um diese zu erkennen und zu bereinigen.

Zu Nummer 2

Beim Erkenntnisziel höchstprivater Informationen wird eine besonders schützenswerte Sphäre von Privatheit berührt. Wenn solche Informationen nicht nur im Einzelfall beschafft werden oder anfallen, sondern systematisch unter Auswertung vorhandener Informationen erschlossen werden sollen, hat dies nochmals besonders erheblichen Rechtfertigungsbedarf und wird deshalb auf die Aufklärung besonders erheblich beobachtungsbedürftiger Bedrohungen beschränkt.

Zu Nummer 3

Die Nummer synchronisiert die Voraussetzungen für Bewegungsprofile einerseits bei der Datenerhebung, andererseits bei der Auswertung, wenn bei letzterer das Erkenntnisprodukt

gleichwertig ist. Dies stellt insbesondere auch Anforderungen an die geodätische Genauigkeit verwendeter Standortinformationen, die beispielsweise bei einer Standortbestimmung nach dem Standort einer Mobilfunk-Basisstation angesichts der Größe der Funkzelle (in ländlicher Region unter Umständen im Radius mehrere Kilometer, auch innerstädtisch typischerweise ungeeignet zur Ermittlung von Adressen) nicht gleichwertig mit GPS-Standortdaten sind. Für den am Maßstab des § 21 bedeutsamen Zeitraum des durch Auswertung zu erstellenden Bewegungsprofils ist die in die Auswertung einbezogene Datenbasis maßgeblich, damit das Erkenntnisprodukt und nicht etwa auch sonstige womöglich im BfV noch vorhandene weitere Informationen.

Zu Absatz 3

Der Absatz trifft eine Auffangregelung für solche qualifizierte Auswertungen, die nicht als Anwendungen absehbar sind, sicher seltene Sonderfälle sind, aber womöglich dennoch vergleichbar gewichtig eingreifend sind wie die besonderen Auswertungen nach Absatz 2. Maßgeblich für die Gewichtung sind die Folgen der Auswertung (vgl. etwa Absatz 2 Satz 1 Nummer 1 Buchstabe a und b) und der gewonnenen Persönlichkeitserkenntnis (vgl. etwa Abdatz 2 Satz 1 Nummern 2 und 3). Bei der Persönlichkeitserkenntnis steht für die Gewichtung Privatheit jenseits der originären Aufklärungsrichtung im Vordergrund. Verhalten oder Beziehungen mit funktionalem Bezug zu den aufzuklärenden Bedrohungen stehen hierdurch in einem Sozialbezug, der unter Verhältnismäßigkeitserwägungen nicht dieselben strengen Anforderungen der Privatheitsausforschung bedingt und danach nicht die besonderen Schwellen des Absatz 2 und 3 erfordert. Wenn etwa Verhaltensmuster bei Bestrebungen oder Beziehungsgeflechte Beteiligter untersucht werden, erreichen die Erkenntnisprodukte generell nicht das Eingriffsgewicht, das Absatz 3 mit erhöhten Anforderungen voraussetzt.

Die Anforderungen nach Absatz 3 sind verfahrensmäßig besonders wirksam gesichert, indem die Prüfung und verbindliche Feststellung beim Unabhängigen Kontrollrat liegt und dieser nach § 41 Absatz 2 notwendig – grundsätzlich vorab – im Rahmen einer Errichtungsanordnung zu beteiligen ist.

Zu Absatz 4

Der Absatz trifft eine Eingrenzung zur personalen Zielrichtung entsprechend der Vorgabe zur Maßnahmerichtung bei nachrichtendienstlichen Mitteln in § 16 Absatz 5, wobei jedoch Nummer 2 auch dem Erkenntnisziel der Verdachtsschöpfung (vgl. Absatz 2 Satz 1 Nummer 1 Buchstabe a) Rechnung trägt.

Zu Absatz 5

Absatz 5 trifft besondere Datenschutzvorkehrungen. Einerseits wird die Kontrollierbarkeit besonders gewährleistet (Satz 1 und 2), dies grundsätzlich durch Abrufprotokollierung (Satz 1). Das BfV ist zu wirtschaftlicher und wirksamer Aufgabenwahrnehmung allerdings auch auf Standard-Software bzw. marktverfügbare Produkte angewiesen ist, die ggf. nicht selbst eine entsprechende Möglichkeit enthalten, etwa Benutzeraccounts zu verwenden, über die mit Zeitstempeln im Einzelnen nachvollziehbar ist, was ein Nutzer genau veranlasst hat. Deshalb sieht Satz 2 hilfsweise eine andere organisatorische Sicherung vor, die beispielsweise eine technisch vorgeschaltete Zugriffskontrolle oder aber auch eine Dokumentationspflicht sein kann.

Satz 3 gibt zyklische Strukturkontrollen des Unabhängigen Kontrollrates vor, damit sich bei diesem datenschutzsensiblen Sachverhalt keine Verwaltungspraxis im Verborgenen etabliert, ohne dass dies im Wechselspiel von Behörde und Datenschutzaufsicht angemessen gestaltet würde.

Zu Absatz 6

Absatz 6 regelt die automatisierte Veranlassung von operativen Anschlussmaßnahmen durch qualifizierte Auswertung. Er beschränkt dies auf den Anlasssachverhalt von Cyberangriffen und die dazu nötigen Abwehrmaßnahmen. Implizit eingeschlossen ist dabei zugleich die Beschränkung auf besondere Bedrohungen nach § 60 Absatz 3, da Interventionsakte bereits allgemein darauf beschränkt sind.

Cyberangriffe sind komplexe Technikvorgänge, die zum einen entsprechende Auswertungswerkzeuge erfordern und zum anderen hohe Reaktionsgeschwindigkeit bei der Anpassung auf Nachsteuerungen des Angreifers. In diesen Fällen sollten die informationstechnischen Gegenmaßnahmen zur wirksamen Abwehr also unmittelbar aus dem Analyseprogramm resultieren. Ein Zwischenschritt menschlicher Bearbeitung leistet hier keine relevante Qualitätssicherung, verzögert aber Abwehr erfolgsgefährdend.

Zu Absatz 7

Der Absatz trifft ergänzende spezielle Vorgaben in Bezug auf Anwendungen der sogenannten künstlichen Intelligenz.

Zu Nummer 1

Die Subsidiarität einer Beschaffung in Drittstaaten – sei es bei nichtöffentlichen oder öffentlichen Stellen – dient der digitalen Souveränität.

Zu Nummer 2

Nummer 2 gibt Qualitätsanforderungen vor. Die Kriterienauswahl orientiert sich an Artikel 15 Absatz 1 KI-VO (EU - 2024/1689). Die KI-VO selbst ist gemäß ihrem Artikel 2 Absatz 3 Unterabsatz 1 (in Übereinstimmung mit Artikel 4 Absatz 2 Satz 3 EUV) im Anwendungsbereich des Bundesverfassungsschutzgesetzes nicht anwendbar. Eine inhaltliche Angleichung mit der KI-VO ist mit der Benennung der abstrakten Qualitätskriterien zu Genauigkeit, Robustheit und Cybersicherheit nicht verbunden. Untergesetzliche Konkretisierungen und technische Standards sind dementgegen gerade je bereichsspezifisch angemessen zu treffen. Dies würde mit Konkretisierungen und Standards zur KI-VO grundsätzlich verfehlt, weil diese für ihren Anwendungsbereich, also gerade nicht zum Verfassungsschutz erfolgen.

Zu Nummer 3

Nummer 3 regelt einen Spezialfall der bereits nach Nummer 2 bestehenden Genauigkeitsanforderung. Diskriminierende, also sachwidrig – entgegen den fachlichen Anforderungen - differenzierende Algorithmen sind mit ihrem fachfremden Ansatz ungeeignet, die Erkenntnisziele zu erreichen, scheiden also sowohl fachlich wie rechtlich aus. Eine entsprechende Qualitätssicherung ist unmittelbar in der Fachlichkeit angelegt. Angesichts der Bedeutung der Fragestellung in der öffentlichen Diskussion wird gleichwohl eine spezielle Regelung aufgenommen.

Zu Nummer 4

Nummer 4 trifft eine organisatorische Vorgabe zur Qualitätssicherung eingesetzter Anwendungen.

Zu § 38 (Datenpflege in Dateisystemen)

Die Regelung entspricht dem bisherigen § 12. Bezugspunkt sind entsprechend moderner Datenschutzgesetzgebung (vgl. Artikel 4 Nummer 6 DSGVO) Dateisysteme. Bisher in § 11 Absatz 2 getroffene Regelungen zu Minderjährigen sind integriert.

Zu Absatz 1

Der Absatz greift den bisherigen § 12 Absatz 1 und 2 auf. Die neue Regelung in Satz 2 Nummer 1 entspricht der auch im Übrigen durchgängigen Berücksichtigung entgegenstehender übermäßiger Aufwände. Im Satz 3 ist die Verarbeitungsbeschränkung einerseits auch auf die Datennutzung erstreckt worden, andererseits ist neben der Einwilligung auch das objektive Betroffeneninteresse weiterverarbeitungsöffnend.

Zu Absatz 2

Der Absatz integriert mit Satz 2 Nummer 1 die Regelung des bisherigen § 11 Absatz 2 Satz 2, wobei die Prüfungspflicht nunmehr angesichts der neuen Ausnahmeöffnung zur Höchstspeicherdauer in Absatz 3 Satz 3 auch für die Fallgruppe des Absatz 3 Satz 1 Nummer 1 gilt.

Zu Absatz 3

Satz 1 Nummern 1 und 2 greifen den bisherigen § 11 Absatz 2 auf.

In Satz 1 Nummer 3 wird die Regelhöchstspeicherfrist bei der Aufklärung von Bestrebungen von bisher 10 Jahren (§ 12 Absatz 3) auf 15 Jahre angehoben. Typischer Aufklärungsgegenstand der Verfassungsschutzbehörden sind längerfristige Phänomene, nicht individuelle Einzelvorfälle. Diese Aufklärungsperspektive erfordert eine risikosensible Einschätzung zur künftigen Aufgabenerforderlichkeit, die endgültigen Informationsverlust trotz Ungewissheit künftiger Erforderlichkeit vermeidet. Dem geltenden Recht liegt die Annahme zugrunde, dass 10 Jahre ohne weiteren Informationsanfall indiziert, eine weitere Speicherung sei nicht mehr erforderlich (weshalb die weitere Speicherung dann durch erkannte Ausnahmegründe zu legitimieren ist). Dies wird rechtstatsächlich nicht bestätigt. In der Vergangenheit sind wiederholt auch länger zurückliegende Vorgänge bedeutsam geworden. So konnte bei Aufklärung des NSU-Komplexes eine Aufarbeitung lediglich anhand von Sachakten rekonstruiert werden. Gleiches gilt auch für die strafrechtlichen Ermittlungen des GBA in Bezug auf das Oktoberfestattentat von 1980, welche 2015 wiederaufgenommen worden waren. Im Falle des Reker-Attentäters lagen bei einer zivilgesellschaftlichen Organisation noch lange zurückliegende Informationen vor, die im Verfassungsschutzverbund schon zuvor zu löschen waren. Weitere Fälle (Mordfall Lübcke) zeigen, dass auch infolge sozialer Bindungen längerfristige Unauffälligkeit resultieren kann, ohne dass dies nachhaltig wirksam bleibt, speziell im Falle der Lockerung oder des Wegbrechens dieser Bindungen. Die bestehende Regelhöchstspeicherfrist von zehn Jahren wird daher dem aktuellen Erkenntnisstand der Risikoabschätzung angepasst.

Satz 2 enthält erstmalig eine verkürzte Höchstspeicherdauer für die „Prüffalldaten“ nach § 34 Absatz 3 Satz 1 Nummer 2.

In Satz 3 wird abweichend vom bisherigen § 12 Absatz 3 Satz 2 darauf verzichtet, auch die Vertretung der Abteilungsleitung aufzuführen, da damit keine zusätzliche funktionale Zuständigkeit, sondern lediglich Abwesenheitsvertretung gemeint ist, die bei Funktionszuständigkeiten generell eingeschlossen ist, also keiner besonderen Erwähnung bedarf. Die sensibleren Fälle des Satzes 1 Nummern 1 und 2 bleiben einer Ausnahmeentscheidung der Amtsleitung vorbehalten (ebenso mit Abwesenheitsvertretungsmöglichkeit).

Zu Absatz 4

Der Absatz enthält eine neue gesetzliche Klarstellung zur Anknüpfung für den Beginn des jeweiligen Fristlaufs.

Zu Absatz 5

Der Absatz stellt das Spezialitätsverhältnis des § 39 klar. Die Aktenführung dient auch der Dokumentation des Verwaltungshandelns und muss dazu anderen Regelungen folgen. Der Anwendungsausschluss bezieht sich auf die Datenverarbeitung in Akten und Aktenauszügen, in denen keine Löschungen erfolgen. Die Akte als Ganzes unterliegt jedoch nach § 39 Absatz 4 Satz 2 parallelen Prüf- und Vernichtungsregelungen, wenn es sich um eine Personenakte zu einem Beteiligten einer Bedrohung handelt.

Zu § 39 (Akten)

Die Regelung entspricht dem bisherigen § 13.

Zu Absatz 1

Die elektronische Akte (bisheriger Absatz 4) wird dem Paragraphen nicht mehr gewissermaßen als Sonderfall angefügt, sondern – da tatsächlich der Regelfall – bereits in die vorangestellte Regelung zum Anwendungsbereich (neuer Absatz 1) aufgenommen.

Absatz 2 synchronisiert die automatisierte Auswertung der elektronischen Akte mit der Auswertbarkeit strukturierter Dateisysteme. Ein Abgleich ist dabei nicht mehr beschränkt auf Akten eng umgrenzter Anwendungsgebiete (bisheriger § 13 Absatz 4 Satz 4), da dafür kein Sachgrund ersichtlich ist und sich der Klärungsbedarf bei der Suche vorhandener Informationen zu einer bestimmten Person nicht auf „eng umgrenzte Anwendungsbereiche“ – eine zudem kaum bestimmte Vorgabe – beschränkt. Die Protokollierungsvorgaben entsprechen dem bisherigen § 13 Absatz 4 Sätze 5 bis 7.

Zu Absatz 2

Der Absatz übernimmt den bisherigen § 13 Absatz 1

Zu Absatz 3

Der Absatz übernimmt den bisherigen § 13 Absatz 2.

Zu Absatz 4

Die Regelung entspricht dem bisherigen § 13 Absatz 3, bringt bei der Vorgabe zur Regelprüfung/-vernichtung in Satz 2 nunmehr aber klar zum Ausdruck, dass sich dies auf Personenakten Beteiligter bezieht, deren etikettierende Wirkung solche Vorgabe erfordert. Die Regelprüfung/-vernichtung betrifft wegen der Aktenvollständigkeit die Akte als Ganzes. Eine gesonderte Betrachtung von Teilen der Akte scheidet gemäß § 38 Absatz 5 aus.

Der im bisherigen § 13 Absatz 3 Satz 6 verwendete Begriff der „erheblichen“ Gefahr wird im neuen Satz 5 ersetzt durch den Bezug auf die übermittlungsrechtfertigenden Rechtsgüter, da die weitere Gefahrenabwehr die Übermittlung voraussetzt, die Grenzen der Übermittlungsbefugnis die effektive Nutzbarkeit der Informationen also ohnehin limitieren. Ergibt sich nachträglich, dass die Annahme, die Akte sei künftig nicht mehr erforderlich, falsch war, entfällt der Tatbestand des Satzes 1 und damit auch die ergänzende Zweckbeschränkung nach Satz 5.

Zu § 40 (Protokolldaten)

Der Paragraph trifft eine einheitliche Regelung zu Protokolldaten. Dies vermeidet sachlich unbegründete Differenzierung und erleichtert wirtschaftliche Durchführung. Dabei erfolgt zur wirksamen retrograden Klärung von Verstößen womöglich langjähriger Innentäter nunmehr eine Aufbewahrung auf 15 Jahre (bisher 5 Jahre in § 6 Absatz 3), die der Regelhöchstspeicherdauer in § 38 Absatz 3 Satz 1 Nummer 3 entspricht.

Zu § 41 (Errichtungsanordnungen)

Die Regelung greift den bisherigen § 14 auf, entwickelt ihn aber zeitgemäß fort. Dies betrifft einerseits die Erstreckung auf Anwendungen, die für automatisierte Auswertungen, eingesetzt werden, und andererseits eine nötigen Flexibilitätsöffnung in den Anforderungen an Festlegungen.

Der Dokumentations- und Ordnungsansatz bezieht sich zentral auf die Auswertbarkeit als der Funktionalität, in der sich der Persönlichkeitsrechtseingriff mit Relevanz für Anschlussmaßnahmen realisiert. Der Verwaltungsaufwand der Errichtungsanordnung wird dabei wirtschaftlich auf die spezifisch relevanten Fälle begrenzt, in denen Daten entweder verbundweit im nachrichtendienstlichen Informationssystem vorgehalten oder mit besonderem Erkenntnispotenzial – nach § 37 – automatisiert ausgewertet werden. Einbezogen werden dabei künftig auch die Programme, die solche komplexeren Auswertungen durchführen.

Die Struktur von Dateisystemen, ihre Nutzung wie auch Analysemethoden müssen dabei anforderungs- und zeitgemäß agil fortentwickelbar sein. Neue Bedarfe müssen kurzfristig umgesetzt werden, bestehen dabei aber womöglich nur zeitlich begrenzt oder auch projekthaft beschränkt auf enge, temporäre Anwendungen. Dem trägt die Option der Typenanordnung nach Satz 2 Rechnung, die kategoriale Festlegungen für zweckverwandte Auswertungen oder Datenbanktypen ermöglicht. Das pflichtgemäße Ermessen bei der Formenwahl muss dabei einerseits die Funktion der Errichtungsanordnung und andererseits Umfang und Dauer der Datenverarbeitung berücksichtigen. Für auf Dauer angelegte große Dateisysteme zu erheblich eingreifenden Auswertungen ist danach generell eine Einzelanordnung geboten.

Die Datenschutzkontrollzuständigkeiten sind an die neue Regelung in § 70 Absatz 2 angepasst. Danach ist künftig grundsätzlich der Unabhängige Kontrollrat anzuhören. Da die Anhörung in der Gelegenheit zur Äußerung besteht, wirkt sich die Zuständigkeitsänderung nur auf nach Inkrafttreten des Gesetzes neu eingeleitete Anhörungsverfahren aus. Bei zuvor eingeleiteten Verfahren, behält die bzw. der Bundesbeauftragte für Daten-schutz und Informationsfreiheit die Möglichkeit, das Verfahren mit einer Einlassung abzuschließen. Es muss nicht etwa neu in neuer Zuständigkeit begonnen werden.

Zu Unterabschnitt 5 (Gemeinsame automatisierte Auswertung)

Zu § 42 (Gemeinsame automatisierte Auswertung mit inländischen öffentlichen Stellen)

Zu Absatz 1

Die Regelung übernimmt nicht die bisherige Regelung des § 22a zu gemeinsamen Dateien, sondern regelt die Option einer gemeinsamen Weiterverarbeitung präziser. Schon die bisherige Regelung bezweckte keine Verantwortungsdiffundierung zu eingegebenen Daten, sondern den fortbestehenden Datenbesitz der eingebenden Stelle, die damit allein befugt blieb, ihren Datensatz zu ändern oder zu löschen. In der Sache geht es danach darum, dass die beteiligten Behörden nach demselben Datenmodell strukturierte Dateisysteme führen und sich dazu automatisierten Abrufzugriff einräumen. Die Bezeichnung als „gemeinsame Datei“ ist für einen solchen Abrufverbund logisch getrennter Dateisysteme, die die beteiligten Stellen jeweils in eigener Zuständigkeit und Verantwortung führen, eher fehlleitend.

Grundsätzlich sind automatisierte Abrufverfahren bereits nach den allgemeinen Vorschriften zur Durchführung von Ersuchens- und Übermittlungsregelungen möglich. Der Mehrwert des § 42 besteht in einer einheitlichen Befugnisgrundlage aller beteiligten Stellen durch Absatz 2. Dazu ist der Anwendungsbereich mit Absatz 1 auf einen Bereich informationeller Zusammenarbeit bezogen, bei dem ohne Ansehung der beteiligten Stellen eine einheitliche Übermittlungsregelung angemessen gestaltbar ist. Dies ist der Fall, wenn materielle

Verfassungsschutzaufgaben (Schutz besonders gewichtiger Rechtsgüter vor Bedrohungen) wahrgenommen werden und operative Anschlussmaßnahmen grundsätzlich ausgeschlossen sind (vgl. § 49 sogar zur Übermittlung nachrichtendienstlich ersterhobener Informationen).

Die in Absatz 1 geregelte Einrichtungsaufgabe umfasst die vorlaufende Koordination der beteiligten Stellen, mündend auch in die Vereinbarung nach Satz 2, sowie unter Umständen technische Services für die Durchführung der Auswertung, wie etwa die Bereitstellung der eigenen Auswertungsanwendung auch für die weiteren beteiligten Stellen. Übernimmt das BfV auch das Hosting der Dateisysteme auf einer von ihm betriebenen technischen Plattform, gilt dafür Absatz 3.

Zu Absatz 2

Satz 1 und 2 synchronisieren die Datenbereitstellung zur gemeinsamen Auswertung mit den jeweils für die innerbehördliche Auswertung getroffenen Regelungen. Im Zusammenwirken mit den Voraussetzungen nach Absatz 1 Satz 1 werden dadurch angemessene Weiterverarbeitungsgrundlagen für die gemeinsame Auswertung geregelt. Dies kann aber nicht für Daten gelten, die nach besonderen Übermittlungsverboten nicht bereitgestellt werden dürfen (Satz 3). Für das BfV betrifft dies insbesondere die Zweckbindungen nach § 25 Absatz 6 (Überwachung informationstechnischer Systeme) und § 27 Absatz 4 (Wohnraumüberwachung), sofern die gemeinsame Auswertung nicht den danach geltenden Anforderungen genügt.

Sätze 4 und 5 regeln – komplementär zum Aufgabenrahmen nach Absatz 1 – ein grundsätzliches Verbot operativer Anschlussmaßnahmen, für das nach Maßgabe von §§ 46 bis 48 Ausnahmen gelten. Beispielsweise kommt in Betracht, dass primärer Zweck der Auswertung die Erforschung und Bewertung von Bedrohungen ist (etwa auf Grund gemeinsam erstellter Lagebilder oder der Auswertung nach Vorgehensmustern von Aufklärungsobjekten), dabei aber Erkenntnisse gewonnen werden, die auch zur einschreitenden Gefahrenabwehr oder Strafverfolgung benötigt werden. Eine solche Sekundärnutzung wird dann nach Maßgabe der einschlägigen Übermittlungsvorschriften des Bundesverfassungsschutzgesetzes geöffnet. Da in solchem Fall sogar die operative Anschlussnutzung nachrichtendienstlich ersterhobener Daten eröffnet ist, kann die Angemessenheit solcher Regelung für einbezogene Daten anderen beteiligter Stellen erst recht angenommen werden.

Zu Absatz 3

Für die technische Gestaltung der gemeinsamen Auswertbarkeit sind unterschiedliche Varianten denkbar. Dass die verschiedenen Dateisysteme dazu physisch auf einem Server geführt werden, ist nicht notwendig, möglicherweise aber zweckmäßig. Übernimmt dies das BfV, ist es nach Absatz 3 auch zu den insoweit gebotenen Maßnahmen für die Sicherheit der Datenverarbeitung verpflichtet.

Zu § 43 (Gemeinsame Dateisysteme mit ausländischen Nachrichtendiensten)

Die Regelung entspricht dem bisherigen § 22b, übernimmt dabei jedoch das neue Schwellensystem der Beobachtungsbedürftigkeit (§ 3 Absätze 6 und 7). Der bisherige Absatz 1 Nummer 1 ist redaktionell bereits in die tatbestandliche Qualifikation des Gefährdungspotenzials integriert. Auf die privilegierte Einrichtung bloßer Indexdateien zur Informationsanbahnung wird mangels praktischen Bedarfs verzichtet. Zeitgemäße Zusammenarbeit ist auf gemeinsame Auswertung gerichtet und benötigt das dazu nötige IT-Werkzeug. Einbezogen werden können nach Absatz 1 Satz 4 künftig auch MAD und BND, was durch eine datenschutzfreundliche Auskunftsregelung (zur Auskunft auch über MAD-/BND-Speicherungen durch BfV) in Absatz 5 Satz 3 ergänzt wird.

Zu Absatz 4

Zu Nummer 2

Zu Buchstabe a

[…]

Zu Buchstabe b

[…]

Zu § 44 (Teilnahme an gemeinsamen Dateisystemen ausländischer Nachrichtendienste)

Die Regelung entspricht dem bisherigen § 22c.

Zu Abschnitt 3 (Übermittlung)

Die neue Gesetzessystematik folgt der Fachaufgabe und gliedert in die Aufklärung (Erstellung des nachrichtendienstlichen Produkts: Erkenntnisse über Bedrohungen) und die Umsetzung der gewonnenen Erkenntnisse entsprechend der Finalität der Aufklärungsaufgabe (BVerfGE 154, 152 - Rn. 217), die auf Folgemaßnahmen zielt. Bei dieser Umsetzung geht es vornehmlich wiederum um informationelle Befugnisse, nämlich die Lieferung von Erkenntnisprodukten an operative Bedarfsträger. Solche Übermittlungen werden in diesem Abschnitt geregelt. Dementgegen sind Übermittlungen an die Verfassungsschutzbehörden, die funktional der Bedrohungsaufklärung durch die Verfassungsschutzbehörden dienen, nunmehr bereits im Abschnitt 2 systematisch eingeordnet. Dieser neuen Systematik folgend werden im Auswertungsabschnitt (in einem eigenen Unterabschnitt 5) künftig auch die bisher in §§ 22a bis 22c getroffenen Regelungen über gemeinsame Dateien als Hilfsmittel der Aufklärung aufgenommen.

Während die Regelung zur Öffentlichkeitsinformation (§ 45) Anpassungen im Interesse verbesserter Normenklarheit enthält, greifen die weiteren Übermittlungsbefugnisse des BfV im Wesentlichen die bisherigen §§ 19 ff. auf, in denen bereits Anpassungen an die Verfassungsrechtsprechung (BVerfGE 163, 43) erfolgt waren. Hinzu kommen nunmehr Nachkorrekturen, die einerseits weitere Verfassungsrechtsprechung aufgreifen (§ 48), andererseits überschießende Auswirkungen vermeiden (§§ 50, 56).

Zu § 45 (Information von Öffentlichkeit und Fachkreisen)

Die Regelung entspricht dem bisherigen § 16.

Zu Absatz 1

Die Regelung zum jährlichen Verfassungsschutzbericht ist weiter als Pflichtaufgabe formuliert (Absatz 2), die sonstige anlass- oder auch lagebedingten Öffentlichkeitsinformation erfolgt dagegen jeweils situationsadäquat und ist danach nunmehr als Ermessensregelung formuliert (Absatz 1). Eine entsprechende ergänzende Öffentlichkeitsunterrichtung ist ebenso dem Bundesministerium des Innern (BMI) als Fachaufsichtsbehörde möglich, ohne dass dies besonderer Regelung bedarf.

Ausdrücklich geregelt ist nunmehr auch die Information der Fachöffentlichkeit, beispielsweise von Fachkreisen der politischen Bildung oder des Wirtschaftsschutzes. Solche Informationen etwa zur Lagebeurteilung – unter Einbezug aktueller wichtiger Ereignisse – erfolgen ggf. ebenso in periodischen Berichtsformaten, sind aber unter Umständen inhaltsabhängig wegen des begrenzten Empfängerkreises nicht notwendig zugleich öffentlich zugänglich, sondern womöglich auch als Verschlusssachen eingestuft. Ein solches Produkt

ist zum Beispiel der Wochenbericht des BfV mit einem Verteilerkreis, der sowohl behördliche Bedarfsträger wie auch das Parlamentarische Kontrollgremium umfasst. Die Erforderlichkeitsvoraussetzung bezieht sich auf die Unterrichtung des Fachkreises, also eine typisierende Betrachtung des Informationsbedarfs dieser Gruppe. Dazu eingerichtete Berichtsformate greifen den allgemeinen Informationsbedarf der Empfängergruppe auf und sind von einer individualisierenden Betrachtung einzelner Mitglieder dieser Gruppe abgelöst.

Ergänzend zum bisherigen speziellen Hinweis auf Wirtschaftsschutz ist wegen der besonderen Bedeutung auch des Wissenschaftssektors für geheimdienstliche Ausforschung durch fremde Mächte nunmehr ebenso der Wissenschaftsschutz, also die Beratung wissenschaftlicher Einrichtungen zur Sensibilisierung und wirksamen Eigensicherung, aufgenommen.

Die Öffentlichkeitsaufklärung insbesondere durch den Verfassungsschutzbericht soll die gesellschaftliche Auseinandersetzung mit den verfassungsschutzrelevanten Bedrohungen unterstützen. Dieser Zweckausrichtung folgend wird nunmehr in Absatz 1 Satz 2, der gleichermaßen für die Öffentlichkeitsunterrichtung des BMI gilt, ausdrücklich geregelt, dass über bloße Prüffälle nicht berichtet wird. Wenn nach vorliegenden Erkenntnissen noch nicht einmal der Verdacht nachrichtendienstlich aufklärungsbedürftiger Bestrebungen besteht, ist die Information über diesen Sachverhalt nicht geeignet, die Auseinandersetzung mit solchen Bestrebungen informationell zu unterstützen. Angesichts des beachtlichen Risikos einer stigmatisierenden Fehldeutung in der Öffentlichkeit muss das öffentliche Interesse an der Information auch über solche Prüftätigkeiten hinter den schutzwürdigen Interessen der betroffenen Person zurücktreten.

Die Berichtserstattung über Verdachtsfälle ist hingegen auch künftig zulässig. Sie ist verfassungsrechtlich möglich (bestätigt mit den Kammerbschlüssen des BVerfG vom 31.05.2022 1 - BvR 98/21 - und - 1 BvR 564/19 -) und bei entsprechender Bedeutung auch zur zivilgesellschaftlichen Auseinandersetzung mit der Erkenntnislage geboten. Nach Satz 2 ist allerdings in der Öffentlichkeitsberichterstattung auch weiterhin speziell darauf hinzuweisen, wenn lediglich ein Verdacht vorliegt. Die Mitteilung des Erkenntnisstandes gehört zur sachgerechten Öffentlichkeitsunterrichtung. Dies kann auch den Fall betreffen, dass das BfV nach seiner Erkenntnislage davon überzeugt ist, dass es sich um extremistische Bestrebungen handelt. War dem eine Berichterstattung zum bloßen Verdachtsfall vorausgegangen, kann zur sachgerechten Öffentlichkeitsunterrichtung sogar geboten sein, ausdrücklich transparent zu machen, wenn das BfV nunmehr die Bestrebungen als gesichert extremistisch betrachtet. Die Möglichkeit, den Erkenntnisstand nicht nur im Verdachtsfall, sondern auch bei Überzeugungsgewissheit transparent zu machen, stellt nunmehr Satz 4 ausdrücklich klar Solche Sachinformationen zum Erkenntnisstand des BfV, die gelegentlich als „Einstufung“ bezeichnet werden, sind rein informatorisch und haben keinen Regelungsgehalt.

Zu Absatz 2

Die Regelung entspricht dem bisherigen § 16 Absatz 2, weicht von dessen Satz 2 aber insoweit ab, als im Verfassungsschutzbericht des BMI die Mitteilung von Strukturdaten zum MAD entfällt. Die Öffentlichkeitsunterrichtung über seinen Geschäftsbereich obliegt dem Bundesministerium der Verteidigung.

Zu Absatz 3

Die Bekanntgabe personenbezogener Daten nach Absatz 4 ist komplementär zur neuen Regelung für fachöffentlichkeitsbestimmte Berichtsprodukte um eine spezielle Regelung hierzu ergänzt (Satz 2). Schranke bilden weiterhin überwiegende schutzwürdige Belange betroffener Personen, bei deren Gewichtung insbesondere Risiken nachteiliger Folgen in Betracht zu ziehen sind. Dabei sind wiederum die Folgerisiken einer Öffentlichkeitsunterrichtung oder einer bloßen Information von Fachkreisen gesondert zu betrachten,

insbesondere wenn Letzteres unter Verschlusssachenschutz erfolgt, also einer besonders engen Begrenzung der Weiterverwendung.

Zu Absatz 4

Die Regelung synchronisiert die Publikation von Produkten externer wissenschaftlicher Forschung mit der Behördenforschung des BfV, soweit das BfV der externen Einrichtung, beispielsweise einem universitären Forscherteam, für dessen Forschung Informationen zugänglich gemacht hat.

Zu § 46 (Übermittlung an inländische öffentliche Stellen zur Gefahrenabwehr)

Die Regelung übernimmt den bisherigen § 19 BVerfSchG, angesichts der Begriffsdefinitionen in § 3 Absatz 8 und 9 hier redaktionell verschlankt.

Zu § 47 (Übermittlung an inländische öffentliche Stellen zum administrativen Rechtsgüterschutz)

Die Regelung baut auf dem bisherigen § 20 auf, der in der Systematik leicht modifiziert wird (z.B. Außenwirtschaftsrecht nicht mehr Materie der Eignungs- oder Zuverlässigkeitsüberprüfung). Zudem wird der Inhalt konsolidiert (ordnungsbehördliche Interventionen auf dem Gebiet des Versammlungsrechts oder der passrechtlichen Ausreiseuntersagung nicht mehr auf Fälle der konkretisierten Gefahr beschränkt) und abgerundet (Gewerbeaufsicht statt lediglich sicherheitsgewerberechtliche Zuverlässigkeitsüberprüfung). Redaktionell wird die Reglung leicht verschlankt.

Übermittelt das BfV von sich aus, ist maßgeblich, ob die Übermittlung aus seiner Sicht erforderlich ist (vgl. § 477 StPO), was naturgemäß nur eine oberflächlich-kursorische Abschätzung der Erforderlichkeit, die fachkompetent erst von der zuständigen Empfängerbehörde vorgenommen werden kann (dazu siehe auch § 49), bedingt. Ist die Übermittlung von einem Ersuchen veranlasst, trägt die ersuchende Stelle grundsätzlich die Verantwortung für die Zulässigkeit der Übermittlung. Das BfV prüft nur, ob das Übermittlungsersuchen im Rahmen einer Aufgabe nach Nummern 1 bis 9 erfolgt und ob ein Übermittlungsverbot nach § 52 entgegensteht (vgl. § 15 Absatz 2 Satz 2 und 3 BDSG 1990).

Zu Absatz 1

Der Absatz führt Zwecke der Risikoprävention auf (BVerfGE 169, 130 - Rn. 113), die durch den Bezug auf Bedrohungen eine enge Verbindung zum Verfassungsschutz aufweisen. Die auf besonders gewichtige Rechtsgüter begrenzte Schutzrichtung und die Enumeration besonderer Risikomaterien in den Nummern des Absatzes beschränken Übermittlungen dabei auf Sachverhalte besonders hohen Gefahrenpotentials.

Die Übermittlung in den Weiterverarbeitungskontext ordnungsbehördlicher Anschlussmaßnahmen bewirkt zugleich, dass zu dieser Weiterverarbeitung – einschließlich der zugrunde liegenden Übermittlung selbst – das Normverständnis der gesetzlichen Weiterverarbeitungsregelungen in dem für die Eingriffsverwaltung typischen Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle weiter konkretisiert werden kann. Sonderanforderungen zur Spezifizierung des gesetzlichen Normprogramms, wie sie noch für heimliche Überwachungsmaßnahmen bestehen (vgl. BVerfGE 162, 1 – Rn. 200), setzen sich im Übergang in den institutionellen Modus offenen Verwaltungshandelns also nicht fort.

Zu Nummer 1

Die Nummer greift den bisherigen § 20 Absatz 1 Satz 1 Nummer 8 auf.

Zu Nummer 2

Die Nummer fasst die bisherigen Nummern 3 und 4 aus § 20 Absatz 1 Satz 1 zusammen. Die gesonderte Erwähnung der Vorbereitung wird nicht übernommen, weil dies ohne weiteres vom benannten Zweck eingeschlossen ist.

Zu Nummer 3

Zu Buchstabe a

Der Buchstabe war bisher als Zuverlässigkeitsüberprüfung in § 20 Absatz 1 Satz 1 Nummer Buchstabe a enthalten.

Zu Buchstabe b

Die Regelung entspricht dem bisherigen § 20 Absatz 1 Satz 1 Nummer 2.

Zu Buchstabe c

Die Ordnungsmaterie ist neu aufgenommen. Im bisherigen Recht waren die Übermittlungen als Fall der Abwehr konkretisierter Gefahren verstanden worden, da die versammlungsrechtlichen Interventionsbefugnisse eine konkretisierte Gefahr – für die öffentliche Sicherheit oder Ordnung – voraussetzen. Das im Einzelfall bedrohte Rechtsgut bestimmt sich dabei auch nach der Zielrichtung des Störungshandelns. Ist das Handeln gegen die freiheitliche demokratische Grundordnung gerichtet, besteht die Gefahr auch für diese Schutzgut. Die erwartbare extremistisch motivierte Sachbeschädigung während des Aufzugs ist eine konkretisierte Gefahr nicht nur für das Eigentum, sondern auch für die freiheitliche demokratische Grundordnung (BT-Drs. 20/9345, Seite 23). Dies ist zur Klarstellung nunmehr bereits allgemein in der Begriffsdefinition durch § 3 Absatz 9 übernommen. Dennoch erscheint übersichtlicher, zusätzlich das Versammlungsrecht in der Übermittlungsvorschrift zur ordnungsbehördlichen Intervention aufzunehmen. Diese Klarstellung besonders praxisbedeutsamer Anwendungsfälle in § 47 verkürzt nicht die Übermittlungsbefugnis nach § 46 in Fällen konkretisierter Gefahr auch an Ordnungsbehörden, unabhängig davon, ob dies auch in § 47 vorgesehen ist (oder in außergewöhnlicheren Fallkonstellationen eben auch nicht).

Zu Nummer 4

Die Regelung bezweckt den Schutz der Funktionsfähigkeit des öffentlichen Dienstes in der wehrhaften Demokratie und dem Vertrauen der Bevölkerung in die rechtsstaatliche Verwaltung.

Zu Buchstabe a

Der Buchstabe entspricht dem bisherigen § 20 Absatz 1 Satz 1 Nummer 1 mit zwei Ergänzungen.

Zum einen wird ergänzend zum öffentlichen Dienst auch auf die Beschäftigung bei Stellen mit Aufgaben der öffentlichen Verwaltung aufgenommen. Auch in Privatrechtsform organisierte Bereiche öffentlicher Verwaltung sind damit einbezogen.

Außerdem werden, wie bereits in § 32 Absatz 1 Satz 1 MADG, Reservisten nach § 1 Reservistengesetz speziell aufgeführt. Zwar werden Reservisten vor Heranziehung zu einer Dienstleistung nach § 60 Soldatengesetz (SG) sicherheitsüberprüft. Bei dienstlichen Veranstaltungen nach § 81 SG, also solche zur militärischen Aus-, Fort- und Weiterbildung (auch zur Schulung und Übung an Waffen), ist dies jedoch nicht der Fall. Deshalb muss der gebotene Informationsfluss unabhängig von der Durchführung einer Sicherheitsüberprüfung eröffnet sein, damit die personalführende Stelle der Bundeswehr von solchen

Informationen veranlasste Maßnahmen ergreifen, insbesondere den Reservisten dauerhaft zurückstellen kann.

Zu Buchstabe b

Das Vertrauen der Bevölkerung in die Sauberkeit der öffentlichen Verwaltung ist wesentliches Element des Vertrauens in die Funktionsgerechtheit der verfassungsmäßigen Ordnung. Wenn Dienstpflichten sogar durch die Begehung von Straftaten verletzt werden, stellt dies die Zuverlässigkeit des Beschäftigten über den Einzelfall hinaus in Frage und schädigt das Ansehen der öffentlichen Verwaltung nachhaltig, wenn dem nicht intervenierend begegnet wird. Deshalb müssen solche Erkenntnisse einer dienstrechtlichen Würdigung zugeführt werden können, unabhängig davon, ob der Sachverhalt auch die Übermittlungsschwelle zur Strafverfolgung nach § 48 erreicht wird. Dabei ist zwar in Rechnung zu stellen, dass durch dienstrechtliche Anschlussmaßnahmen schwere Folgen eintreten können. Diese sind jedoch ihrerseits von der Schwere der Dienstpflichtverletzung abhängig, so dass die nähere Folgenbetrachtung zur Verhältnismäßigkeitssicherung noch nicht in die Übermittlungsvoraussetzungen vorwirken muss. Zur Vermeidung einer übermäßigen Streubreite werden Übermittlungen allerdings auf den Verdacht strafbarer Handlungen beschränkt.

Zu Nummer 5

Die Regelung greift die bisherige Aufführung des Aufenthaltsrechts in § 20 Absatz 1 Satz 1 Nummer 5 Buchstabe b auf. Ergänzt wird dies um die Ausreiseuntersagung (z.B. § 10 PassG). Dies ist bislang als Fall der Übermittlung wegen konkretisierter Gefahr behandelt worden (vgl. Begründung zu Nummer 3 Buchstabe c), wird aber der Übersichtlichkeit halber nunmehr hier mit aufgeführt. Auch hier sind mit der benannten Finalität die diesem Ziel dienen Maßnahmen (wie die Passentziehung, § 8 PassG) einbezogen. Eine komplementäre Regelung zur Einreise ist als aufenthaltsrechtliche Maßnahme in der Benennung diesr Materie bereits eingeschlossen.

Zu Nummer 6

Die Regelung übernimmt den bisherigen § 20 Absatz 1 Satz 1 Nummer 9.

Zu Nummer 7

Die Regelung war bisher im Zusammenhang mit Zuverlässigkeitsüberprüfungen enthalten (§ 20 Absatz 1 Satz 1 Nummer 5 Buchstabe a).

Zu Nummer 8

Die Regelung greift die bisher enthaltene sicherheitsgewerberechtliche Zuverlässigkeitsüberprüfung auf (§ 20 Absatz 1 Satz 1 Nummer 5 Buchstabe a) und erweitert den Tatbestand insgesamt auf die Materie des Gewerberechts. Dies umfasst die wirtschaftsverwaltende Aufsicht über Gewerbeausübung in jedwedem Sektor. Enthalten ist damit beispielsweise auch die Übermittlung an die nach dem Gaststättengesetz zuständige Behörde, wenn diese die Information zur Prüfung von Auflagen benötigt, beispielsweise einem vorübergehenden Verbot des Ausschanks alkoholischer Getränke im Zusammenhang mit extremistischen Veranstaltungen.

Zu Nummer 9

Ergänzend zu Nummer 8 wird der Finanzsektor – allgemeiner Gesetzessystematik folgend – im Interesse von Normenklarheit gesondert in Nummer 9 aufgeführt. Dies schließt die bisherige Regelung des § 20 Absatz 1 Satz Nummer 7 ein. Die Regelung beschränkt sichnicht auf Maßnahmen nach § 6a KWG, sondern befugt auch im Übrigen zu Übermittlungen für Aufgaben der sektoralen Aufsicht, soweit dies besonders gewichtigen Rechtsgütern – speziell dem Verfassungsschutz – dienlich ist.

Zu Nummer 10

Die Nummer entspricht dem bisherigen § 20 Absatz1 Satz 1 Nummer 5.

Zu Nummer 11

Die Übermittlungsbefugnis betrifft den Sachverhalt, dass sich extremistische Beobachtungsobjekte oder fremde Mächte Mittel verschaffen wollen, um ihre Bestrebungen oder Tätigkeiten zu betreiben, und eine öffentliche Stelle Einwirkungsmöglichkeiten besitzt, dies zu verhindern. Fälle sind beispielsweise kommunale Veranstaltungsräume, die für eine extremistische Versammlung genutzt werden sollen, ohne dass dieser Sachverhalt der Kommune ohne weiteres erkennbar ist, etwa weil eine Person als Veranstalter auftritt, der von der Kommune nicht zuordenbar ist, und eine auf den ersten Blick unverfängliche thematische Ausrichtung benannt wird. Ein vergleichbarer Sachverhalt ist die Beantragung einer Sondernutzungsgenehmigung z.B. für einen Stand in einer Fußgängerzone. Ein anderes Beispiel wäre der Versuch, eine Immobilie zu erwerben, um darin etwa eine Schulungsstätte für extremistische Bestrebungen oder eine Versammlungsstätte zur Stärkung des organisatorischen Zusammenhalts einzurichten. Hier kann u.U. in Betracht kommen, dies mit Ausübung eines Vorkaufsrechts nach § 24 BauGB zu verhindern.

Das Bundesverfassungsgericht hat in seinem Beschluss zum Hessisches Verfassungsschutzgesetz (BVerfGE 169, 130) seine Rechtsprechung bereits dahingehend fortentwickelt, dass die von ihm formulierten Schwellenvoraussetzungen auch bei personen- oder gruppenbezogener Risikoprävention erfüllt sein können (Rn. 113). Damit ist als Schwelle die Risikoprävention bezeichnet. Für die Güterabwägung der Verhältnismäßigkeit ist dabei unerheblich, ob das Risiko durch besondere Tatgelegenheiten (wie etwa eine sicherheitsempfindliche Tätigkeit) oder die Verfügbarkeit besonderer Tatmittel begründet wird und ob dazu ein besonderes fachrechtliches Überprüfungsverfahren vorgesehen ist (wie im Waffengesetz) oder die Überprüfung im Rahmen der allgemeinen Amtsermittlung des Entscheidungssachverhalt durch die zuständige Behörde erfolgt (wie bei einem Nutzungsvertrag zu einer kommunalen Veranstaltungsstätte). Die Vorenthaltung von Tatmitteln für Bedrohungen dient unmittelbar den Rechtsgütern des Verfassungsschutzes. Die Verfassungsentscheidung für die im Verfassungsschutz institutionalisierte Frühaufklärung extremistischer Gefährdungen unterstreicht deren Gewicht und die Übermittlungsbefugnis setzt darüber hinaus noch das besondere Gefährdungspotenzial wenigstens erheblicher Beobachtungsbedürftigkeit voraus. Zudem ist erst die Eignung zur erheblichen, also gewichtigen Förderung der Bedrohung übermittlungsrechtfertigend.

Zu Nummer 12

Die Nummer regelt ebenso, Bedrohungen massiv förderliche Mittel zu entziehen, nämlich Finanzmittel, die hier durch Steuerhinterziehung verfügbar werden und deren Verfügbarkeit folglich durch Information der Finanzverwaltung künftig entzogen werden kann.

Zu Absatz 2

Der Absatz entspricht dem bisherigen § 20 Absatz 2.

Zu Absatz 3

Der Absatz übernimmt den bisherigen § 20 Absatz 1 Satz 2, der allerdings auch auf gesetzlich besonders geregelte Anfrageverfahren im Rahmen der Leistungsverwaltung, also auch au Absatz 2 erstreckt und deshalb als Absatz 3 gefasst wird.

Zu § 48 (Übermittlung an Strafverfolgungsbehörden zur Strafverfolgung)

Die verfassungsrechtlichen Anforderungen an die Regelung von Übermittlungen zur Strafverfolgung richten sich nach dem Kriterium der hypothetischen Datenneuerhebung. Dabei

kommt eine Übermittlung von Daten, die eine Verfassungsschutzbehörde ersterhoben hat, nur zum Schutz eines herausragenden öffentlichen Interesses und daher nur zur Verfolgung besonders schwerer Straftaten in Betracht, wobei als Schwelle für die Übermittlung konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht vorliegen müssen (BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, BVerfGE 169, 130-235, Rn. 199).

Eine Übermittlung nachrichtendienstlich ersterhobener personenbezogener Daten darf generell nur zum Schutz eines herausragenden öffentlichen Interesses erfolgen (BVerfGE 162, 1 <118 Rn. 250>; vgl. auch BVerfGE 133, 277 <329 Rn. 123>; 154, 152 <268 Rn. 219>; 156, 11 <52 Rn. 105>). Für Maßnahmen, die der Strafverfolgung dienen und damit repressiven Charakter haben, kommt es auf das Gewicht der Straftaten an (vgl. Rn. 110), die der Gesetzgeber in - jeweils näher bestimmte - erhebliche, schwere und besonders schwere Straftaten eingeteilt hat (vgl. BVerfGE 141, 220 <270 Rn. 107> mit Bezugnahme auf BVerfGE 109, 279 <343 ff.>; vgl. auch BVerfGE 162, 1 <118 Rn. 251>). Maßgeblich für die Schwere des tatbestandlichen Unrechts sind der Rang des verletzten Rechtsguts und andere tatbestandlich umschriebene, gegebenenfalls auch in einem Qualifikationstatbestand enthaltene Begehungsmerkmale bzw. weitere Tatfolgen. Sie allein müssen bereits die besondere, deutlich über dem Durchschnitt liegende Schwere des jeweiligen Straftatbestandes begründen (BVerfGE 109, 279 <344>). Dabei gibt der Strafrahmen einer Deliktsnorm einen maßgebenden Anhaltspunkt dafür, ob es sich abstrakt um eine besonders schwere Straftat handelt (vgl. BVerfGE 109, 279 <347>; 125, 260 <329>). Bei der Bestimmung des Unrechtsgehalts und des Strafrahmens eines Delikts verfügt der Gesetzgeber über einen Beurteilungsspielraum (vgl. BVerfGE 109, 279 <347>; 129, 208 <243>; BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, BVerfGE 169, 130-235, Rn. 202).

Zu Absatz 1

Die Regelung entspricht dem bisherigen § 21 Absatz 1. Ersucht eine Strafverfolgungsbehörde das BfV um Übermittlung von Daten, liegt die Verantwortung für die Zulässigkeit des Ersuchens bei ihr. Das BfV prüft allerdings, ob von ihm anzuwendende besondere Übermittlungsregelungen entgegenstehen. Dies sind hier die Schranken der speziellen Übermittlungsbefugnis des § 48. Das BfV muss danach prüfen, ob die Strafverfolgung wegen eines Delikts nach Absatz 2 erfolgt. Die Dichte des Verdachtes, der das Ersuchen initiiert, ist nur von der ersuchenden Strafverfolgungsbehörde einzuschätzen. Das BfV übt keine Aufsicht über die Strafverfolgungsbehörde aus und ist danach nicht gehalten nachzuprüfen, dass dem Ersuchen bestimmte Tatsachen zugrunde liegen oder die Verdachtsannahme überhaupt berechtigt ist.

Zu Absatz 2

Der Absatz definiert die besonders schweren Straftaten neu und trägt damit dem Beschluss des Bundesverfassungsgerichts zum Hessischen Verfassungsschutzgesetz (BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, BVerfGE 169, 130-235) Rechnung. Die Qualifizierung einer Straftat als besonders schwer muss nach diesem Beschluss in der Strafnorm selbst einen objektivierten Ausdruck finden (Rn. 206). Dieser Anforderung trägt § 48 Absatz 2 Rechnung.

Maßgeblich für die Schwere des tatbestandlichen Unrechts sind der Rang des verletzten Rechtsguts und andere tatbestandlich umschriebene, gegebenenfalls auch in einem Qualifikationstatbestand enthaltene Begehungsmerkmale und weitere Tatfolgen (a.a.O. Rn. 202). Dem trägt die neue Nummer 2 (tatbestandlich umschriebenen Begehungsformen oder Tatfolgen) Rechnung.

Wird beispielsweise wegen des Verdachts einer mitgliedschaftlichen Beteiligung an einer kriminellen Vereinigung (§ 129 StGB), die durch Begehung einer Sachbeschädigung (§ 303 StGB – isoliert kein übermittlungsfähiges Delikt) erfolgt ist, übermittelt, kann auch das

tateinheitliche Delikt der Sachbeschädigung verfolgt werden und zwar auch dann, wenn sich der Verdacht der kriminellen Vereinigung nicht gerichtsverwertbar anklagereif verdichten lässt.

Zu Nummer 1

Ausgehend vom Strafrahmen einer Strafnorm liegt eine besondere Schwere einer Straftat jedenfalls dann vor, wenn sie mit einer Höchstfreiheitsstrafe von mehr als fünf Jahren bedroht ist (vgl. BVerfGE 109, 279 <347 f., 349>; 165, 1 <93 Rn. 179>). Nach der gesetzlichen Systematik wird in Tatbeständen mit einem fünf Jahre übersteigenden oberen Strafrahmen sogleich eine Höchststrafe von zehn Jahren Freiheitsentzug oder mehr normiert. Sie ist denjenigen Delikten vorbehalten, die ein besonders schweres Tatunrecht aufweisen und damit den Bereich der mittleren Kriminalität eindeutig verlassen (vgl. BVerfGE 109, 279 <348>; BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, BVerfGE 169, 130-235, Rn. 203). Dies berücksichtigt die Regelung in Nummer 1, indem dort festgehalten wird, dass besonders schwere Straftaten solche Straftaten sind, die im Höchstmaß mit Freiheitsstrafe von mehr als 5 Jahren bedroht sind.

Zu Nummer 2

Die besondere Schwere der Straftat wird allerdings nicht allein durch den Strafrahmen indiziert (vgl. BVerfGE 109, 279 <344>). Jedenfalls für die Qualifizierung als schwer kann auch das geschützte Rechtsgut sowie dessen Bedeutung für die Rechtsgemeinschaft von Belang sein und daher bei der Einordnung des Gewichts einer Straftat ergänzend zum Strafrahmen berücksichtigt werden. Entsprechend kann eine Einstufung eines Straftatbestands als "schwer" bei einer Gesamtschau vertretbar sein, die insbesondere die jeweils geschützten Rechtsgüter in den Blick nimmt (vgl. BVerfGE 129, 208 <243>). Nichts anderes gilt im Ergebnis für die Einstufung einer Straftat als besonders schwer. Zwar hat im Ausgangspunkt der Strafrahmen eine maßgebende Indizwirkung. Auch hat das Bundesverfassungsgericht jedenfalls für die Wohnraumüberwachung und Online-Durchsuchung für das Vorliegen einer besonders schweren Straftat einen Strafrahmen mit einer Höchstfreiheitsstrafe von mindestens fünf Jahren nicht ausreichen lassen (vgl. BVerfGE 109, 279 <347 ff.>; 141, 220 <338 Rn. 316>). Im Übrigen aber kann eine Straftat mit einer angedrohten Höchstfreiheitsstrafe von mindestens fünf Jahren auch dann als besonders schwer eingestuft werden, wenn dies nicht nur unter Berücksichtigung des jeweils geschützten Rechtsguts und dessen Bedeutung für die Rechtsgemeinschaft, sondern auch unter Berücksichtigung der Tatbegehung bzw. Tatfolgen vertretbar erscheint (BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, BVerfGE 169, 130-235, Rn. 205).

Entsprechend listet die Anlage 1 zu § 48 Absatz 2 Nummer 2 Delikte mit einer angedrohten Höchstfreiheitsstrafe von mindestens fünf Jahren auf, deren Rechtsgüter eine hohe Bedeutung für die Rechtsgemeinschaft haben und die aufgrund einer objektivierten besonderen Begehungsform und/oder Tatfolge als besonders schwere Straftat im Sinne des Absatz 1 einzuordnen sind.

Zu § 49 (Übermittlung an inländische öffentliche Stellen ohne Möglichkeit operativer Anschlussmaßnahmen)

Die Regelung übernimmt den bisherigen § 22, wobei in Absatz 1 und 2 jeweils der einschränkende Satz 2 im Interesse wirksamer Aufgabenwahrnehmung entfällt (ein verfassungsrechtliches Erfordernis, Erhebungsschwellen bei der nachrichtendienstlichen Weiterverarbeitung grundsätzlich fortzuschreiben, besteht nicht; BVerfGE 141, 220 – Rn. 280, 289; 162, 1 – Rn. 270). Der bisherige Wortlaut stellte dabei auf belastende Maßnahmen mit Außenwirkung ab, Dies sollte Folgeeingriffe beschreiben, die nicht lediglich inormationell bleiben (Eingriff in die informationelle Selbstbestimmung durch Verarbeitung personenbezogener Daten), sondern aktionell direkt die individuelle Freiheitsausübung beschränken. Dies hat in der Praxis zu dem Missverständnis geführt, es sei eine Abgrenzung von

Binnenakten der Verwaltung intendiert, wonach auch Datenerhebungen bei Dritten außenwirkende Akte seien. Dieser Fehlinterpretation wird nunmehr mit Übernahme der Formulierung des Bundesverfassungsgerichts vorgebeugt.

Absatz 2 begründet eine besonders intensive Zusammenarbeit im nachrichtendienstlichen Bereich durch umfassende Teilhabe an sämtlichen relevanten Informationen (im Gegenstrom komplementäre Pflicht des BND nach § 10 Absatz 4 Satz 2 Nummer 1). Dies legt eine technische Unterstützung der Prozesse nahe, speziell wechselseitige Abrufverfahren auf geeignete strukturierte Datenbanken bei angemessenen organisatorischen Vorkehrungen zu Geheimscutz, Rechteverwaltung und Protokollierung. Gesetzlicher Regelung bedarf dies nicht, es bleibt sachgerechter der flexiblen Verwaltungsgestaltung, angepasst an die jeweiligen Bedarfe und technischen Gegebenheiten, überlassen.

Zu § 50 (Übermittlung an inländische öffentliche Stellen von Daten aus Gefahrenaufklärung)

Die vom Bundesverfassungsgericht formulierten Übermittlungsanforderungen beruhen auf dem von ihm formulierten Kriterium der hypothetischen Datenneuerhebung (BVerfGE 162, 1 - Ls. 3 und Rn. 231 ff.), das es für die Übermittlung nachrichtendienstlich ersterhobene Daten an Behörden mit operativen Befugnissen fortentwickelt (Rn. 170 ff).

Das Gericht hat das Kriterium allgemein bereits in seinem BKAG-Urteil (BVerfGE 141, 220) dogmatisch begründet. Im Kern stellt es eine besondere Finalitätsanforderung: Voraussetzung für eine Zweckänderung (auch durch Übermittlung) ist danach, dass die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten (BVerfGE 141, 220 - Rn. 288). Grundsätzlich verneint hat das Gericht dabei ausdrücklich die Relevanz von Schwellenanforderungen (etwa hinsichtlich des erforderlichen Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts), da die diesbezüglichen Anforderungen unter Verhältnismäßigkeitsgesichtspunkten primär den Anlass nur unmittelbar für die Datenerhebung selbst bestimmten, nicht aber auch für die weitere Nutzung der erhobenen Daten. Für die Übermittlung ist grundsätzlich regelmäßig ausreichend, dass sich aus den Daten – ggf. in Verbindung mit weiteren Kenntnissen der Empfängerbehörde - ein konkreter Ermittlungsansatz ergibt (Rn. 289).

Davon abweichende Besonderheiten gelten allerdings für die Übermittlung nachrichtendienstlich ersterhobener Daten (BVerfGE 162, 1 – Rn. 253), da diese Privilegierung der Zweckänderung gegenüber der Erhebung nur auf Daten Anwendung finden könne, die von Polizeibehörden unter den für diese geltenden Anforderungen erhoben sind, denen aber nicht zwangsläufig auch die Datenerhebung durch eine Verfassungsschutzbehörde unterlag (Rn. 170 ff.), da für sie abgesenkte Erhebungsschwellen genügen (Rn. 156). Die Schwellenabsenkung ist gerechtfertigt, weil sich das Eingriffsgewicht einer Erhebung auch nach den Folgen bestimmt und nach der Befugnisausstattung von Nachrichtendiensten allein informationelle Folgeeingriffe zu gewärtigen sind. Dies ändert sich bei Übermittlung an Stellen mit operativen Interventionsbefugnissen. Deshalb muss bei solcher Übermittlung die Übermittlungsschwelle das neue Folgenpotenzial gewichtend einbeziehen. Deshalb verlangt das Bundesverfassungsgericht hierfür die Schwelle, die für polizeilicher Gefahrerforschung durch heimliche Überwachungsmaßnahmen mit hoher Eingriffsintensität gilt. Dies ist die konkretisierte Gefahr für besonders gewichtige Rechtsgüter (BVerfGE 141, 220 - Rn. 112; BVerfGE 162, 1 - Rn. 158).

Nach diesem Ansatz kompensieren also die speziellen Übermittlungsschwellen die abgesenkte Erhebungsschwelle. Daraus folgt, dass dort, wo bereits die Datenerhebung nicht unter abgesenkten Voraussetzungen erfolgt ist, auch keine Sonderanforderungen an die Übermittlung zu stellen sind. Wenn die nachrichtendienstlich aufzuklärende Situation als konkretisierte Gefahr für besonders gewichtige Rechtsgüter zu qualifizieren ist, kann damit für die hierbei gewonnenen Informationen von den Sonderanforderungen an

Übermittlungsschwellen abgesehen werden. Für die Übermittlung von Daten, die auch die Polizei in solcher Situation ebenso hätte erheben dürfen, reicht dann wieder das Erfordernis konkreter Veranlassung (als tatsächlicher Anhaltspunkt, an dem empfängerseitige Folgeermittlungen ansetzen können).

Die Strafverfolgungsübermittlung ist in diesen Fällen also nicht an besondere Übermittlungsschwellen zu binden (BVerfGE 141, 220 - Rn. 289), aber an Straftaten, die den Einsatz intensiv eingreifender heimlicher Erhebungsmittel rechtfertigen (Rn. 288). Im Regelungssystem der Strafprozessordnung sind dies Straftaten von erheblicher Bedeutung, vgl. VM-Einsatz (§ 110a StPO) oder längerfristige Observation (§ 163f StPO). Der Begriff ist im Strafrecht etabliert und durch Rechtsprechung konkretisiert und danach zureichend inhaltlich bestimmt, um ebenso im Verfassungsschutzrecht aufgegriffen zu werden.

Zu § 51 (Übermittlung an inländische nichtöffentliche Stellen)

Zu Absatz 1

Die Regelung übernimmt den bisherigen § 22a und ergänzt bedarfsgerecht weitere Übermittlungssachverhalte. Der neue Absatz 1 Satz 2 regelt nunmehr die Subsidiarität gegenüber Übermittlungen an öffentliche Stellen, falls erheblich beeinträchtigende Folgen zu gewärtigen sind. Soweit eine Fachaufgabe von einer dazu zuständigen Verwaltungsbehörde wahrgenommen werden kann und das BfV an sie übermitteln darf, hat dies den Vorrang gegenüber einem nachrichtendienstlichen Kontakt mit nichtöffentlichen Stellen. Die Qualifikation als Beeinträchtigung erfolgt dabei aus der wertenden Perspektive der Rechtsordnung. Wenn etwa im Rahmen des Wirtschaftsschutzes gegenüber Cyberangriffen sensibilisiert wird und dadurch Erfolgsaussichten für Cyberangriffe reduziert werden, ist dies keine Beeinträchtigung von Angreifern, sie werden lediglich in die Schranken des Rechts verwiesen.

Der bisherige allgemeine Bezug der Übermittlung auf den Schutz besonders gewichtiger Rechtsgüter entfällt. Diese Zielrichtung wird gerade in den Nummern des Absatzes konkretisiert. Insofern war der allgemeine Zusatz in Bezug auf Nummern 1 und 2 überflüssig, in Bezug auf Nummer 3 hingegen teils unverständlich. Das Gewollte wird nunmehr deutlicher zum Ausdruck gebracht, indem Nummer 3 auf den Schutz vor Bedrohungen bezogen wird, also beispielsweise dem Schutz vor extremistischen Missbrauch von Fördermitteln.

Der Zweck nach Absatz 1 Nummer 1 bezeichnet die Finalität, bezieht also auch Unterstützungstätigkeiten der nicht-öffentlichen Stelle ein, etwa bei der Entwicklung von Mitteln oder Methodiken der nachrichtendienstlichen Aufgabenwahrnehmung.

Mit Absatz 1 Nummer 3 Buchstabe c wird nunmehr auch der Wirtschaftsschutz aufgenommen, zu dem das BfV intensiv berät, vornehmlich ohne Übermittlung personenbezogener Daten, was aber im Einzelfall aber geboten sein kann,

Der Zweck nach Absatz 1 Nummer 3 Buchstabe f (Präventions-, Ausstiegs- oder Deradikalisierungsprojekte) ist dabei künftig nicht mehr auf den Schutz solcher Projekte beschränkt, sondern kann auch deren sonstigen Unterstützung dienen. In der Regel werden solche Übermittlungen zwar auf der Einwilligung der betroffenen Person beruhen (so dass eine spezielle Befugnis nicht erforderlich ist), es sind aber auch Sonderfälle denkbar (z.B. Übermittlung Daten Dritter), in denen ebenfalls Übermittlung zulässig sein sollte.

In die Aufgabe der Kinder- und Jugendhilfe (Buchstabe g) sind in erheblichem Ausmaß private Träger eingebunden sind. Datenübermittlungen zum Schutz des Kindeswohls ermöglichen der empfangenden Stelle etwa eine Thematisierung potenzieller Kindeswohlgefährdungen im Rahmen einer laufenden Beratung.

Die neue Nummer 4 ist darauf gerichtet, über Bestrebungen in Fällen zu informieren, in denen Extremisten Möglichkeiten nutzen, die von Dritten eröffnet werden. Dabei geht es

darum, den Dritten eine informierte Entscheidung in gesellschaftlicher Verantwortung zu eröffnen, ob sie solche Bestrebungen dergestalt objektiv fördern wollen. Bei den Mitteln sind Online-Plattformen (Buchstabe a) als Agitationsmedium großer Reichweite, Veranstaltungsstätten als Basis der Außenwirkung wie auch der Stärkung organisatorischen Zusammenhalts (Buchstabe b), finanzbezogene Dienstleistungen als operative Grundlage des Aktionspotenzials (Buchstabe c) und Schießsporteinrichtungen als Trainingsstätten bewaffneter Militanz (Buchstabe d) aufgeführt. Für finanzbezogene Dienstleistungen wird dabei auf die Dienste nach § 2 GwG Bezug genommen, sie sind also nicht beschränkt auf Finanzdienstleistungen nach § 1 Absatz 1a Satz 2 KWG, sondern umfassen insbesondere auch Bankgeschäfte (§ 1 Absatz 1a Satz 2 KWG) und Zahlungsdienste oder das E-Geld-Geschäft (§ 1 Absatz 1 Satz 2 bzw. Absatz 2 Satz 2 ZAG).

Nummer 5 schafft Informationsmöglichkeiten, wo ein besonderer organisatorischer Wirkungsrahmen Beteiligten von Bedrohungen spezifisches Gefährdungspotenzial eröffnet. Hier soll ebenso wie bei der tatmittelbezogenen Nummer 4 der betreffenden Stelle informationell befähigt werden, selbst in gesellschaftlicher Verantwortung darüber zu entscheiden, ob sie dies unterbindet. Als folgengewichtige Organisationsrahmen für Agitation Beschäftigter oder von Mitgliedern sind Jugendeinrichtungen wegen der besonderen Vulnerabilität der Zielgruppe Buchstabe a), Reservistenverbände wegen des besonderen Potenzials des militärischen Hintergrundes (Buchstabe b) sowie Parteien (Buchstabe c) und politische Vereine wegen der immanenten Zielrichtung politischer Wirksamkeit sowie gemeinnützige und mildtätige Vereine (Buchstabe d) als besondere Gelegenheiten, verdeckt Anschlussfähigkeit herzustellen, aufgeführt. Da die Übermittlung zum Schutz vor Bedrohungen erforderlich sein muss, ist durchgängig Voraussetzung, dass für den Aufklärungsadressaten potenziell intransparent ist, für welche Zwecke, die von ihm eröffneten Möglichkeiten genutzt werden. Es geht allein um Transparenz, die Entscheidung über Folgen bleibt uneingeschränkt beim Dritten. Das BfV nimmt keine ordnungsbehördliche Funktion wahr, sondern allein seine originäre Aufgabe des Verfassungsschutzes durch Aufklärung, wie sie etwa auch den jährlichen Verfassungsschutzberichten zugrunde liegt.

Zu Absatz 2

Das Nachteilsverbot in Absatz 2 ist modifiziert. Um den Übermittlungszwecken verbessert Rechnung tragen zu können, werden Interventionen auch bereits zur Risikoprävention ermöglicht. Da dazu von den privaten Empfängerstellen keine hoheitlichen Befugnisse eingesetzt werden können und sie ihrerseits in Ausübung ihrer grundrechtlichen Freiheitsrechte handeln, braucht dies nicht ebenso restriktiv gestaltet zu werden, wie hoheitliche Anschlussmaßnahmen. Zudem gilt nach Absatz 1 Satz 1 ohnehin der Vorrang der Übermittlung an öffentliche Stellen, der die Bewältigung ordnungsrechtlicher Konfliktszenarien vorab in das bereichsspezifische Verwaltungsrecht ausleitet. Absatz 2 hat dadurch nur einen von vornherein sehr engen Anwendungsbereich.

Zu Absatz 1

Zu Nummer 5

Zu § 52 (Übermittlungsverbote)

Die Regelung folgt dem bisherigen § 23, wobei allerdings im Harmonisierungsinteresse nunmehr die neue Regelung des § 30 MADG in der Fassung des Regierungsentwurfs des Gesetzes zur Stärkung der Militärischen Sicherheit in der Bundeswehr (BR-Drs. 440/25) übernommen wird.

Zu § 53 (Minderjährigenschutz bei Inlandsübermittlung)

Die Regelung greift den bisherigen § 24 auf, gliedert dessen Inhalt systematischer und harmonisiert auch die Formulierung systematisierend. Wird die Beobachtung eines vormals Minderjährigen als Erwachsener fortgesetzt, erfolgt zu den vorhandenen Daten bei

Übermittlungen sachgerecht keine Differenzierung danach, ob sie noch zum Verhalten im Minderjährigenalter angefallen waren. Entscheidend ist hier, ob auch solche Daten für den Übermittlungszweck erforderlich sind.

Zu Nummer 1

Die Regelung entspricht dem bisherigen § 24 Satz 2, wobei jedoch bei der Anwendung des neuen § 51 der bisherige Ausschluss von Nummer 3 Buchstaben a bis d und h entfällt. Angesichts des Ausschlusses belastender Folgen ist ein solcher noch darüber hinaus gehender Ausschluss nicht angemessen. Die bisherige Einschränkung hatte insgesamt geringe Praxisbedeutung, ihr Wegfall kann jedoch speziell zum Schutz zweckgemäßer Verwendung öffentlicher Vorteilszuwendungen beitragen. Insgesamt sollten sachlich gebotene und angemessene Übermittlungen nicht unnötig ausgeschlossen werden.

Zu Nummer 2

Die Regelung greift den bisherigen § 24 Satz 3 Nummer 1 auf, allerdings ohne die bisherige Beschränkung beim administrativen Rechtsgüterschutz. Wenn das Ordnungsrecht besondere Vorkehrungen zum Schutz besonders gewichtiger Rechtsgüter trifft, sollte der Schutz auch wirksam sein, wenn Bedrohungen von Jugendlichen ausgehen.

Zu Nummer 3

Die Regelung erfasst bei der Anwendung des § 46 unter engeren Voraussetzungen die noch nicht von Nummer 2 erfassten Personen, die jünger als 14 Jahre alt sind. Die Formulierung des bisherigen Satzes 3 Nummer 2 wird redaktionell angepasst. Der bisherige Tatbestand „wenn nach den Umständen des Einzelfalls nicht ausgeschlossen werden kann, dass“ ist mit der negativen Formulierung in seinem positiven Voraussetzungsgehalt schwer zu erfassen. Klarer wird der Sachverhalt als Gefahrenverdacht formuliert, der nachrichtendiensttypisch niederschwellig ist, also zwar anknüpfend Indiztatsachen voraussetzt, Schlussfolgerungen hieraus aber wesentlich auf nachrichtendienstlichem Erfahrungswissen beruhen und dieser Verdacht sich wiederum auf die künftige Entstehung konkreter Gefahren bezieht. Im Ergebnis genügt eine entsprechende - einzelfallbezogen vertretbare - Risikoannahme.

Zu Buchstabe a

Die Regelung entspricht dem bisherigen § 24 Satz 3 Nummer 2 Buchstabe a.

Zu Buchstabe b

Die Regelung entspricht dem bisherigen § 24 Satz 3 Nummer 2 Buchstabe b. Allerdings sind auch die Mitgliedstaaten von EU und NATO mit aufgenommen. Dabei handelt es sich um Systeme gegenseitiger kollektiver Sicherheit. Dem entspricht, Informationen nicht nur zum Schutz der Organisationen, sondern auch zum Schutz der Bündnispartner zu verwenden.

Zu § 54 (Weiterverarbeitung durch Empfänger)

Die Regelung entspricht dem bisherigen § 25.

Zu § 55 (Übermittlung an ausländische sowie über- und zwischenstaatliche Stellen)

Die Regelung entspricht dem bisherigen § 25a. In der Minderjährigenschutzregelung des Absatzes 5 sind nunmehr bei Nummer 1 – wie bereits in § 53– nicht nur EU und NATO, sondern auch deren Mitgliedstaaten aufgenommen.

Zu § 56 (Ohne Ausübung besonderer Befugnisse gewonnene personenbezogene Daten)

Die Regelung verbeitert die bisherige herkunftsbezogene Übermittlungsregelung des § 25d auf solche Daten, die das BfV ohne Ausübung besonderer Befugnisse gewonnen hat. Dabei wird zur angemessenen Gestaltung der Übermittlungsschwelle im Näheren unterschiden.

Zu Absatz 1

Absatz 1 greift den bisherigen § 25d Absatz 1 auf. Eine Regelung zur automatisierten Übermittlung (bisheriger Satz 2) ist überflüssig und entfällt daher, auch zur Vermeidung unzutreffender Umkehrschlüsse für die übrigen Übermittlungsvorschriften.

Zu Absatz 2

Absatz 2 regelt den bisher in § 25d Absatz 2 geregelte Sachverhalt neu. Die Übermittlung dieser Informationen wird nicht mehr an die besonderen Voraussetzungen nach §§ 42 bis 45 gebunden. Diese Voraussetzungen folgen Rechtsprechungsanforderungen, die das Bundesverfassungsgericht ausdrücklich beschränkt auf Informationen gefordert hat, die mit nachrichtendienstlichen Mitteln erlangt worden waren (BVerfGE 162, 1 – Rn. 170, 234). Sie sind sachlich darin begründet, dass Nachrichtendienste heimliche Überwachung niederschwelliger ausführen können, weil sie über keine aktionellen Befugnisse verfügen, dies aber bei Übermittlung an Stellen mit solchen Befugnissen durch angehobene Schwellen auszugleichen ist (a.a.O. Rn. 158 f., 170). Die in § 8 Absatz 1 Satz 2 bezeichnete Schwelle (konkrete Veranlassung durch Einzelfallerforderlichkeit) ist dagegen kein Nachrichtendienstprivileg, so dass eine angehobene Übermittlungsschwelle unnötig ist.

Zu Absatz 3

Absatz 3 greift die vorstehenden Erwägungen insgesamt für Informationen auf, die nicht auf Grund besonderer Befugnisse (§ 3 Absatz 10) qualifiziert eingreifend gewonnen worden sind. Nicht mit nachrichtendienstlichen Mitteln gewonnen sind auch Informationen, bei denen das BfV zwar nicht transparent gemacht hat, wer die Daten erhebt, dabei aber auch kein schutzwürdiges Vertrauen in Anspruch genommen hat. Dies schließt beispielsweise allgemeine Internetermittlungen auch unter Verwendung einer Identitätsangabe ein, in deren Wahrhaftigkeit im Kommunikationskontext typischerweise kein Vertrauen investiert wird (vgl. BVerfGE 120, 274 – Rn. 311). Die Finalität zum Schutz besonders gewichtiger Rechtsgüter bleibt aber auch insoweit beibehalten. Informationen, die von ausländischen Nachrichtendiensten erlangt worden sind, werden jedoch von der erleichterten Übermittlung ausgenommen. Damit werden sie den vom BfV selbst nachrichtendienstlich gewonnenen Informationen gleichgestellt (obwohl typischerweise unbekannt bleibt, mit welchen Mitteln der ausländische Nachrichtendienst Informationen erhoben hat, regelmäßig auch nicht Rohdaten, sondern Erkenntnisse vom Partner übermittelt werden und die fremde Erhebung auch kein dem BfV zurechenbarer Eingriff ist).

Zu Absatz 4

Absatz 4 ist die Komplementärregelung zu Absätzen 2 und 3 für Strafverfolgungsübermittlungen. Die in Absätzen 2 und 3 geregelten Tatbestände der Datenerlangung beruhen nicht auf einem nachrichtendienstspezifischen Erhebungsprivileg, so dass hier eine Beschränkung der Übermittlung auf einen Deliktskatalog nicht erforderlich ist.

Zu § 57 (Übermittlung zum Schutz der betroffenen Person)

Die Regelung greift den bisherigen § 25b auf. Dabei erfolgt künftig aber eine allein objektive Interessenbetrachtung (weiterhin beschränkt auf Evidenz). Bei Mitteilung entlastender Erkenntnisse an Strafverfolgungsbehörden braucht also nicht zuvor die Einwilligung des Betroffenen eingeholt zu werden (was oftmals auch nicht in Betracht kommt, wenn dem

Betroffenen nicht bekannt werden darf, dass dem BfV solche Informationen zu seiner Person vorliegen). In anderen Sachverhalten kann auch nicht auf eine hypothetische Einwilligung sachgerecht abgestellt werden, etwa wenn der Betroffene sich aufgrund psychischer Probleme selbst gefährdet oder eine Gefährdung eines minderjährigen Betroffenen gerade vom Personensorgeberechtigten ausgeht. Die Regelung betrifft mit der Evidenzvoraussetzung im Ergebnis also Sachverhalte, in denen ohnehin mit Einwilligung zu rechnen ist, mit Ausnahme von Sonderkonstellationen, in denen der Schutzzweck dennoch gerade Übermittlung gebietet, dies im nachrichtendienstlichen Handlungsrahmen bei Umständen, die typischerweise ohnehin keine Konsultation des Betroffenen ermöglichen. Die Änderung dient damit gleichermaßen der Effizienz auch der Effektivität der Schutzmaßnahme.

Die Regelung geht als Spezialregelung für Schutzübermittlungen hierfür den Beschränkungen der übrigen Übermittlungsvorschriften vor. Satz 2 verdeutlicht, dass dies auch gegenüber der Minderjährigenschutzregelung in § 53 gilt. Übermittlungen zur Jugendhilfe sind also nicht an eine konkretisierte Gefahr gebunden und schließen auch keine Anschlussmaßnahmen aus, die im Rahmen der übergeordneten Hilfe auch belastende Wirkungen entfalten können.

Zu § 58 (Weitere Verfahrensregelungen)

Die Regelung entspricht dem bisherigen § 25c. Die Weiterverarbeitungsregelungen zu den nach Absatz 1 zu fertigenden Protokolldaten ist nunmehr querschnittlich in § 38 enthalten. Dabei gelten diese besonderen Folgeregelung weiterhin nur für solche Daten, die ausschließlich zum datenschutzbezogenen Protokollierungszweck nach Absatz 1 generiert worden sind. Die Fachdokumentation bleibt unbenommen, unterliegt also insbesondere auch nicht der Löschungsregelung des § 38.

Absatz 3 enthält – komplementär zu § 10 Absatz 1 Satz 2 – eine Regelung zur Einrichtung automatisierter Abrufverfahren. Die vorausgesetzte Eignung hat rechtliche Anforderungen (speziell die Gewährleistung der Übermittlungsvoraussetzungen) wie auch fachliche, die einerseits in technischen Bedingungen liegen und andererseits bei einem Nachrichtendienst im typischerweise gebotenen Geheimschutz. Gleichwohl kommen praktische Anwendungsfälle in Betracht, insbesondere in der Zusammenarbeit mit dem BND oder für Aufgaben nach § 49 Absatz 3 (etwa in der Sicherheitszusammenarbeit in gemeinsamen Zentren). Zur Kooperation mit den Landesverfassungsschutzbehörden und dem MAD ergibt sich solche technische Gestaltungsoption bereits aus § 6 Absatz 2 Satz 1.

In Absatz 4 Satz 4 ist neu eine Befristung der Mitteilungspflicht nach Übermittlung an nichtöffentliche Stellen aufgenommen. Der Zusatz dient der Verwaltungsvereinfachung, wenn auch nach langer Zeit eine Mitteilung nicht möglich war. Dies erscheint in Abwägung des hohen Gemeinwohlinteresses an wirtschaftlicher Verwaltung mit Betroffeneninteressen angemessen, da umgekehrt das Betroffeneninteresse an nachgängiger Kenntniserlangung bei lange zurückliegenden Sachverhalten in der Regel gemindert ist.

Zu § 59 (Nachberichtspflicht)

Die Regelung entspricht dem bisherigen § 26, erweitert die Nachberichtspflicht jedoch auch für den Sachverhalt der vorausgegangenen (Fach-)Öffentlichkeitsinformation.

Zu Abschnitt 4 (Schutzmaßnahmen)

Zu § 60 (Schutzmaßnahmen)

Die Regelung ergänzt die Übermittlungsbefugnisse des Abschnitts 3 um eine Befugnis, bereits selbst Schutzmaßnahmen vorzunehmen, um hierdurch im Interesse wirksamen Rechtsgüterschutzes Schutzlücken zu schließen. Die originäre Abwehraufgabe des Nachrichtendienstes besteht als Informationsdienstleister in der Weitergabe von Erkenntnissen auf Grund der informationellen Befugnisse in §§ 45 bis 57, um die Empfänger ihrerseits bei

der Abwehr der Bedrohungen informationell zu unterstützen. § 60 eröffnet zum wirksamen Rechtsgüterschutz dem BfV ergänzend auch die Möglichkeit, aktionell gegen Bedrohungen einzuschreiten. Zwar darf das BfV danach auf Gegenstände einwirken (wie bereits im Rahmen informationeller Befugnisse auch, etwa durch Eingriff in die Integrität informationstechnischer Systeme), es darf jedoch nicht körperliche Gewalt gegen Personen ausüben, was sich bereits unmittelbar aus dem Katalog der Einwirkungsobjekte in Absatz 2 Satz 1 ergibt, zusätzlich aber auch noch in Absatz 2 Satz 2 ausdrücklich herausgestellt wird. Die geregelte Intervention bleibt in der verdeckten Operation und ohne Möglichkeit, polizeitypisch Maßnahmen gegenüber Einzelnen mit Zwang durchzusetzen (vgl. BVerfGE 162, 1 – Rn. 154), im nachrichtendienstlichen Gepräge.

Der Übergang von informationeller zu aktioneller Fallbearbeitung erfordert wegen der geänderten Folgenpotenzialität allerdings eine angemessene Schwellenregelung, die für das BfV in § 60 ausgestaltet wird. Insgesamt bleibt der behördliche Charakter, Gefahren zu erforschen und Abwehr grundsätzlich durch Informationsweitergabe zu operationalisieren, in der Gesamtschau erhalten. Die Regelungen berücksichtigen lediglich, dass bei Gelegenheit der Gefahrerforschung auch Situationen auftreten, die zum wirksamen Rechtsgüterschutz eigenes Einwirken des BfV auf gefährdende Abläufe erfordern, und tragen dem insoweit punktuell Rechnung. Dies schließt Schutzlücken und ist hierdurch einerseits generisch in der auf Wirksamkeit angelegten Gesetzgebungskompetenz zum bundesbehördlichen Verfassungsschutz eingeschlossen, wie auch getragen von der staatlichen Schutzaufgabe, einschließlich grundrechtlicher Schutzpflichten.

Bei der Verhältnismäßigkeitswürdigung ist zudem zu berücksichtigen, dass die Interventionsbefugnisse sich gegenständlich auf Sachverhalte geringerer Eingriffsbedeutung beschränken, indem sie lediglich gegen Mittel, die zum Einsatz für Bedrohungen bestimmt sind, eröffnet ist. Besonders ausgeprägt ist dies, wo auf Einsatzmittel eines anderen Staates eingewirkt wird und danach ein grundrechtlicher Bezug ganz fehlt. Zudem ist der Tatbestand auf besondere Bedrohungen beschränkt, nämlich solche mit dem außerordentlichen Aktions- und Wirkungspotenzial eines staatlichen Angreifers bzw. solche mit der besonderen Schädigungsdimension eines terroristischen modus operandi, dabei gerichtet gegen herausragende Gemeinwohlinteressen und zudem nicht lediglich im Einzelfall bestehend, sondern strukturell angelegt (näher Begründung zu Absatz 3). Hier wären Schutzlücken rechtsstaatlich intolerabel. Eine insofern strukturell defizitäre Sicherheitsgewährleistung könnte die Legitimation des Staates grundlegend in Frage stellen.

Die verdeckten Einwirkungen stehen dabei unter vielfältiger unabhängiger Kontrolle. Soweit hierbei personenbezogene Daten verarbeitet werden, übt der Unabhängige Kontrollrat auch hier die Datenschutzkontrolle aus. Seine Zustimmung ist nach § 61 Absatz 2 Satz 2 zudem konstitutiv für die Einstufung der besonderen Bedrohungen und den erst hierdurch eröffneten Einsatz einwirkender Maßnahmen, eben beschränkt auf Phänomene, deren verhältnismäßigkeitssichernde Gefährlichkeit vom Unabhängigen Kontrollrat testiert ist. Schließlich steht der Normvollzug nach § 63 insgesamt unter laufender Kontrolle sowohl des Unabhängigen Kontrollrates wie des Parlamentarischen Kontrollgremiums, was wirksam gewährleistet, dass die Vollzugspraxis keine Fehlentwicklung nimmt.

Zu Absatz 1

Absatz 1 enthält eine Befugnis, die zugleich die entsprechende Aufgabe implizit einschließt. Eine besondere Aufgabenergänzung in § 2 Absatz 2 erscheint nicht sachgerecht, da die Verfassungsschutzaufgabe nicht originär hierauf gerichtet ist, die Regelung trägt vielmehr lediglich einem bei der Bedrohungsaufklärung eintretendem Handlungsbedarf Rechnung. Die annexe Ausgestaltung kommt in Satz 1 speziell zum Ausdruck. Das Kriterium der Erforderlichkeit umgehenden Einwirkens bezeichnet die Schutzlückensituation, bei der Verzögerungen durch Abgabe an eine andere Stelle Erfolgsrisiken begründen.

Satz 2 formuliert die Schutzlückensituation speziell, in der wirksame Abhilfe nur durch Eingreifen des BfV möglich ist.

Satz 3 verpflichtet zur Dokumentation der Maßnahmen, was auch effizienter Kontrollierbarkeit dient.

Zu Absatz 2

Der Absatz beschränkt die Einwirkungshandlungen der Schutzmaßnahmen auf einen Maßnahmekatalog. Der Maßnahmekatalog impliziert zugleich eine Beschränkung der Maßnahmerichtung auf Verantwortliche der Bedrohungssituation (jedenfalls im Sinne von Zustandsverantwortlichkeit) wie auch den Ausschluss personengerichteter Zwangsmaßnahmen, der zudem speziell in Satz 2 verdeutlicht wird.

Zu Nummer 1

Die Nummer regelt die Einwirkung auf Gegenstände, die zur Förderung der Bedrohung bestimmt sind. Der Begriff des Gegenstandes ist umfassend und betrifft Sachen (Buchstabe a) und Informationen (Buchstaben b bis d), wobei es nicht auf deren physische Verarbeitung ankommt (b und d), sondern ebenso unkörperliche Informationen (c) erfasst sind.

Zu Buchstabe a

Tatmittel sind beispielsweise Waffen oder Grundstoffe zur Herstellung von Sprengstoffen Ebenso können informationstechnische Geräte einschließlich der dort verwendeten Anwendungen (z.B. Software-Werkzeuge für Cyberangriffe) Tatmittel sein, sowohl in Angriffsoperationen wie auch als Koordinations- oder Führungsmittel innerhalb der Bedrohungen.

Auch Mittel, die erst künftig eingesetzt werden sollen, sind umfasst. Dies bezieht Beschaffungsvorgänge zu Tatmitteln, die etwa auf der Lieferkette manipuliert werden, ein.

Die Einwirkung kann auch durch Bereitstellung funktionsuntauglicher Tatmittel erfolgen.

Zu Buchstabe b

Das Einwirken kann zur Abwehr erforderlich sein, indem die Übertragung unterbunden, umgeleitet oder verändert wird. Die Informationsübertragung bezieht einerseits insbesondere sämtliche Telekommunikation (§ 3 Nr. 59 TKG) ein (inkl. Maschinenkommunikation mittels technischer Signale), ohne anderseits auf eine Übertragung mittels Kommunikationsanlagen beschränkt zu sein. Die Umleitung kann z.B. erforderlich sein, damit ein maliziöser Datenstrom nicht das vom Angreifer gewählte Zielsystem erreicht (damit dort keinen Schaden anrichten kann), für den Angreifer die Intervention aber unentdeckt bleibt, also die weitere Aufklärung laufender Angriffskampagnen und -muster unbeeinträchtigt bleibt.

Der Übertragungsvorgang wird als Gesamtheit betrachtet. Einwirkungsgegenstand ist danach nicht lediglich ein Datenstrom, sondern auch eine Speicherung auf dem Über-tragungsweg vor Erreichen des Empfängers, beispielsweise auf einem e-mail-Server.

Zu Buchstabe c

Wie bereits die inhaltliche Verfälschung übertragener Informationen, kann auch die gezielte sonstige Fehlinformation Beeinflussungsmittel sein, um Schädigungen zu vereiteln. Denkbar wären etwa Fehlinformationen über Tatgelegenheiten, die eine verdeckte Hilfsperson an den Angreifer heranträgt, um seine Angriffsrichtung in unschädliche Handlungen fehlzuleiten.

Buchstabe c erfasst Fehlinformation, die auf Steuerung von Bedrohungsaktivitäten oder des Zusammenwirkens Beteiligter zielt. Abzugrenzen ist dies von Fehlinformationen – etwa in Form einer Legendierung einer Person unter falscher Identität – die lediglich der Abtarnung dienen.

Zu Buchstabe d

Gegenstand können beispielsweise technische Anleitungen zur Herstellung von Sprengstoffen oder zur Sabotage öffentlicher Betriebe, etwa zu Schwachstellen und Sabotagemöglichkeiten bei Anlagen der Stromversorgung, sein. Weiteres Beispiel sind Beutedaten aus einem Cyberangriff, die der Angreifer noch nicht abschließend gesichert, sondern zur Verschleierung des Rücklaufs zunächst außerhalb seines Bereichs zwischengespeichert hat.

Zu Nummer 2

Der Begriff der Güter entstammt dem Außenwirtschaftsrecht (§ 2 Absatz 3 AWG).

Abweichend von Nummer 1 ist bei Nummer 2 unerheblich, ob die Güter im Weiteren zu gegen Deutschland gerichteten Bedrohungen eingesetzt werden sollen. Die Sicherheit des Bundes ist im Lichte der Einbettung Deutschlands in die kollektiven Sicherheitssysteme der Vereinten Nationen und der Europäischen Union auch im Sinne einer allgemeinen Gewährleistung der Sanktionsdurchsetzung und des Proliferationsausschlusses zu verstehen.

Zu Buchstabe a

Buchstabe a erfasst sämtliche Ausfuhrbeschränkungen nach dem Außenwirtschaftsge-setz und nach unmittelbar anzuwendendem Unionsrecht, speziell in Bezug auf Rüs-tungsgüter (inkl. Dual use) sowie durch Unionsrecht sanktionsverstrickte Güter.

Zu Buchstabe b

Buchstabe b ergänzt die Fälle, in denen bereits eine Ausfuhrbeschränkung besteht (Buchstabe a), um die Fälle, in denen eine administrative Ausfuhrbeschränkung nach § 6 AWG möglich wäre. Der dortige Rückbezug auf § 4 AWG schließt dessen Erläuterung in § 5 AWG um spezielle Fälle („insbesondere“) ein.

Zu Absatz 3

Absatz 3 definiert näher die interventionsrechtfertigenden Anlasssachverhalte. Sie sind geprägt von einem modus operandi (Nummer 1: terroristisches Vorgehen) bzw. der Systematik des Vorgehens (Nummer 2) und dabei jeweils qualifiziert durch hohes Gefährdungspotenzial bei besonderer Schadensintensität, die im terroristischen Vorgehensmuster bzw. der extremen Aktions- und Wirkungsmacht eines staatlichen Angreifers angelegt sind. Hierdurch ist einerseits generell für absehbare Zukunft mit solchen schädigenden Ereignissen zu rechnen (da modus operandi bzw. systematisches Vorgehen), andererseits muss der Schutzansatz komplementär strukturell ansetzen, darf sich nicht allein auf die Verhinderung eines isolierten Einzelereignisses ausrichten, sondern muss das Aktionspotenzial der operierenden Strukturen vorzugsweise insgesamt schwächen, dadurch dann auch die Realisierung jeden einzelnen künftigen Angriffs erschweren, hierdurch auch Angriffe verhindern und Schadenspotenzial eingrenzen. Solcher Abwehrauftrag deckt sich im Besonderen mit dem nachrichtendienstlichen Auftragsprofil, zwar auch auf Personen zu zielen, dies jedoch vornehmlich im Funktionszusammenhang übergeordneter Angreiferstrukturen.

Zu Nummer 1

Die Regelung erfasst terroristische Bestrebungen. Die tatbestandlich vorausgesetzten Planungen beziehen sich auf diesen modus operandi, sind also auf der Art nach bestimmte

Aktionen gerichtet, ohne dass bereits eine konkretisierte Tatplanung vorausgesetzt wird. Terroristische Bestrebungen beeinträchtigen besonders gewichtig die Sicherheit des Bundes, auch indem bei ungehindertem Betreiben typischerweise das Vertrauen der Bevölkerung in die staatliche Sicherheitsgewährleistung beeinträchtigt wird. Die prognostische Folgenqualifikation erheblicher Unruhe in großen Teilen der Bevölkerung ist mithin regelmäßig im terroristischen Vorgehensmodell angelegt, bleibt aber bezogen auf die konkrete Bestrebung zu prüfen. Große Teile der Bevölkerung können auch betroffen sein, wenn sich die Bestrebungen nur gegen eine Bevölkerungsgruppe richtet und die Unruhe vornehmlich in dieser Gruppe zu erwarten wäre, ebenso bei lediglich regional operierenden Bestrebungen.

Zu Nummer 2

Hoheitliche Einwirkungen auswärtiger Staaten auf deutschem Gebiet mit Auswirkungen auf deutsche Interessen (sicherheitsgefährdend oder geheimdienstlich operierend) verletzen generell die Sicherheit des Bundes, wenn sie – wie hier per se der Fall – ohne Zustimmung Deutschlands ausgeführt werden. Liegen Erkenntnisse über solche systematischen Tätigkeiten eines anderen Staates in Deutschland vor, dann ist auch für absehbare Zukunft mit weiteren solchen Tätigkeiten zu rechnen. Wenn in der Bevölkerung der Eindruck entsteht, dass der deutsche Staat solchem Treiben fremder Staaten in Deutschland nicht wirksam begegnen kann, höhlt dies das Vertrauen in die Funktionsfähigkeit der staatlichen Ordnung aus. Die Folgenqualifikation der besonders schweren Schäden weist allerdings über die bloße Verletzung der Gebietshoheit hinaus, ist aber regelmäßig ebenso darin angelegt, dass die fremde Macht systematisch in Deutschland operiert, wenn die Operationen schädigend ausgerichtet sind, speziell bei systematischer Spionage oder Sabotage, auch im virtuellen Raum durch planvolle Cyberangriffe, aber auch bei systematischen Einflussoperationen, die die demokratische Willensbildung verdeckt manipulieren oder transnationaler Repression gegen Exil-Oppositionelle in Deutschland.

Zu Absatz 4

Der Absatz betont die Beachtung der Verhältnismäßigkeit speziell.

Zu § 61 (Anordnung von Schutzmaßnahmen)

Zu Absatz 1

Der Absatz gibt begrenzende Grundentscheidungen vor, einerseits zu den Bedrohungen, gegen die Schutzmaßnahmen ergriffen werden dürfen, andererseits zu den eröffneten Maßnahmen.

Zu Absatz 2

Die Qualifikation als Bedrohung im Sinne des § 60 Absatz 3 ist der Amtsleitung vorbehalten. Sie muss zumindest jährlich neu geprüft und entschieden werden. Auch unterjährig ist die Einstufung aufzuheben, wenn sie vom Sachverhalt nicht mehr getragen ist. Die Einstufung unterliegt unabhängiger Rechtskontrolle durch den Unabhängigen Kontrollrat. Sie wird erst mit seiner Feststellung der Rechtmäßigkeit wirksam. Bei Gefahr im Verzug eröffnet Absatz 5 allerdings auch, vorläufig Anordnungen bereits auf Grundlage der Amtsleitungsentscheidung zu treffen (entsprechend § 31 Absatz 2 bis 4 UKRat-Gesetz).

Zu Absatz 3

Der Absatz gibt vor, dass der zulässige Maßnahmerahmen für jede eingestufte Bedrohung spezifisch festzulegen ist und zwar durch die Amtsleitung oder eine von ihr dafür festgelegte Abteilungsleitung. Die Maßnahmeauswahl ist bereits gesetzlich in § 60 Absatz 2 eng beschränkt. § 61 Absatz 3 bezweckt eine bedrohungsbezogene Spezifizierung. Diese kann eine festzulegende Teilmenge des gesetzlich eröffneten Instrumentars ebenso umfassen wie alle gesetzlich eröffneten Maßnahmen. Entscheidend ist eine Auseinandersetzung mit

den phänomenspezifischen Handlungsmöglichkeiten und -bedarfen. Sollte unerwartet Bedarf zum Einsatz zunächst nicht vorgesehener Maßnahmen auftreten, ermöglicht das Entscheidungsverfahren mit der möglichen Abteilungsleitungszuständigkeit gleichermaßen eine praxisgerechte Anpassungsflexibilität wie auch eine besondere Prüfungs- und Entscheidungszuständigkeit (und -verantwortung), die die Gesamtentscheidung nicht auf der ansonsten möglichen operativen Ebene (Absatz 4 Satz 1 Nummer 2, 2.Fall) belässt.

Zu Absatz 4

Zu Nummer 1

Die besonderen Maßnahmen unter Eingriff in private IT-Systeme oder die Wohnung werden über eine besondere Zuständigkeit der Einzelfallanordnung zusätzlich verfahrensgesichert, komplementär in Satz 2 auch durch unabhängige Vorabkontrolle des Einzelfalls.

Zu Nummer 2

Die Nummer enthält den Regelfall der Anordnungszuständigkeit, nämlich bei einer Abteilungsleitung oder einem von ihr bestimmten Volljuristen.

Zu Absatz 5

Der Absatz enthält für die Entscheidungen, die grundsätzlich unabhängiger Vorabkontrolle unterliegen, Eilfallregelungen für Gefahr im Verzug, die die Anwendung des dafür bereits allgemein im UKRat-Gesetz vorgesehenen Verfahrens vorsehen.

Zu § 62 (Unterstützung von Schutzmaßnahmen)

Der Paragraph regelt die Unterstützung durch Dritte. Nach Satz 1 nimmt der Dritte an der Rechtfertigung der BfV-Maßnahme teil, bei öffentlichen Stellen auch unabhängig davon, ob sie für eigene Aufgaben solche Befugnis besitzen, also amtshilfeerweiternd. Die Verantwortlichkeit für die Maßnahme bleibt unabhängig von der technischen Durchführung durch Dritte beim BfV. Die Rechtfertigung der Dritten ergibt sich aus dem Ersuchen. Sie haben demgemäß auch keine eigenen Prüfpflichten, komplementär das BfV keine Begründungsobliegenheit zum – regelmäßig geheimschutzbedürftigen – Rechtfertigungssachverhalt. Da die Dritten aber notwendig von der Maßnahme Kenntnis erlangen, sind sie nach Satz 2 entsprechend § 9 Absatz 3 zur Verschwiegenheit verpflichtet.

Satz 3 verstärkt die Unterstützungsrechtfertigung zur Unterstützungspflicht, dies für alle öffentlichen Stellen (Nummer 1), bei nichtöffentlichen Stellen (Nummern 2 und 3) jedoch beschränkt auf bereits besonders pflichtige Stellen (vgl. § 170 TKG und § 11 Absatz 1 Nummer 1 Buchstabe c), die im vorliegenden Zusammenhang besonders relevant sind.

Satz 4 schränkt die Unterstützungspflicht nach allgemeinen Grundsätzen ein, hier zugleich auch für die nichtöffentlichen Verpflichteten. Diese erhalten zudem im Falle der Hilfeleistung eine angemessene Entschädigung.

Zu § 63 (Besondere Kontrolle der Durchführung von Schutzmaßnahmen)

Das Berichtswesen nach Absatz 1 und 2 unterstützt die politische Kontrolle des Parlamentarischen Kontrollgremiums. Der Bericht des Bundesministeriums des Innern nach Absatz 1 bietet einen Gesamtüberblick, der eine quantitative Betrachtung durch umfassende Statistik eröffnet ebenso wie eine qualitative Analyse nach Anlässen und Wirkungen. Absatz 2 ergänzt dies durch unabhängige Stichprobenkontrollen der Rechtmäßigkeit durch den Unabhängigen Kontrollrat, die zugleich das Gesamtbild des Parlamentarischen Kontrollgremiums anreichern. Insgesamt wird damit ein wirksames Kontrollsystem als Vorkehrung gegen etwaige Fehlentwicklungen der Durchführungspraxis eingerichtet.

Zu Abschnitt 5 (Weitere Regelungen zur Eigensicherung)

Der Abschnitt übernimmt die bisherigen §§ 26b, 26c. Die Eigensicherung ist zwar nunmehr als spezielle Aufgabe in § 2 Absatz 4 geregelt und dies betreffende Gefährdungen in die Bedrohungsdefinition (§ 3 Absatz 4) aufgenommen, so dass die allgemeinen Befugnisse nach §§ 8 ff. auch insoweit anwendbar sind. Für bestimmte Gefährdungslagen, speziell zur Liegenschaftssicherung sind aber weiter situativ bedingt spezielle Befugnisse geboten, die auch aus Gründen inhaltlicher Bestimmtheit weiter mit den bereits bisher in §§ 26b, 26c getroffenen besonderen Regelungen beibehalten bleiben und in dem Abschnitt um weitere Regelungen ergänzt werden.

Zu § 64 (Schutz des Eigensicherungsbereichs)

Die Regelung übernimmt den bisherigen § 26b, wobei dessen Absatz 8 aber mit der neuen Einbettung der Eigensicherung in die allgemeinen Aufgaben- und Befugnisregelungen obsolet geworden ist.

Im Übrigen wird der bisherige Bezug auf sicherheitsgefährdende oder geheimdienstliche Tätigkeiten durch den mit diesem Gesetz neu eingeführten Begriff der funktionsgefährdenden Tätigkeiten (§ 2 Absatz 4) ersetzt.

Zu Absatz 1

In Absatz 1 wird nun auch ausdrücklich auf das Hausrecht Bezug genommen, um zu verdeutlichen, dass trotz erweiterter Regelungen (z.B. Ergänzung in Absatz 4 um einen Fall der Hausrechtsausübung) weiterhin kein das Hausrecht verdrängendes abschließendes Regelungsmodell besteht, sondern auch künftig Hausrecht zur Eigensicherung ausgeübt werden kann. Im Übrigen enthält der Abschnitt gemäß dem Vorbehalt des Gesetzes nötige Befugnisregelungen mit den dazu zu treffenden Ergänzungsregelungen, etwa zum Verfahren. Sonstige, eingriffsfreie Aufgabenwahrnehmung gründet sich allein auf die Aufgabennorm des § 2 Absatz 4. Dies betrifft beispielsweise die Untersuchung des Liegenschaftsumfelds nach dort deponierten Sachen, die nach Absatz 6 Nummer 2 sichergestellt werden können, oder die Detektion von Drohnen, auch um sie ggf. nach § 66 Absatz 1 Nr. 2 abzuwehren.

Zu Absatz 2

In Absatz 2 wird der Fall der Identitätsfeststellung in Satz 2 neu aufgenommen.

Zu Absatz 3

In Absatz 3 Nummer 4 wird zusätzlich auch Durchsuchung auf Gegenstände eröffnet, die verdeckt für funktionsgefährdende Tätigkeiten eingebracht werden sollen.

Zu Absatz 4

In Absatz 4 wird neben der bisherigen Raumüberwachung durch Videotechnik im neuen Satz 1 auch die verdachtsunabhängige Durchsuchung von Räumen aufgenommen. Solche Maßnahmen können auch auf das Hausrecht gestützt werden, Da dies allerdings ebenso für die Videoüberwachung gilt und diese bereits geregelt ist, erscheint folgerichtig, auch die Durchsuchung von Räumen im Gesetz aufzunehmen.

Zu Absatz 5

In Absatz 5 verdeutlicht eine neu eingefügte Nummer 2, dass auch vorschriftswidrig eingebrachte Gegenstände – z.B. ein Smartphone – sichergestellt und untersucht werden können, so dass sich mithin nicht mehr die Frage stellt, ob das vorschriftswidrige Einbringen

bereits als tatsächlicher Anhaltspunkt für eine funktionsgefährdende Tätigkeit zu bewerten ist.

Zu Absatz 6

In Absatz 6 wird eine Regelung zur Sicherstellung verdächtiger, nicht personenzuordenbarer Gegenstände im Nahumfeld des Eigensicherungsbereichs aufgenommen (neue Nummer 2), beispielsweise verdeckt aufgestellte Videotechnik. Das Absuchen des Liegenschaftsumfelds nach solchen Sachen hat keinen Eingriffsgehalt und ist damit auf § 2 Absatz 4 zu stützen.

Zu Absatz 7

Absatz 7 fügt die bisher als Verfahrensregelung in § 26c Absatz 7 enthaltene Vorschrift zur Anwendung unmittelbaren Zwangs wegen des Eingriffsgehalts nunmehr in die materielle Befugnisregelung des § 63 ein. Inhaltlich wird die Vorschrift bruchloser in das Bundesrecht eingefügt, indem die einschlägigen Regelungen des Gesetzes über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes zur Konturierung und Beschränkung der Befugnis entsprechend anwendbar werden. Dies führt mit der Nummer 3 zur ergebnisgleichen Regelung gegenüber dem bisherigen § 26c Absatz 7. Neu hingegen sind die Anwendungsfälle in Nummern 1 und 2.

Zu Nummer 1

Nummer 1 erfasst sowohl die Gefahr des unbefugten Zutritte wie auch die bereits eingetretene Störung. Anders als bei Nummer 3 werden hier die Mittel unmittelbaren Zwangs nicht speziell eingeschränkt. Erfolgt der Angriff bewaffnet oder mit gefährlichen Werkzeugen müssen zu dessen Abwehr unter Umständen als ultima ratio auch Waffen eingesetzt werden.

Zu Nummer 2

Ebenfalls neu ist die Abwehr gegenwärtiger Gefahren nach Nummer 2. Auch für solche Gefahrenabwehr sind die Zwangsmittel nicht beschränkt, weil hier ebenso auf den jeweiligen Angriff – der womöglich mit Waffen ausgeführt wird – jeweils adäquat reagiert werden muss.

Zu Nummer 3

Die Regelung entspricht dem bisherigen § 26c Absatz 7.

Zu Absatz 8

Die Regelung entspricht dem bisherigen § 26b Absatz 9.

Zu § 65 (Verfahren im Eigensicherungsbereich)

Die Regelung übernimmt den bisherigen § 26c, wobei der Kernbereichsschutz nunmehr in die neue Vorschrift des § 66 (Ergänzende Regelungen zur Verarbeitung personenbezogener Daten) als dortiger Absatz 2 aufgenommen ist und die Anwendung unmittelbaren Zwangs in §59 Absatz 6. Zudem wird in Absatz 5 ein Schlusssatz angefügt, der die Rückgabe eines Gerätes der Informations- und Kommunikationstechnik von der Mitwirkung bei der vorherigen Herstellung eines auswertbaren Speicherabbildes abhängig macht.

Zu § 66 (Schutz vor unbemannten Fluggeräten)

Die Regelung wird über den bisher mit § 26b Absatz 7 vorgesehenen Liegenschaftsschutz hinaus künftig auch zur Absicherung eingesetzter Personen und daher als eigener

Paragraph getroffen. Da der Liegenschaftsschutz erhalten bleibt, und im Übrigen die Einsatzsicherung auch nicht auf nachrichtendienstliche Operationen beschränkt ist, bleibt die Regelung im gesonderten Abschnitt der Eigenschutzmaßnahmen, anders als die Absicherung verdeckt eingesetzter Personen mit § 28, der als reiner Annex zum Einsatz nachrichtendienstlicher Mittel dort geregelt ist.

Zu Absatz 1

Schutzobjekt sind sowohl der Eigensicherungsbereich (wie bisher) als auch eingesetzte Personen (neu). Der Einsatzbezug verknüpft die Regelung mit der Wahrnehmung der dienstlichen Aufgabe. Eine Absicherung im privaten Bereich ist von der Vorschrift nicht eröffnet. Zur normenklaren Eingrenzung der Abwehrbefugnis wird diese auf einen Radius von 100 Meter um die Schutzobjekte begrenzt. Der 100-Meter-Radius ist bereits in § 21h Absatz 3 Nummer 4 LuftVO enthalten und für eine wirksame Intervention auch nicht zu reduzieren. Der Aufklärungsradius, in dem Fluggeräte detektiert werden, ist zur Lageerfassung und -prüfung notwendig wesentlich weiter, ohne dass dies näherer gesetzlicher Regelung bedürfte, denn die bloße Detektion des Fluggerätes hat keinen eigenen Eingriffsgehalt.

Der Bezug auf § 21h Absatz 3 Nummer 4 der Luftverkehrs-Ordnung bleibt erhalten, da er den Überflug ohne Höhenbegrenzung auf 100 Meter einbezieht. Die Regelung bezieht sich auf das geografische Gebiet, unabhängig davon, ob womöglich eine in der Vorschrift vorbehaltene Zustimmung der zuständigen Stelle vorliegt. In der gegenwärtigen Situation des Überflugs muss die Befugnis zur wirksamen Abwehr an dem feststellbaren Sachverhalt anknüpfen. Falls – grundsätzlich nicht erwartbar – eine Zustimmung vorliegt, sind etwaige Schäden nach Absatz 3 zu regulieren.

Zu Absatz 2

Im Falle eines abgewehrten Drohneneinsatzes ist die Untersuchung des eingesetzten Tatmittels zur Aufklärung des Vorfalls erforderlich. Dies ermöglicht Absatz 2, nötigenfalls auch mit Mitteln unmittelbaren Zwangs. Die Aufklärung des Vorfalls jenseits der Untersuchung der Drohne ist in der allgemeinen Vorschrift des § 63 Absatz1 mitgeregelt.

Zu § 67 (Ergänzende Regelungen zur Verarbeitung personenbezogener Daten)

Die Verarbeitung personenbezogener Daten nach diesem Abschnitt erfolgt zur behördlichen Aufgabe der Eigensicherung (§ 2 Absatz 4) und findet danach grundsätzlich ohne Weiteres ihre Grundlage in §§ 8 ff. Eine Besonderheit der Wahrnehmung dieser Aufgabe nach diesem Abschnitt besteht allerdings darin, dass sie teils bereits vorbeugend – situativ präventiv – erfolgt, also beispielsweise sämtliche Personen mit Liegenschaftszutritt kontrolliert werden, unabhängig davon, ob zur Person Anhaltspunkte für funktionsgefährdende Tätigkeiten bestehen. Diesen Besonderheiten trägt der neue § 67 mit ergänzenden Regelungen Rechnung.

Zu Absatz 1

Der Absatz ergänzt die allgemeine Befugnis in § 9 Absatz 1 um eine zusätzliche Befugnis, die ihrerseits nicht bereits im Einzelfall bestehende Anhaltspunkte auf Bedrohungen voraussetzt, sondern dem Präventionszweck gemäß bereits aus Anlass der Risikosachverhalte nach Nummern 1 und 2 ausgeübt werden kann.

Zu Absatz 2

Der Absatz integriert die bisher in § 26c Absatz 6 enthaltene Regelung zum Kernbereichsschutz inhaltlich in den neuen Datenverarbeitungsparagraphen. Die Ausgestaltung erfolgt dabei nunmehr im Verweisungsweg auf die mit dem neuen Bundesverfassungsschutzgesetz in § 31 querschnittlich (für die Anwendung nachrichtendienstlicher Mittel) getroffene Regelung zum Kernbereichsschutz.

Zu Absatz 3

Die anlassgebenden Risikosituationen nach Satz 2 rechtfertigen die Speicherung als Personendatensatz allein zur Prüfung auf tatsächliche Anhaltspunkte für funktionsgefährdende Tätigkeiten. Deshalb trifft der Absatz entsprechende Einschränkungen, die sich insbesondere bei der Zweckbindung und Speicherhöchstdauer auswirken, indem auf die Maßgaben verwiesen wird, die in §§ 36, 38 bereits zur Prüffallregelung des § 36 Absatz 2 Satz 1 Nummer 2 getroffenen sind. Dies betrifft nur die geregelte strukturierte Speicherung zur Person. Sonstige Speicherungen, insbesondere in Sachvorgängen und -akten, bleiben hiervon unberührt.

Satz 2 Nummer 2 betrifft Personen, die in einem Zusammenhang mit einem nach Buchstaben a und b aufklärungsbedürftigen Sachverhalt stehen, wenn dieser Zusammenhang seinerseits zur Klärung des Sachverhalts aufklärungsbedürftig ist. Dabei kann es sich beispielsweise um den Eigentümer von Gegenständen nach Buchstabe a oder den Führer des Fluggerätes nach Buchstabe b handeln, wenn noch unklar ist, ob der Gegenstand oder Flug eine funktionsgefährdende Funktion hatte.

In Nummer 2 Buchstabe a ist § 63 Absatz 5 Nummer 1 deshalb nicht aufgeführt, weil in diesem Sachverhalt bereits tatsächliche Anhaltspunkte für funktionsgefährdende Tätigkeiten vorliegen, so dass hier auch eine strukturierte Speicherung zur Person nach § 36 Absatz 2 Satz 1 Nummer 1 ohne weiteres eröffnet ist.

Zu § 68 (Mitbestimmung bei Maßnahmen der Eigensicherung)

Die Eigensicherung des BfV insbesondere durch technische Einrichtungen dient der Funktionssicherung der Behörde gegen Angriffe auf ihre Funktionsfähigkeit. Allerdings würde eine Mitbestimmung der Personalvertretung beim Einsatz von Maßnahmen der Eigensicherung die Wirksamkeit dieser Eigensicherungsmaßnahmen gefährden. Denn es würde ein größerer Personenkreis von den konkreten Maßnahmen Kenntnis erlangen. Daher werden mit der vorliegenden Regelung Ausnahmen von den Regelungen zur Mitbestimmung in § 80 Absatz 1 Nummer 18 und Nummer 21 Bundespersonalvertretungsgesetz vorgesehen. Damit entfällt bei Maßnahmen der Eigensicherung die Mitbestimmung des Personalrats bei Regelungen der Ordnung in der Dienststelle und des Verhaltens der Beschäftigten (Nummer 18) und Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen (Nummer 21).

Da sich der Zweck dieser Vorschrift am Ziel der wirksamen Eigensicherung ausrichtet, dürfen die nach § 68 der Mitbestimmung entzogenen Maßnahmen ausschließlich zur Eigensicherung und nicht zur Ordnung allgemeiner Arbeitsverhältnisse (etwa zur Leistungskontrolle) angewendet werden. Zudem muss das BfV auch in diesen Fällen im vertrauensvollen Zusammenwirken mit der Personalvertretung Mitarbeiterbelange sachgerecht berücksichtigen. Angesichts der besonderen Gefährdung des BfV besteht insoweit allerdings ein genereller Vorrang der Sicherung des BfV gegen funktionsgefährdende Tätigkeiten von Innentätern. Mit Blick auf das Ziel, die Funktionsfähigkeit der Behörde zu gewährleisten, überwiegen hier die Aspekte des Gemeinwohls.

Auch eine nähere gesetzliche Eingrenzung der von der Mitbestimmung ausgenommenen Eigensicherungsmaßnahmen bietet sich mit Blick auf das Ziel der Funktionssicherung nicht an. Die nähere Ausgestaltung von Eigensicherungsmaßnahmen muss flexibel bleiben, um an die jeweiligen örtlichen, technischen und situativen Anforderungen der Beschäftigungsbehörde angepasst werden zu können. Der Behörde muss also ein Gestaltungsspielraum verbleiben.

Zu Abschnitt 6 (Allgemeiner Datenschutz und Rechtskontrolle)

Zu § 69 (Anwendung des Bundesdatenschutzgesetzes)

Die Regelung entspricht dem bisherigen § 27. Die bisher querschnittlich für die gesamte Datenverarbeitung in § 8 Absatz 1 Satz 1, letzter Halbsatz geregelte Einwilligung wird nunmehr als querschnittliche Regelung in § 69 angefügt (Maßgabe am Ende der Nummer 2).

Zu § 70 (Unabhängige Rechts- und Datenschutzkontrolle)

Die Regelung ordnet die Kontrollzuständigkeiten neu und mit dem integralen Ansatz zur Kontrolle der operativen Aufgabenwahrnehmung in Absatz 2 Nummer 1 dabei effektiver.

Mit dem Artikel 10-Gesetz entfällt auch die Sonderkontrolleinrichtung der G 10-Kommission.

Der jeweils sektoral (Absatz 2 Nummer 1 und Nummer 2) integrale Kontrollansatz verringert Schnittstellenbedarfe zwischen den Kontrollinstanzen, erübrigt aber keineswegs punktuelle Zusammenarbeit, soweit Bezüge zwischen den jeweiligen Zuständigkeiten bestehen, etwa hinsichtlich der informationellen Zusammenarbeit des BfV mit anderen Bundesbehörden, die der Datenschutzkontrolle der/des BfDI unterliegen. Insoweit ist Abstimmung zwischen den Kontrollinstanzen geboten, ohne dass dies gesetzlicher Anleitung bedarf.

Da Regelungsgegenstand nicht allein die Datenschutzkontrolle, sondern auch die Kontrolle von Schutzmaßnahmen (§ 60) einbezogen ist, wird die Paragraphenüberschrift um den Begriff der Rechtskontrolle ergänzt.

Zu Absatz 1

Der Absatz greift das allgemeine Petitionsrecht des bisherigen § 28 Absatz 1 auf und erstreckt es auf Schutzmaßnahmen.

Zu Absatz 2

Der Absatz regelt die Aufgabenverteilung zwischen Unabhängigem Kontrollrat und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Zu Nummer 1

Zu Buchstabe a

Die Regelung stärkt wirksame Kontrolle, indem sie eine integrale Kontrollzuständigkeit für die operative Aufgabenwahrnehmung des BfV schafft, diese also nicht in die Vorabkontrolle von Anordnungen durch eine Stelle (Unabhängiger Kontrollrat, § 34) und die allgemeine Datenschutzkontrolle durch eine andere Stelle (bisher BfDI) aufspaltet, sondern die Gesamtzuständigkeit im Unabhängigen Kontrollrat fusioniert. Dies bezieht auch die fachunterstützenden Aufgaben ein, sowohl in technischer Hinsicht (wie die Bereitstellung von Datenverarbeitungsanlagen und Fachanwendungen) wie auch operativ (bei gebündelten Querschnittsaufgaben, etwa bei der Observation oder Finanzermittlungen). Die Kontrolle am Maßstab des Bundesverfassungsschutzgesetzes ist danach insgesamt Sache des Unabhängigen Kontrollrates. Dies schließt die Eigensicherung als operative Aufgabe ein, zumal der Schwerpunkt hier bei Angreifern liegt, die der Beobachtung des BfV unterliegen, so dass eine unterschiedliche Zuständigkeitszuordnung einer wirksamen Wahrnehmung der Kontrollaufgabe abträglich wäre.

Der Kontrollrahmen erstreckt sich auf die Datenverarbeitungsverantwortlichkeit des BfV, bei Verbunddatenbanken (wie das nachrichtendienstliche Informationssystem oder die Antiterrordatei) also auf Datensätze im BfV-Besitz und dann auf allgemeine organisatorische oder

technische Anforderungen, wenn das BfV die Datenbank bereitstellt (wie beim nachrichtendienstlichen Informationssystem, nicht bei der Antiterrordatei).

Wie die Vorabkontrolle bestimmter Anordnungen ist auch die Datenschutzkontrolle des Unabhängigen Kontrollrates gehalten, bei ihrer Durchführung auch besondere Funktionsanforderungen effektiver Aufgabenwahrnehmung der kontrollierten Behörde zu berücksichtigen und mit dem eigenen Kontrollauftrag zum schonenden Ausgleich zu bringen. Das gilt speziell für das Erfordernis des Quellenschutzes (vgl. § 13 Absatz 4 UKRat-Gesetz).

Zu Buchstabe b

Entsprechend der Systematisierung durch Nummern 1 und 2 liegt die Kontrolle der operativen Aufgabenwahrnehmung auch in Bezug auf Schutzmaßnahmen ebenso beim Unabhängigen Kontrollrat.

Zu Nummer 2

Im Übrigen verbleibt es bei der Datenschutzkontrolle der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Diese betrifft beispielsweise die Personaldatenverarbeitung im BfV oder auch dessen Mitwirkung bei Sicherheitsüberprüfungen. Insoweit ist die Erwägung einer integralen Kontrollzuständigkeit kein Argument für die Aufgabenübernahme durch den Unabhängigen Kontrollrat. Umgekehrt wäre es widersinnig, im Prozess der Sicherheitsüberprüfung die Kontrolle der zuständigen Stelle und der mitwirkenden Behörde auf verschiedene Kontrollbehörden aufzuspalten. Auch eine Kontrolle der Personalverwaltung gewinnt nicht an Wirksamkeit, wenn sie mit der Kontrolle der operativen Aufgaben verbunden wird. Umgekehrt wird insoweit eine Fachexpertise (zur Fachmaterie des Personaldatenrechts) benötigt, die für die Kontrolle der operativen Aufgaben bedeutungslos, aber bei der/dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit querschnittlich aufgebaut ist.

Zu Absatz 3

Absatz 3 verweist im Interesse der der Normenklarheit auf die jeweils die Kontrolle regelnden Gesetze. Die Pflicht des BfV zur Unterstützung der oder des Bundesbeauftragten für den Datenschutzes richtet sich dabei nach § 36a SÜG. Die bereichsspezifische Unterstützungsregelung ist identisch mit dem bisher geltenden § 28 Absatz 3, der allerdings durch die Neureglung ersetzt wird, so dass darauf nicht verwiesen werden kann.

Zu § 71 (Auskunft an betroffene Personen)

Die Regelung übernimmt den bisherigen § 15 gestaltet ihn im Einbezug von Akteninhalten aber betroffenenfreundlicher. Bisher war dieser Anspruch in § 15 Absatz 1 Satz 2 auf Speicherungen beschränkt, über Fundstellennachweise im Nachrichtendienstlichen Informationssystem erschlossen sind. Der neue Absatz 1 Satz 2 bezieht alle auf den Auskunftssachverhalt bezogen Daten der betroffenen Person ein, die mit vertretbarem Aufwand einbeziehbar sind. Dies gilt per se für die strukturiert zur Person gespeicherten Daten, die im Nachrichtendienstlichen Informationssystem nachgewiesen und dadurch aufwandsgering zuordenbar und auffindbar sind. Im Übrigen kann ein unverhältnismäßiger Aufwand etwa dann vorliegen, wenn bei sonstigen Daten bereits deren Auffinden erheblichen Aufwand verursacht, insbesondere durch Prüfung der Frage, ob die festgestellten Informationen überhaupt den Antragsteller betreffen (Identitätsprüfung), speziell wenn eine erhebliche Anzahl an Dokumenten gesichtet und geprüft werden müsste. Im Falle unverhältnismäßigen Aufwandes intendiert die Regelung zugleich eine grundsätzlich ablehnende Ausübung des verbleibenden Ermessens. Im Regelfall kann die Behörde dann das Auskunftsbegehren insoweit ohne fallbezogene Ermessensbetätigung unter Verweis auf die gesetzliche Wertung ablehnen.

Allgemein gilt, dass es zur Erfüllung des Auskunftsanspruchs grundsätzlich ausreicht, wenn der Inhalt der gespeicherten Daten zusammengefasst und mit eigenen Worten wiedergegeben wird (vgl. BVerwGE 183, 158 – Rn. 27). Auch hierbei sind also allgemeine Anforderungen wirtschaftlicher Verwaltung zur Vermeidung unangemessener Aufwände berücksichtigungsfähig.

In Absatz 2 Nummer 2 wird der geschützte Personenkreis über die bisher erwähnten „Quellen“ hinaus auf alle „verdeckt eingesetzte Personen“ schutzzweckkonform erweitert. Hierunter zu verstehen sind sowohl verdeckt eingesetzte Bedienstete als auch verdeckte Hilfspersonen.

Bei der Regelung zur Begründung einer Auskunftsablehnung in Absatz 4 wird das Kontrollverfahren an die neue Zuständigkeit des Unabhängigen Kontrollrates angepasst und danach die Begründungspflicht gegenüber dem Unabhängigen Kontrollrat in den Ausschlussgründen nach Satz 4 mit der – engen – allgemeinen Regelung des UKRat-Gesetzes synchronisiert.

Zu Abschnitt 7 (Schlussvorschriften)

Zu § 72 (Kontrolle und Durchsetzung von Unternehmenspflichten)

Die Regelung übernimmt die Bestimmungen des § 183 TKG für die entsprechende Aufsicht über die gesetzlichen Pflichten nach §§ 11 bis 15, auch in Verbindung mit deren Konkretisierungen in Verordnungen nach § 77.

Zu § 73 (Besondere Anzeige- und Genehmigungspflicht für ausgeschiedene Bedienstete)

Zu Absatz 1

[…]

Zu Absatz 2

[…]

Zu § 74 (Strafvorschriften)

Zu Absatz 1

Die Regelung greift die partikuläre Regelung des bisherigen § 18 G 10 verallgemeinernd auf, indem nunmehr die allgemeine Stillschweigensverpflichtung des § 9 Absatz 3 Nummer 1 strafbewehrt wird.

Zu Absatz 2

Absatz 2 regelt besonders schwere Fälle der Straftat nach Absatz 1. Der Strafrahmen entspricht dem nach Absatz 3.

Zu § 75 (Ordnungswidrigkeiten)

Die Regelung übernimmt den bisherigen § 19 G 10 insgesamt für die Unternehmenspflichten und erweitert die Bußgeldbewehrung der Verpflichtungen beim vorbeugenden personellen Geheimschutz auf die neue Vorsorgepflicht nach § 14 Absatz 3 Satz 6. Zudem wird der neue § 72 Absatz 1 Satz 2 angelehnt an § 208 Absatz 2 Nummer 61 TKG ebenfalls bußgeldbewehrt.

Der Bußgeldrahmen wird an neuere vergleichbare Regelungen angepasst. Absatz 2 Nummer 1 orientiert sich an der Bußgeldbewehrung des § 170 Absatz 1 Nummer 6 TKG durch § 228 Absatz 7 Nummer 3 TKG, da es gleichermaßen um die Vereitelung der rechtlich vorgesehenen Informationsgewinnung geht. Absatz 2 Nummer 2 sanktioniert die Verletzung von Pflichten zu organisatorischen Vorkehrungen, weshalb sich der Bußgeldrahmen an der Bewehrung von § 170 Absatz 1 Nummer TKG durch § 228 Absatz 7 Nummer 2 TKG orientiert. Absatz 2 Nummer 3 greift den Rahmen aus § 228 Absatz 7 Nummer 4 TKG auf.

Zu Absatz 1

Zu Nummer 5

[…]

Zu Nummer 6

[…]

Zu Absatz 2

Zu Nummer 4

[…]

Zu Nummer 5

[…]

Zu § 76 (Spannungs- und Verteidigungsfall)

Im Spannungs- und Verteidigungsfall gewinnen Bedrohungen, denen der Verfassungsschutz begegnet eine neue Qualität und Dimension. Dies bedingt, dass die Angemessenheitsrelation gegenüber Verfahrenslasten und operativen Risiken wie auch die Zumutbarkeitsabwägung zur Inanspruchnahme Dritter situationsgerecht neu auszutarieren ist. Dem dienen die Maßgaben dieses Paragraphen.

Zu Absatz 1

Der Absatz regelt den Anwendungsbereich des Paragraphen.

Zu Absatz 2

Der Absatz eröffnet, Auskunftspflichten und technische Mitwirkungspflichten Privater bei Sonderbedarfen im Spannungs- oder Verteidigungsfall zu erweitern. Dies betrifft gleichermaßen den Verpflichtetenkreis, wie die Leistungsgegenstände. Verpflichtet werden können jedoch nur Unternehmen der gewerblichen Wirtschaft. Die Verpflichtung bleibt beschränkt auf Leistungen, die mit ihren betrieblichen Mitteln (wenn auch womöglich neben ihrem betrieblichen Einsatzfeld) möglich sind. Einbezogen sind Materialien des Geschäftsbetriebs wie etwa Handbücher oder technische Spezifikationen zu betrieblichen Produkten, die möglicherweise vom nachrichtendienstlichen Gegenüber genutzt werden und danach von Aufklärungsinteresse sind.

Grundsätzlich liegt die Befugnis beim BMI. Mit Zustimmung des BMI kann auch das BfV selbst die Befugnis ausüben. Die Zustimmung kann auch allgemein für eine Reihe gleichgelagerter Fälle erteilt werden. Das Gleichgelagertsein betrifft sowohl den Bedarfssachverhalt wie auch den Umfang der Mitwirkungspflichten, die in der Zustimmung der Art nach festzulegen sind.

Ein Unterstützungsersuchen darf betriebliche Belange des Verpflichteten oder konkurrierende Sicherstellungspflichten nicht übermäßig beeinträchtigen. Die Mitwirkung ist angemessen zu entschädigen, wobei die Angemessenheit nicht auf Marktpreise referenziert, sondern auf eine grundsätzliche Kostendeckung abzielt, dabei aber auch lagebedingt die Sozialpflichtigkeit von Eigentum besonders berücksichtigen kann.

Zu Absatz 3

Zu Nummer 1

Die Nummer erweitert die Geeignetheit von Personen zu VP-Einsätzen. Ein Anwerben von Parlamentsmitgliedern oder deren Bediensteter bleibt aber weiter ausgeschlossen.

Zu Nummer 2

In der Lage des § 75 steht die effiziente Zielerreichung im Vordergrund, wohingegen Erwägungen subsidiärer sachlicher Zuständigkeit zurücktreten müssen. Da in solchen Fällen typischerweise eine wechselseitige Informationspflicht besteht, um für eine wirksame Gefahrenabwehr ein Gesamtbild der vorliegenden Informationen bei allen an der Phänomenaufklärung beteiligten Sicherheitsbehörden herzustellen, wird im Ergebnis die Grundrechtseingriffe nicht verbreitert. Gleichwohl bleibt bei den besonderen Maßnahmen des Vollzugriffs auf Privat-IT und der Wohnraumüberwachung im Lichte der Verfassungsrechtsprechung die Verfahrensvereinfachung auf den Verteidigungsfall beschränkt.

Der Effizienzvorrang gilt bei IT-Angriffen gemäß Satz 2 gleichermaßen für die Mittelauswahl zwischen Unternehmensauskunft und Selbstvornahme (Buchstabe a) und auch für die Sicherungskopie vor Löschung des vom Angreifer noch nicht vereinnahmten Beutegutes (Buchstabe b). Solche Kopie liegt grundsätzlich auch im fachlichen Interesse der Sachverhaltsauswertung, kann aber lagebedingt unter Umständen unpraktikabel sein, speziell wenn bei großen Datenmengen eine längerdauernde Verbindung nötig ist, die dem Angreifer zugleich die Ausforschung der BfV-infrastruktur eröffnet, oder bei groß angelegten Kampagnen eine Vielzahl von Vorgängen in kürzester Zeit zu bearbeiten sind.

Zu Nummer 3

Der Absatz eröffnet eine längere Anordnungsdauer. Die unabhängige Vorabkontrolle bleibt davon unberührt (dazu Absatz 8), kann im Rahmen ihrer Entscheidung bei Verhältnismäßigkeitsbedenken also die Maßgabe reduzierter Dauer treffen.

Zu Absatz 4

In der Lage bestehen besondere Anforderungen an Ausforschungssicherheit und operative Abschirmung ebenso wie die Notwendigkeit, eigene Ressourcen auf die operative Aufgabenwahrnehmung zu konzentrieren. Deshalb entfallen hier Mitteilungen und Auskünfte. Ein Ermessen – oder ein korrespondierender Anspruch auf Ermessenausübung – verbleibt angesichts übergeordneter Effizienzerfordernisse nicht.

Für Mitteilungen bei Intensiveingriffen der inhaltlichen Telekommunikationsüberwachung, des Vollzugriffs auf Privat-IT und der der Wohnraumüberwachung ist dies allerdings im Spannungsfall nicht angemessen, wenn dieser lediglich höchstens drei Monate besteht. In diesen Fällen erfolgt während des Spannungsfalls lediglich die Entlastung von der Mitteilungsprüfung und -bearbeitung, die insoweit für die Zeit nach dem Spannungsfall zurückgestellt wird.

Zu Absatz 5

Die Regelung dient der Entlastung von lagebedingt nachrangigen Verwaltungsaufwänden.

Zu Absatz 6

Die Regelung öffnet Übermittlungen im Rahmen der lagebezogenen Neugewichtung der veranlassenden Gemeinwohlbelange erweitert.

Zu Nummer 1

Die Nummer ermöglicht, besonders wichtige Rechtsgüter durch Informationsweitergabe für Vorsorgemaßnahmen wirksamer zu schützen.

Zu Nummer 2

Die Nummer ermöglicht die Übermittlung zur Strafverfolgung in allen Fällen, in denen tatsächliche Anhaltspunkte für eine Tat vorliegen, die der Durchführung oder Förderung von Bedrohungen diente. Diese Erweiterung ist im Spannungs- und Verteidigungsfall insbesondere deshalb geboten, weil solche Lagezuspitzung erwartbar mit einer Verschärfung hybrider Bedrohungen einhergeht, mit denen der Aggressor speziell auch gesellschaftliche Konflikte zu verschärfen sucht, um die Abwehrfähigkeit des Gemeinwesens zu schwächen. Dies geschieht in Formen direkter Einflussnahme, etwa durch „low level Agents“, die zu gesellschaftlichen Konfliktthemen Provokationen inszenieren, ebenso wie durch Nutzung extremistischer Resonanzböden, die mit aufhetzenden Narrativen und Desinformationen gespeist werden, um Radikalisierung zu befeuern und zu Aktionen gerade auch mit kriminellen Mitteln anzutreiben. Deshalb ist in solcher Situation existentieller Bedrohung des Gemeinwesens eine Rundumstärkung der Resilienz auch gegenüber Bestrebungen nötig, die gegen Bestand und Grundlagen des Gemeinwesens im Innern gerichtet sind. Dazu gehört auch, extremistische Straftaten konsequent zu verfolgen.

Zu Absatz 7

Die Regelung dient der Entlastung von lagebedingt nachrangigen Verwaltungsaufwänden. Unterstützungsleistungen zur Datenschutzkontrolle sind nur noch auf Anforderung des Parlamentarischen Kontrollgremiums nötig (Satz 1). Vorsichtungen auf Kernbereichsrelevanz (Satz 2) erfolgen durchweg nurmehr durch eine behördenintern unabhängige Stelle (nicht mehr extern durch den unabhängigen Kontrollrat) und nur dann, wenn konkret veranlasst (nicht mehr pauschal bei Wohnraumüberwachung).

Zu Absatz 8

Die Regelung ermöglicht eine zweistufige Reduktion der Ableitung von Operativressourcen in Kontrollverfahren. Mit Satz 1 ist allgemein dem Unabhängigen Kontrollrat eröffnet, seinerseits Verfahrenserleichterungen vorzusehen. Satz 2 eröffnet eine umfassende Entlastung durch einvernehmliche Entscheidung von Bundesregierung und Parlamentarischem Kontrollgremium, wie dies bereits in § 52 Absatz 2 Nummer 1 des MAD-Gesetzes in der Fassung des Gesetzes zur Stärkung der Militärischen Sicherheit in der Bundeswehr vorgesehen ist. Voraussetzung dafür ist, dass solcher prioritärer Ressourceneinsatz für die Operativaufgaben in der Sonderlage des Spannungs- bzw. Verteidigungsfalles zwingend ist.

Zu § 77 (Anwendung durch Landesbehörden für Verfassungsschutz)

Die Regelung erstreckt den Anwendungsbereich einzelner Bestimmungen auch auf den Landesvollzug. Damit wird das dazu geltende Recht des bisherigen Bundesverfassungsschutzgesetzes und Artikel 10-Gesetzes fortgeschrieben, aber in einer Regelung gebündelt. Die Regelungen des Abschnitts 1 – zur Zusammenarbeit der Verfassungsschutzbehörden – sind bereits dort an die LfV adressiert. Zur Relevanz der Begriffsbestimmungen trifft Absatz 3 eine Klarstellung.

Zu Absatz 1

Absatz 1 erstreckt benannte Vorschriften auch auf den Landesvollzug.

Zu Nummer 1

Die Regelung greift den bisherigen § 17 Absatz 2 zur Mitteilung über das Antreffen von Personen auch für die Länder allgemein auf, also ohne Beschränkung auf grenzpolizeiliche Mitteilungen. Die Verweisung bezieht lediglich § 10 Absatz 3 Satz 1 ein. Für Ausschreibungen in EU-Systemen (§ 10 Absatz 3 Satz 2) bleibt es wie im bisherigen § 17 Absatz 3 bei Ausschreibungen durch Nachrichtendienste des Bundes.

Zu Nummer 2

Die Regelung übernimmt die bisherige Geltung des Artikel 10-Gesetzes auch für den Landesvollzug. Die reine Verkehrsdatenauskunft wird – wie bisher – nicht bundesrechtlich zum Landesvollzug geregelt. Deshalb bezieht sich die Anwendungserstreckung auf die Datenerhebung über Inhalte. Bei solcher Datenerhebung kann dann allerdings auch die Erhebung der Verkehrsdaten (Umstände der Telekommunikation) einbezogen sein.

Der Bezug auf § 22 bezieht auch dessen Absatz 2 ein. Damit bleibt auch die sogenannte „Quellen-TKÜ“ (bisher: § 11 Absatz 1a G 10) bundesrechtlich auch für den Landesvollzug der LfV mit geregelt. Die materielle Schwelle bleibt dabei nach § 22 Absatz 2 Satz 6 in Verbindung mit § 26 Absatz 2 Nummer 1 – wie allgemein bereits nach § 22 Absatz 1 – die besonders erhebliche Beobachtungsbedürftigkeit. Zum Schutz des IT-Systems und der Eingriffsdokumentation sind nach § 22 Absatz 2 Satz 6 und 7 im Ergebnis die Vorgaben des § 23 Absatz 4 auch im Landesvollzug zu beachten.

§ 22 ist auf die Kommunikationsüberwachung (Absatz 2 Satz 1) ausgerichtet. Zugleich geregelt wird aber auch die Überwachung von nicht-kommunikativer Telekommunikation im Sinne von § 3 Nummer 59 TKG, also von Signalübertragung mittels TK-Anlagen. Hierfür gelten nach § 22 Absatz 2 Satz 2 die Voraussetzungen der §§ 23, 25 und 26. Dies gilt gleichermaßen für den Landesvollzug (ebenso wie die Verfahrensmaßgaben nach § 22 Absatz 2 Satz 3 bis 5).

Zu Nummer 3

Die Regelung übernimmt den bisherigen § 26a. Der Normzweck entsprechend sind auch die Ergänzungsnormen in §§ 52, 53, 59 anwendungsberufen. Geregelt sind lediglich Mindestübermittlungspflichten. Soweit Landesrecht weitergehende Übermittlungspflichten vorsieht, kollidiert dies nicht mit der bundesrechtlichen Regelung und bleibt von ihr unberührt. Ebenso bleiben etwaige weitergehende Übermittlungsbefugnisse des Landesrechts unberührt.

Zu Absatz 2

Absatz 3 entspricht der Regelung des Absatzes 1 Nummer 5 für den umgekehrten Weg der Übermittlung, hier von anderen Behörden an Verfassungsschutzbehörden.

Zu Absatz 3

Nach der Regelung gelten die Begriffsbestimmungen in § 3 Absätze 1 bis 3, die die Aufgabenregelung des § 2 Absatz 1 ergänzen, auch für die Aufgabendurchführung der Landesverfassungsschutzbehörden. Die weiteren Begriffsbestimmungen sind für den Landesvollzug dagegen nur insoweit maßgeblich, wie die erläuterten Bergriffe tatbestandlich in Vorschriften verwendet werden, die nach den Absätzen 1 und 2 im Landesvollzug anzuwenden sind.

Zu § 78 (Verordnungsermächtigung)

Die Verordnungsermächtigung greift die bisherigen Regelungen in § 2 Absatz 1b G10 (jetzt Nummer 1) und § 8b Absatz 8 (jetzt Nummern 2 und 3 auf). Die bisher in § 8b Absatz 8 Satz 2 Nummer 4 enthaltene Vorgabe zur Regelung der Zuständigkeit für die Entgegennahme der Daten ist nun in Nummer 2 Buchstabe c mit dem Zusatz der Adressierung aufgegriffen. Geregelt werden soll auch hier die Unternehmenspflicht, nicht eine Verwaltungszuständigkeit.

Die Entschädigung mitwirkungspflichtiger Unternehmen richtet sich künftig mit § 11 Absatz 7 einheitlich nach dem Justizvergütungs- und -entschädigungsgesetz, so dass dazu keine Verordnungsermächtigung mehr nötig ist.

Das durch die Verordnung näher ausgestaltete Gesetzesrecht liegt nicht im Landesvollzug. Näher geregelt werden Unternehmenspflichten zur Mitwirkung an Ermittlungen des BfV. Die Ermächtigung schließt nicht die Durchführung des § 77 ein.

Ermächtigungsadressaten sind auch Bundeskanzleramt und Verteidigungsministerium, da aufgrund entsprechender Ermächtungen im MAD-Gesetz und BND-Gesetz parallele Regelungen zu treffen sind, die aber, soweit sie sich gegenständlich entsprechen, inhaltlich synchron zu gestalten sind.

Die Bundesratszustimmung ist gemäß Artikel 80 Absatz 2 GG vorgesehen, da Teile des durch die Verordnung näher ausgestalteten Gesetzesrechts mittelbar über den Anwendungsbefehl in § 75 Absatz 1 Nummer 2 auch den Landesvollzug betreffen,

Zu § 79 (Einschränkung von Grundrechten)

Die Regelung entspricht dem bisherigen § 29.

Zu § 80 (Übergangsvorschriften)

Zu Absatz 1

Satz 1 legt fest, dass Anordnungen, die bereits vor Inkrafttreten des Gesetzes erfolgt und zu diesem Zeitpunkt noch nicht ausgelaufen sind, für die neue höchstzulässige Anordnungsdauer nach § 33 Absatz 4 Satz 1 durchgeführt werden dürfen. Diese Anpassung entlastet den Unabhängigen Kontrollrat von einer schwer zu bewältigenden Anfangslast einer zu hohen Zahl von Verlängerungsanordnungen, die erstmalig nach dem neuen Recht erfolgen. Zwar sind Verlängerungsanordnungen sind grundsätzlich mit weniger Prüfungsaufwänden als die erstmalige Grundanordnung verbunden, da der Grundsachverhalt bereits vorausgegangener Prüfung unterlag. Für den Unabhängigen Kontrollrat sind aber die nach Inkrafttreten erstmalig anfallenden Verlängerungen im Prüfungsaufwand faktisch Erstanordnungen gleichstehend, da er erstmalig damit befasst wird. Ist diese gesetzlich vorgesehene (einmalige) Befristung abgelaufen, kann eine Verlängerung nur nach der neuen Rechtslage erfolgen.

Zu Absatz 2

Zur praktikablen Umsetzung der neuen Prozesse des Anordnungs- und Vorabkontrollverfahrens ist eine Übergangsregelung angezeigt. Die Übergangsregelung ändert nichts am Inkrafttretenszeitpunkt speziell des § 34, d.h. es ist rechtlich möglich die Vorabkontrolle sogleich durchzuführen. Praktisch ist das aber nicht durchgängig realisierbar, weil sowohl die allgemeine Organisation (Aufbau entsprechender Kapazitäten, Definition behördeninterner Prozesse) wie auch die einzelne Anordnung einen Bearbeitungsvorlauf erfordert. Die Übergangsvorschrift eröffnet dazu ein gleitendes Einphasen ab Inkrafttreten des Gesetzes und bereits vor Ablauf der Übergangsfrist, das infolge ebenso zur zeitlichen Entzerrung der Verfahren-saufwände bei Verlängerungsanordnungen führt.

Hiervon ausgenommen sind Maßnahmen, die den in § 34 Absatz 1 Satz 1 Nummer 6, 9 und Absatz 4 genannten Maßnahmen entsprechen. Zur Beschränkung des Telekommunikationsgeheimnisses und zur Wohnraumüberwachung galten bereits vor Inkrafttreten des Gesetzes besondere gesetzliche Verfahrensanforderungen, einschließlich unabhängiger Vorabkontrolle, die nicht übergangsweise entfallen, sondern sogleich in das neue System transferiert werden sollen. Mit der Befugnis zur Online-Überwachung wird eine neue Maßnahme von einem Eingriffsgewicht eingeführt, das auch nicht übergangsweise mindere Verfahrensanforderungen duldet. Die Ausnahmeregelung ist also eine gewichtende Priorisierung in der Einführung der neuen Verfahren.

Zu Absatz 3

Der Absatz bezieht die Betroffenenmitteilung als Element des neuen Prozesses in die gleitende Prozessetablierung ein, ohne allerdings dabei bereits bisherige Mitteilungspflichten übergangsweise entfallen zu lassen.

Zu Absatz 4

Absatz 3 sieht den Neuerlass der Dienstvorschrift über nachrichtendienstlichen Mittel vor, was die Zustimmungs- und Unterrichtungserfordernisse nach § 16 Absatz 4 zur Folge hat. Die in § 16 Absatz 4 Satz 2 eröffnete Erprobungsoption soll eine Offenheit lediglich für künftige Entwicklungen schaffen. Dies gewährleistet § 79 Absatz 4. Ergibt sich erst durch nachträgliche technische Entwicklungen qualifiziertes Eingriffsgewicht eines Mittels, das zuvor der Art nach nur einfach eingreifend war, dann fällt die Erprobung dieser neuen technischen Optionen als neue qualifizierte Standardmaßnahme ebenso unter die Erprobungsvorschrift, das Mittel ist in dieser Qualität neu.

Zu Absatz 5

Der Absatz enthält eine Übergangsregelung für die Ablösung der bisherigen Anwendung des Artikel 10-Gesetzes durch die Länder durch die neue Regelung in § 77 Absatz 1 Nummer 2. In den Ländern besteht Ausführungsgesetzgebung zur landesseitigen Anwendung des Artikel 10-Gesetzes mit Regelungen zur unabhängigen Vorabkontrolle, die womöglich nicht unmittelbar auf die künftige Durchführung des § 77 Absatz 1 Nummer 2 anwendbar ist. Um einerseits keine kontrollfreie Anwendungspraxis zu eröffnen und andererseits den Ländern die Anpassung ihres Durchführungsrechts zu ermöglichen, enthält der Absatz die Möglichkeit, übergangsweise im Land das Artikel 10-Gesetz weiter anzuwenden. Bis Ende 2029 muss die Rechtsanpassung aber erfolgt sein.

Zu Artikel 2 (Gesetz über den Bundesnachrichtendienst)

Artikel 2 enthält das neugefasste Stammgesetz für den Bundesnachrichtendienst.

Zu Abschnitt 1 (Aufgaben, allgemeine Befugnisse und Vorgaben)

Zu § 1 (Bundesnachrichtendienst)

In § 1 Absatz 1 wird erstmals eine allgemeine Beschreibung der Rolle des Bundesnachrichtendienstes innerhalb der Behördenlandschaft aufgenommen, dies insbesondere in Bezug auf die sicherheitsbehördliche Architektur der Bundesrepublik Deutschland.

Die Regelung spiegelt (das bisher geltende Verständnis auch) auf gesetzlicher Ebene wider, dass der Bundesnachrichtendienst – als zivile Bundesoberbehörde, vgl. Absatz 2 – der Auslandsnachrichtendienst der Bundesrepublik Deutschland ist.

In seiner Rolle als Auslandsnachrichtendienst sammelt der Bundesnachrichtendienst zur Gewinnung von Erkenntnissen über das Ausland, die von außen- oder sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen und wertet sie aus (vgl. hierzu § 2). Er ist der alleinige Auslandsnachrichtendienst der

Bundesrepublik Deutschland und dabei auch mit der militärischen Auslandsaufklärung betraut (vgl. etwa BT-Drs. 20/14594: „Der BND ist […] der auch mit der militärischen Auslandsaufklärung beauftragte Auslandsnachrichtendienst der Bundesrepublik Deutschland…“).

§ 1 Absatz 2 entspricht dem bisherigen § 1 Absatz 1. Die in Satz 2 enthaltene Maßgabe, dass der Bundesnachrichtendienst einer polizeilichen Dienststelle nicht angegliedert werden darf, ergibt sich bereits aus Absatz 2 Satz 1 und hat keinen zusätzlichen Regelungsgehalt: Eine Angliederung wäre schon deshalb nicht möglich, weil der Bundesnachrichtendienst dem Bundeskanzleramt nachgeordnet ist. Anders als das Bundesministerium des Innern hat das Bundeskanzleramt keine nachgeordneten Polizeibehörden, sodass eine Angliederung ohnehin ausgeschlossen ist. Da Satz 2 indes auch als einfachgesetzliche Normierung eines „organisatorischen Trennungsgebotes“ verstanden wird, wurde die – sprachlich etwas zu einseitige – Vorschrift gleichwohl erneut fortgeschrieben.

Zu § 2 (Aufgabe)

§ 2 beinhaltet die Aufgabenzuweisung des Bundesnachrichtendienstes.

Die (Primär-)Aufgabe des Bundesnachrichtendienstes ist die nachrichtendienstliche Auslandsaufklärung, um die Bundesregierung mit Entscheidungsgrundlagen zur Sicherung ihrer außen- oder sicherheitspolitischen Handlungsfähigkeit zu versorgen (vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 128). Dies meint im Grundsatz, dass es dem Bundesnachrichtendienst obliegt, Vorgänge im Ausland zu einem breiten und variablen Themenspektrum zu beobachten, dessen Eingrenzung grundsätzlich (nur) durch einen spezifischen Auslandsbezug und eine qualifizierte außen- oder sicherheitspolitischen Dimension angelegt ist. Diese qualifizierte außen- oder sicherheitspolitische Dimension setzt voraus, dass sich die Aufklärung auf eine Bedrohung für besonders gewichtige Rechtsgüter (einschließlich der außenpolitischen Handlungsfähigkeit der Bundesrepublik Deutschland, die auch durch Unkenntnis über politische oder wirtschaftliche Ereignisse und Entwicklungen in aufklärungsbedürftigen Staaten bedroht sein kann) bezieht. Der Bundesnachrichtendienst ist dergestalt eine Sicherheitsbehörde. Neben der Erfüllung dieser „Primäraufgabe“ dient die nachrichtendienstliche Auslandsaufklärung aber auch weiteren, in der Diktion des Bundesverfassungsgerichts, „Sekundäraufgaben“. Hierunter fallen insbesondere die Gefahrenfrüherkennung (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 128) und die Aufklärung von Straftaten mit „internationaler Dimension“ (BVerfG, Urteil vom 14. Juli 1999, 1 BvR 2226/94 u.a., Rn. 201ff.).

Die Aufklärungstätigkeit des Bundesnachrichtendienstes dient insgesamt dem Schutz besonders gewichtiger Rechtsgüter vor Bedrohungen (zu der rechtssystematischen Einordnung bereits oben). Die Aufklärung einer Bedrohung ist aber kein Selbstzweck, sondern dient der Begegnung dieser Bedrohung. Hierfür ist eine entsprechende Information staatlicher und nichtstaatlicher Stellen über erkannte Bedrohungen essentieller Bestandteil der Aufgabe des Bundesnachrichtendienstes. Die Informationsweitergabe unterfällt damit als logische Folge der Aufklärungstätigkeit ebenfalls der Aufgabe des Bundesnachrichtendienstes. Sämtliche Akteure sowie auch die Öffentlichkeit, für die außen- oder sicherheitspolitische Informationen von Bedeutung sind, sind geeignete Informationsadressaten für Erkenntnisse des Bundesnachrichtendienstes. Dies betrifft einerseits „klassische“ Empfänger nachrichtendienstlicher Informationen wie politische Entscheidungsträger oder öffentliche Stellen, insbesondere solche, die betraut sind mit der Strafverfolgung oder der Gefahrenabwehr (der Bundesnachrichtendienst ist insoweit bereits in seiner regelmäßigen Tätigkeit mit der informationellen Gefahrenabwehr betraut). Darüber hinaus sind indes auch weitere Akteure notwendige Informationsadressaten. Dies beinhaltet etwa die Öffentlichkeit (vgl. § 69) oder individuelle Adressaten wie z.B. die Opfer von Cyberangriffen oder Wirtschaftsunternehmen, wenn diese über Bedrohungen informiert oder sensibilisiert werden müssen.

Die nähere einfachgesetzliche Definition der (sicherheitsbehördlichen) Aufgabe einer nachrichtendienstlichen Auslandsaufklärung ist in Absatz 1 Satz 2 enthalten und beinhaltet die Sammlung und Auswertung aller Informationen, die Auswirkungen auf die Sicherheit der Bundesrepublik Deutschland oder deren Beziehungen zu anderen Staaten haben können. Die Erfüllung dieser Aufgabe ist von überragendem öffentlichem Interesse (vgl.: BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 161ff.). Dabei verdeutlichen die verfassungsgerichtlichen Maßgaben, dass die Tätigkeit des Bundesnachrichtendienstes – auch soweit sie der „Versorgung der Bundesregierung mit Informationen für ihre außen- und sicherheitspolitischen Entscheidungen [dient, um] sich im machtpolitischen Kräftefeld der internationalen Beziehungen zu behaupten, und (…) folgenreiche Fehlentscheidungen [zu] verhindern (vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 162) – nicht losgelöst von einem Schutz besonders gewichtiger Rechtsgüter erfolgt. Auch insoweit ist verfassungsgerichtlich bestätigt, dass es „mittelbar zugleich um die Bewahrung demokratischer Selbstbestimmung und den Schutz der verfassungsrechtlichen Ordnung“ (BVerfG, a.a.O.) geht.

Die (neue) gesetzliche Systematik greift dies auf: Der Schutz eines Rechtsgutes setzt begrifflich voraus, dass ein schädigendes Ereignis oder Bestreben droht, vor dem das Rechtsgut geschützt werden muss. Im polizeirechtlichen Kontext ist dies eine „Gefahr“ – im nachrichtendienstlichen Kontext wird demgegenüber – auch um zum Ausdruck zu bringen, dass die Nachrichtendienste gerade weit im Vorfeld einer Gefahr aufklären – stattdessen der Begriff der „Bedrohung“ verwandt. Durch diese „Konsolidierung“ des Auftrags des Bundesnachrichtendienstes auf die Früherkennung von Bedrohungen wird zugleich die (seit dem verfassungsgerichtlichen Urteil vom 19. Mai 2020, 1 BvR 2835/17 angelegte) künstliche Trennung zwischen „politischer Unterrichtung“ und „Gefahrenfrüherkennung“ (vgl. etwa § 19 im bisherigen Recht) aufgelöst.

Zu Absatz 1

§ 2 Absatz 1 weist dem Bundesnachrichtendienst seinen Aufklärungsauftrag zu und definiert den Begriff der „nachrichtendienstlichen Auslandsaufklärung“.

Wie im geltenden Recht bereits als Aufgabe normiert, sammelt der Bundesnachrichtendienst Informationen, die von außen- oder sicherheitspolitischer Bedeutung sind und wertet diese aus. Der bisherigen Auslegung folgend wird im BND-Gesetz nun nicht mehr außen-*und* sicherheitspolitische Bedeutung formuliert. Stattdessen wird insofern sprachlich das bisherige Verständnis in der Formulierung nachgezogen, vgl. Schenke/Graulich/Ruthig; Sicherheitsrecht des Bundes, 2. Auflage, Rn. 34: „[Der nachrichtendienstliche Auftrag] umfasst die Gesamtheit derjenigen Handlungen, Zustände und Absichten, welche aktuelle oder spätere Erkenntnisse außen- oder sicherheitspolitischer Relevanz als möglich erscheinen lassen.“] Damit ist nun gesetzlich klargestellt, dass auch solche Vorgänge dem Aufklärungsauftrag unterfallen, welche prima facie allein außenpolitischer Bedeutung haben (wenngleich es sich insoweit systematisch auch um die Früherkennung von Bedrohungen für die außenpolitische Handlungsfähigkeit handelt). Hierzu zählen beispielsweise Wahlgeschehen in Nicht-Krisenstaaten und deren Auswirkungen auf andere Staaten, Staatengemeinschaften oder Bündnisse, Reformen im Ausland ohne konkreten Sicherheitsbezug, Kabinettsumbildungen etc. Der Bundesnachrichtendienst soll damit auch aussagefähig sein zu humanitären Lagen in anderen Staaten, die keine offensichtliche sicherheitspolitische Bedeutung erreichen, sowie in Fragen im Bereich des Wirtschaftsschutzes. Von sicherheitspolitischer Bedeutung sind – korrespondierend zu der Funktion des Bundesnachrichtendienstes als auch militärischer Auslandsnachrichtendienst der Bundesrepublik Deutschland – zugleich die für die Aufgabenerfüllung der Bundeswehr bedeutsame Informationen. Die Aufklärung rein innerdeutscher Sachverhalte wird hingegen nicht von der Aufgabe des Bundesnachrichtendienstes erfasst, da es hier bereits keinen Bezug zu „Erkenntnissen über das Ausland“ gibt.

Ziel des Aufklärungsauftrags des Bundesnachrichtendienstes ist die Früherkennung von Bedrohungen für besonders gewichtige Rechtsgüter (BVerfG, Urteil vom 26. April 2022,

1 BvR 1619/17, Rn. 241, m.w.N. sowie BVerfG, Beschluss vom 29. September 2022, 1 BvR 2354/13, Rn. 127f.). Dabei ist nicht erforderlich, dass für einzelne Aufklärungsmaßnahmen oder -sachverhalte bereits eine unmittelbare Bedrohung faktisch gegeben ist. Entsprechend sieht das Gesetz vor, dass die aufklärende Tätigkeit des Bundesnachrichtendienstes gerade der Früherkennung von Bedrohungen gegen die genannten Rechtsgüter dient, was auch bei Aufklärungen und Informationssammlungen im Vorfeld einer Bedrohung gegeben ist. So werden durch den Bundesnachrichtendienst auch langfristige und unbestimmte Entwicklungen in den Blick genommen, aus denen erst im weiteren Verlauf Bedrohungen gegen die geschützten Rechtsgüter erwachsen können – für die Früherkennung ist es gerade geboten den „status quo“ zu betrachten, um das Entstehen einer Bedrohung erkennen zu können. Bei den oben genannten Beispielen „Wahlgeschehen in Nicht-Krisenstaaten und deren Auswirkungen auf andere Staaten, Staatengemeinschaften oder Bündnisse, Reformen im Ausland ohne konkreten Sicherheitsbezug, Kabinettsumbildungen etc.“ ist dabei eine Bedrohung (oder gar eine spezifische Gefährdung) – hier z.B. des Rechtsgutes der außenpolitischen Handlungsfähigkeit der Bundesrepublik – nicht schon akut oder auch nur konkret absehbar. Gleichwohl dient, da die Aufgabe des Bundesnachrichtendienstes gerade auf die Vorfeldaufklärung gerichtet ist, auch diese Aufklärungstätigkeit mittelbar dem Schutz der außenpolitischen Handlungsfähigkeit, da die Bundesregierung durch Informationen des Bundesnachrichtendienstes befähigt werden muss, auf politische Veränderungen in anderen Staaten frühzeitig oder kurzfristig zu reagieren, diese Veränderungen im globalen Kontext einordnen zu können und insoweit insgesamt handlungsfähig zu sein. Allen Bedrohungen gemein ist dabei, dass sie bei verständiger Würdigung ex ante zumindest theoretisch geeignet sein müssen, ihre jeweiligen Ziele zu erreichen. Eine völlig dilettantische Vorgehensweise ohne jedwede Aussicht auf Erfolg (z.B. durch das Vertrauen auf übernatürliche Kräfte) begründet keine besondere Aufklärungsbedürftigkeit. Dies gilt freilich nur, sofern nicht Mittel eingesetzt werden, welche eine besondere Bedrohungslage begründen (z.B. Waffen o.ä.).

Rechtssystematisch handelt es sich bei Absatz 1 Satz 2 um die Festschreibung des im Rahmen der oben genannten Rechtsprechung des Bundesverfassungsgerichts ausgeführten Umstandes, dass die Tätigkeit der Nachrichtendienste des Bundes grundsätzlich dem Schutz besonders gewichtiger Rechtsgüter dient. Die Auslandsaufklärung zielt immer auf Informationen von außen- oder sicherheitspolitischer Bedeutung und damit geht es mittelbar zugleich um den Schutz besonders gewichtiger Rechtsgüter (vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 162).

Satz 3 ist klarstellend. Der in Satz 1 enthaltene Auftrag des Bundesnachrichtendienstes schließt auch diejenigen Tätigkeiten mit ein, die als „Annex“ denknotwendigerweise mitumfasst sein müssen, damit der Bundesnachrichtendienst seine Aufgabe erfüllen kann. So muss es dem Bundesnachrichtendienst zur Aufgabenerfüllung selbstverständlich auch ermöglicht werden, Liegenschaften anzumieten, Mitarbeiter einzustellen oder sein Kantinenwesen zu betreiben. Eine Ermächtigungsgrundlage für diese Tätigkeiten bedarf es – schon mangels einer Grundrechtsrelevanz – nicht.

Über diese allgemeinen Tätigkeiten hinaus entstammt dem besonderen Auftrag des Bundesnachrichtendienstes indes auch eine „besondere“ (da sie von besonderer Wichtigkeit sind – ihre Herleitung und entsprechend auch die klarstellende Funktion der Vorschrift ist dabei unverändert) Annexaufgabe. Dies sind die in Satz 3 explizit genannten Tätigkeiten, welche die Auslandsaufklärung begleiten, ihr vorausgehen oder nachgelagert sind, wenn sie zur „Eigensicherung“ erforderlich sind. Diese Tätigkeiten sind nicht nur in besonderem Maße notwendig, damit der Bundesnachrichtendienst die ihm zugewiesenen Aufgabe der Auslandsaufklärung wirksam durchführen kann. Die Regelung des Satzes 3 ist auch deshalb erforderlich, weil die hieraus abgeleiteten konkreten einzelnen Maßnahmen nicht zwingend und unmittelbar auf die Auslandsaufklärung ausgerichtet sind; da es sich hierbei indes um die Grundstufe nachrichtendienstlicher Befugnisse handelt, stellt die Regelung in Satz 3 sicher, dass diese Befugnisse auch dann zum Einsatz kommen können, wenn sie zum Zwecke der Eigensicherung erfolgen. Zuletzt können auch diese Maßnahmen prinzipiell

eine grundrechtliche Relevanz zeitigen, sodass eine gesetzliche Regelung auch aufgrund der Wesentlichkeitstheorie erforderlich ist.

Erfasst sind solche Tätigkeiten, die der Bundesnachrichtendienst zur Sicherung seiner Liegenschaften, Mitarbeitenden wie auch der sonstigen Personen, die für ihn tätig sind, etwa die nachrichtendienstlichen Verbindungen, Methoden, Gegenstände und geheimhaltungsbedürftigen Informationen ergreifen muss, um unbefugten Informationsabfluss zu verhindern, die genannten Personen zu schützen und allgemein gegen ihn gerichtete, sicherheitsgefährdende oder nachrichtendienstliche Tätigkeiten zu unterbinden. Hierzu wird der Bundesnachrichtendienst praktisch gehalten sein, durch geeignete – bei Wahrung der jeweiligen Eingriffsvoraussetzungen auch durch nachrichtendienstliche – Maßnahmen den eigenen Geschäftsbereich aufzuklären. Regelmäßig wird es sich bei Bedrohungen in diesem Zusammenhang zugleich um Bedrohungen von herausgehobener Bedeutung handeln.

Sonstige partielle Aufgabenzuweisungen wie z.B. im Rahmen von Abschnitt 4 oder in anderen Gesetzen (z.B. dem Sanktionsdurchsetzungsgesetz) bleiben unberührt.

Satz 1 und 2 statuieren zugleich rechtssystematisch auch die tatbestandliche „Grundstufe“ der nachrichtendienstlichen Tätigkeit. Die nachrichtendienstliche Auslandsaufklärung begründet dergestalt die Erhebungsschwelle für den (im Regelfall noch wenig eingriffsintensiven) Einsatz von Maßnahmen zur Informationsgewinnung. Auch der Einsatz der nachrichtendienstlichen Mittel auf dieser „Grundstufe“ dient dabei dem Schutz besonders gewichtiger Rechtsgüter vor Bedrohungen, unabhängig davon, ob diese Bedrohungen schon manifest sind. In den nachfolgenden Vorschriften finden sich sodann die „Qualifikationsstufen“ (als erste Qualifikationsstufe die erheblichen Bedrohungen und als zweite Qualifikationsstufe die Bedrohungen von herausgehobener Bedeutung), welche auch den Einsatz eingriffsintensiverer nachrichtendienstlicher Mittel rechtfertigen - darauf weist Satz 3 hin. Dabei gilt, dass das Vorliegen der ersten Qualifikationsstufe immer auch den Einsatz von nachrichtendienstlichen Mitteln der Grundstufe und das Vorliegen der zweiten Qualifikationsstufe immer auch den Einsatz von nachrichtendienstlichen Mitteln der ersten Qualifikationsstufe sowie der Grundstufe rechtfertigt. Dies wird in der Regelungssystematik des Gesetzes dadurch zum Ausdruck gebracht, dass die tatbestandliche Schwelle der Erhebungsbefugnisse eine Erforderlichkeit „zumindest“ für die Grundstufe bzw. die erste Qualifikationsstufe voraussetzt.

Aus Satz 2 ergibt sich zuletzt auch das Verhältnis von Informationen und Erkenntnissen: Informationen sind die einzelnen erlangten Daten, Erkenntnisse sind typischerweise Auswerteprodukte, bei denen erlangte Informationen in der Regel durch den Bundesnachrichtendienst angereichert und bestätigt bzw. bewertet wurden.

Zur Konkretisierung der Aufgabe des Bundesnachrichtendienstes, Bedrohungen gegen die Rechtsgüter im Sinne des Absatzes 2 möglichst frühzeitig zu erkennen und aufzuklären, wird nachfolgend in den §§ 3 und 4 ein (gestuftes) System der Bedrohungen ausformuliert, die typischerweise eine Gefährdung dieser besonders gewichtigen Rechtsgüter indizieren. Eine Einzelzuordnung einzelner Bedrohungen zu einzelnen Rechtsgütern erfolgt nicht. Sie kann auch nicht erfolgen, da eine Zuordnung stets vom konkret aufzuklärenden Vorgang oder von der konkret aufzuklärenden Fallkonstellation abhängig ist, ggf. in seinen bzw. ihren einzelnen Facetten auch mehreren Rechtsgütern zugleich zuzuordnen sein kann. Vielmehr dient die besondere Aufgabe der nachrichtendienstlichen Tätigkeit der Auslandsaufklärung in ihrer Gesamtheit dem Schutz der (qualitativ auf einer Stufe stehenden) besonders gewichtigen Rechtsgüter im Sinne des Absatzes 2 in ihrer außen- oder sicherheitspolitischen Dimension. Die Aufklärungstätigkeit des Bundesnachrichtendienstes zur Erfüllung seines gesetzlichen Auftrags ist als Erfüllung einer einheitlichen Aufgabe zum Schutz dieser Rechtsgüter zu verstehen. Vgl. dazu die mit Blick auf die Verfassungsschutzaufgaben ergangene, aber auch auf die nachrichtendienstliche Tätigkeit des Bundesnachrichtendienstes übertragbare, geltende Rechtsprechung des Bundesverfassungsgerichts vom

26. April 2022, 1 BvR 1619/17, Rn. 241 (m.w.N.) sowie vom 29. September 2022, 1 BvR 2354/13, Rn. 127f.

In Satz 4 wird auf die in den §§ 3 und 4 geregelten „Qualifikationsstufen“ der Bedrohungen für besonders gewichtige Rechtsgüter, deren Früherkennung die nachrichtendienstliche Auslandsaufklärung zum Ziel hat, verwiesen. Diese Bedrohungen gegen besonders gewichtige Rechtsgüter, namentlich die „erheblichen Bedrohungen“ (§ 3) und „Bedrohungen von herausgehobener Bedeutung“ (§ 4) bilden die materiellen Schwellen für die Durchführung eingriffsintensiver Maßnahmen durch den Bundesnachrichtendienst.

Diese Qualifikationsstufen sind Teil der in diesem Gesetz eingeführten Stufensystematik, die sicherstellt, dass die in den jeweiligen Befugnisnormen festgelegten materiellen Schwellen mit den eingriffsrechtfertigenden Gemeinwohlinteressen in einem verfassungskonformen Verhältnis zueinander stehen. Mittels diese Stufensystems (Grundstufe der nachrichtendienstlichen Auslandsaufklärung (§ 2 Absatz 1) – erhebliche Bedrohungen (§ 3) – Bedrohungen von herausgehobener Bedeutung (§ 4)) wird ein normenklares und kohärentes Verhältnismäßigkeitssystem gebildet, dass den Anforderungen an die Verhältnismäßigkeit nachrichtendienstlicher Maßnahmen gerecht wird, indem es eingriffsintensive Maßnahmen nur beim Vorliegen erheblicher Bedrohungen oder Bedrohungen von herausgehobener Bedeutung zulässt.

Die Qualifikationsstufen enthalten die Ausformulierung von Bedrohungen, die durch den Bundesnachrichtendienst zur Erfüllung seines Aufklärungsauftrages zum Schutz des Gemeinwohlinteresses typischerweise aufzuklären sind. Die Beurteilung der Bedrohungspotenzialität von Aufklärungszielen wird durch diese Vorschriften gesteuert. Die mit Hilfe der Bedrohungen dargestellten Vorgänge/ Konstellationen sind unterschiedlich gefährlich. In der Regel am stärksten gefährdet sind die bedrohten Rechtsgüter in den Konstellationen der Bedrohungen mit herausgehobener Bedeutung (Zweite Qualifikationsstufe). Durch die erheblichen Bedrohungen (Erste Qualifikationsstufe) werden die Rechtsgüter typischerweise stärker gefährdet als in den Grundkonstellationen der nachrichtendienstlichen Auslandsaufklärung (Grundstufe der nachrichtendienstlichen Aufklärung, jenseits der Katalogs der Bedrohungen erheblicher oder herausgehobener Art wie beispielsweise die Sammlung von Informationen zu Wahlen / Wahltendenzen / Entwicklungen in einem ausländischen Staat, ohne dass damit bereits eine erhebliche oder herausgehobene Bedrohung verbunden ist). Der Gesetzentwurf gewichtet also das Gemeinwohlinteresse an der Aufklärungsaufgabe des Bundesnachrichtendienstes abstufend und schafft so unterschiedliche materielle Schwellen für den Einsatz nachrichtendienstlicher Mittel. Nur die Bedrohungen des § 3 (Erste Qualifikationsstufe: erhebliche Bedrohungen) und diejenige des (§ 4 (Zweite Qualifikationsstufe: Bedrohungen von herausgehobener Bedeutung) rechtfertigen dabei eingriffsintensive nachrichtendienstliche Maßnahmen.

Es handelt sich hierbei um nicht schematisch abschließende Kategorien einer erhöhten Bedrohungspotenzialität. So schreibt die gesetzliche Regelung in ihrer Funktion als Qualifikationsstufe nicht bereits normativ eine unwiderlegbare Vermutung für eine erhöhte Aufklärungsbedürftigkeit fest, ohne dass es einer weiteren Prüfung der Potentialität des Aufklärungsziels im Einzelfall bedürfte. Auch muss gerade bei der Auslandsaufklärung des Bundesnachrichtendienstes eine schnelle Reaktionsmöglichkeit auf globale Entwicklungen gewahrt werden; dem trägt die Regelung in ihrer Ausformung als Indizienkatalog Rechnung.

Aufzuklärende Sachverhalte können also grundsätzlich als Fallkonstellationen der Grundstufe, der ersten oder der zweiten Qualifikationsstufe auftreten. Es hat daher jeweils eine Bewertung der aufzuklärenden Thematik bzw. des Sachverhalts anhand der gesetzlich festgelegten Merkmale (*besondere Beeinträchtigung* für die Annahme des § 3 - „erhebliche Bedrohung“; *erhöhtes Gefährdungspotenzial* für die Annahme des § 4 - „Bedrohung von herausgehobener Bedeutung“) zum Zweck der Einordnung in das Stufensystem zu erfolgen.

Die bisherige Regelung in § 1 Absatz 2 Satz 2 entfällt. Um seinen Aufklärungsauftrag zu erfüllen wird der Bundesnachrichtendienst im Bundesgebiet wie auch im Ausland tätig. Das BND-Gesetz enthält nunmehr normenklare Regelungen mit Blick auf die Tätigkeit des Bundesnachrichtendienstes gegenüber Personen mit deutscher Staatsangehörigkeit, Personen, die sich im Bundesgebiet aufhalten, juristischen Personen und Personen, die nicht in einer vergleichbaren Nähebeziehung zur deutschen Staatsgewalt stehen (Ausländerinnen und Ausländer im Ausland). Für die nachrichtendienstliche Tätigkeit gelten abhängig von der durch die Maßnahme betroffenen Person nach der Rechtsprechung des Bundesverfassungsgerichts differenzierte Maßstäbe; dies wird in den Regelungen im BND-Gesetz nunmehr normenklar berücksichtigt. Vgl. dazu BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 186, wonach eine nachrichtendienstliche Maßnahme gegenüber einer Ausländerin oder einem Ausländer im Ausland ein geringeres Eingriffsgewicht aufweisen kann, da diese Personengruppe typischerweise nicht dem Zugriff weiterer deutscher Behörden unterliegt und ist damit in deutlich verringertem Ausmaß Folgemaßnahmen ausgesetzt ist. Die nachrichtendienstliche Auslandsaufklärung betrifft vor allem Vorgänge in anderen Ländern, in denen der deutsche Staat nicht über Hoheitsbefugnisse verfügt, siehe dazu auch BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 161: „Zudem erfolgt die Aufklärung von Vorgängen in anderen Ländern unter besonderen Handlungsbedingungen, weil der deutsche Staat allenfalls punktuell mit eigenen Erkenntnisquellen präsent ist und nicht über Hoheitsbefugnisse verfügt, die ihm einen unmittelbaren Zugriff auf Informationen ermöglichten. Erst dies rechtfertigt dort den Verzicht auf konkretisierende Eingriffsschwellen.“ Das Bundesverfassungsgericht hebt hervor, dass es bei der Frage der Ausgestaltung angemessener Schwellen auch auf die potentiellen Folgen der Maßnahmen für die Betroffenen ankommt. Hierzu auch BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 157: „Das Eingriffsgewicht wird generell durch die denkbare Verwendung der Daten mitbestimmt.“. Wird der Bundesnachrichtendienst gegenüber Ausländerinnen und Ausländern im Ausland tätig und sammelt Informationen über diese, sind im Ausland regelmäßig operative Anschlussmaßnahmen durch deutsche Stellen ausgeschlossen, so dass die Folgen für betroffene Personen im Ausland durch mögliche Folgemaßnahmen typischerweise gering sind.

Zu Absatz 2

Zu der in Absatz 2 getroffenen Einordnung von Rechtsgütern als besonders gewichtig lassen sich aus der jüngeren Rechtsprechung des Bundesverfassungsgerichts zum Sicherheitsrecht Anhaltspunkte für eine solche – verfassungsrechtlich angeleitete – Systematisierung von Rechtsgütern entnehmen. So zählt das Bundesverfassungsgericht in mittlerweile gefestigter Rechtsprechung zum Kreis der „besonders gewichtigen Rechtsgüter“, den Bestand und die Sicherheit des Staates, Leib, Leben und Freiheit der Person sowie Einrichtungen der Kritischen Infrastruktur (vgl. etwa BVerfGE°30,°1,°18;°120,°274,°328; 133,°277,°365; 141,°220,°296; 154,°152,°269; 156,°11,°55; BVerfG, Urteil vom 26.°April 2022, 1 BvR 1619/17, Rn. 236,°243,°254f.; BVerfG, Beschluss vom 9.°Dezember 2022, 1 BvR 1345/21, Rn. 179; BVerfG, Urteil vom 16.°Februar 2023, 1 BvR 1547/19, Rn. 105). In seiner Entscheidung vom 26.°April 2022 (1 BvR 1619/17, Rn. 243) hält das Bundesverfassungsgericht zum „besonders gewichtigen Rechtsgut“ fest, dass besonders gewichtige Rechtsgüter Leib, Leben und Freiheit der Person sowie der Bestand oder die Sicherheit des Bundes oder eines Landes sind. Darüber hinaus kann auch der Schutz von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, zu diesem Kreis gezählt werden.

Eine abschließende Benennung der besonders gewichtigen Rechtsgüter ist mit dieser Rechtsprechung nicht verbunden und wäre dogmatisch auch nicht begründbar, da der Bestand an Rechtsgütern des einfachen Rechts und des Verfassungsrechts durch den einfachen bzw. verfassungsändernden Gesetzgeber verändert werden kann. Das hervorgehobene Gewicht der besonders gewichtigen Rechtsgüter beruht auf deren existenzsichernder Bedeutung für die Gemeinschaft und den Einzelnen. Besonders gewichtigen Rechtsgütern

kommt daher für den Erhalt der Existenz von natürlichen Personen und Subjekten des Völkerrechts eine systemische Bedeutung zu.

Diese Bedeutung wird in den Nummern°1 bis°6 (bisher ähnlich in § 11b Absatz 1) für den Tätigkeitsbereich des Bundesnachrichtendienstes konturiert. Die Rechtsgüter im Sinne des Absatz 2 sind besonders gewichtig, da ihre Verletzung regelmäßig schwere Schäden für den äußeren und inneren Frieden oder der Rechtsgüter Einzelner bzw. hochrangiger Gemeinschaftsgüter zur Folge hätte (vgl. dazu auch BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 176). Die Rechtsgüter, deren Schutz die Tätigkeit des Bundesnachrichtendienstes dient, sind besonders hochrangig und von hohem verfassungsrechtlichem Gewicht (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 150, 174).

In der Rechtsprechung werden derartige Rechtsgüter teilweise als „überragend wichtige“, „(besonders) hochrangige“, „Rechtsgüter von herausragendem öffentlichem Interesse bzw. Gewicht“ oder „besonders gewichtig“ bezeichnet. So werden z.B. die Rechtsgüter „Leib, Leben oder Freiheit der Person“ in den Entscheidungen mal als „überragend wichtige“ (vgl. BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 243) mal als „besonders gewichtige Rechtsgüter“ (BVerfG, Urteil vom 20 April 2016, 1 BvR 966/09 und 1140/09, Rn. 108) bezeichnet.

Im Sinne der Normenklarheit wird im BND-Gesetz einheitlich der Begriff der *besonders gewichtigen* Rechtsgüter verwendet.

Im Vergleich zur bisherigen Aufzählung in § 11b Absatz 1 ist die Aufzählung nunmehr etwas weniger ausdifferenziert gewählt, so dass hier einzelne im Rechtsgüterkatalog des bisherigen § 11b Absatz 1 aufgezählten Rechtsgüter als Unterfälle der hier gewählten grundlegenden Rechtsgüter miterfasst und nicht mehr einzeln aufgeführt werden. Zu den in dieser Neufassung im Vergleich zum bisher in § 11b Absatz 1 enthaltenen Rechtsgüterkatalog nicht mehr ausdrücklich separat im Gesetzestext aufgenommenen, aber nach wie vor in gleichem Maße umfassten Unterfällen siehe auch nachfolgende Begründung der Nummern 1 bis 6. Die Neufassung ist insofern nicht mit einer inhaltlichen Kürzung verbunden, sondern dient lediglich der Verschlankung auf gesetzlicher Ebene.

Je nach konkret aufzuklärender Fallkonstellation werden die Rechtsgüter jeweils unterschiedlich ausgeprägt bedroht. So werden die Rechtsgüter durch die nachfolgend in § 3 Absatz 1 geregelten erheblichen Bedrohungen typischerweise stärker gefährdet als in sonstigen Konstellationen der Auslandsaufklärung nach Absatz 1 (Grundstufe der nachrichtendienstlichen Auslandsaufklärung). In der Regel am stärksten gefährdet sind die Rechtsgüter im Falle von Bedrohungen mit herausgehobener Bedeutung (§ 4).

Zu Nummer 1

Der Bestand oder die Sicherheit der in der Aufzählung von Buchstabe a) bis c) enthaltenen Gebietskörperschaften, Institutionen und Einrichtungen ist ein besonders gewichtiges Rechtsgut.

Völkerrechtssubjekte sind unverzichtbare Rahmenbedingungen für ein Leben des Staatsvolkes in Freiheit und Sicherheit. In einer zunehmend globalisierten Welt sind zudem die Existenzbedingungen einzelner Staaten in hohem Maße miteinander verschränkt und voneinander abhängig und werden als zentrale gemeinsame Interessen durch Bündnisse und supranationale Einrichtungen wahrgenommen. Bedeutsame internationale Organisationen im Sinne dieser Regelung sind die Europäische Union als supranationale Organisation, die Europäische Freihandelsassoziation und der Zusammenschluss des Nordatlantikvertrages. Der Bestand und die Sicherheit verbündeter Staaten sowie der Bündnisse selbst besitzen deshalb eine existenzsichernde Funktion für die Bundesrepublik Deutschland. Der Schutz solcher Einrichtungen stellt gleichermaßen wie der Schutz von nationalen Einrichtungen ein besonders gewichtiges Rechtsgut dar.

Auch die Sicherheits- und Arbeitsfähigkeit von Einrichtungen Deutschlands oder etwa auch derjenigen von Mitgliedstaaten sowie Einrichtungen der Europäischen Union, des Nordatlantikvertrages und der Europäischen Freihandelsassoziation sind als Bestandteil dieses Rechtsguts zu sehen. Jeder Staat (und jede inter- und supranationale Organisation) benötigt zur Herstellung und Aufrechterhaltung seiner Funktionsfähigkeit wesentliche Einrichtungen. Hierzu gehören neben Einrichtungen, wie etwa die Verkehrsnetze oder administrativen Dienststellen, auch solche, die von privater Seite betrieben werden, wie zum Beispiel Kritische Infrastrukturen auf dem Gebiet der Energie- oder Wasserversorgung. Es kann sich hier auch um Rechtgüter oder Sachen von bedeutendem Wert handeln, deren Erhaltung im öffentlichen Interesse geboten ist. Häufig ginge mit einer Störung der Funktionsfähigkeit auch eine Gefahr für Leib und Leben einer Person oder für den Bestand oder die Sicherheit des Bundes oder eines Landes einher. Dieses Rechtsgut umfasst beispielsweise auch die grundsätzliche Funktionsfähigkeit von (Sicherheits-)Behörden als Teil der staatlichen Sicherheitsstruktur einschließlich des Bundesnachrichtendienstes und seiner wesentlichen Fähigkeiten für die Wahrnehmung des gesetzlichen Auftrags.

Diesem Rechtsgut zugeordnet werden kann auch die Handlungsfähigkeit der Bundesrepublik Deutschland oder der Europäischen Union auf dem Gebiet des Grenzschutzes sowie des Aufenthalts- und Staatsangehörigenrechts (bisher § 11b Nummer 7). Die territoriale Hoheit stellt ein Wesenselement staatlicher Souveränität dar. Das umfasst die Befugnis der Bestimmung über das Aufenthaltsrecht nichtdeutscher Staatsangehöriger auf deutschem Hoheitsgebiet einschließlich der gezielten Übernahme von Verantwortung für Flüchtende und andere Schutzsuchende durch völkerrechtliche Vereinbarungen. Die Umsetzung dieser Verpflichtung und Verantwortung erfordert eine Kenntnis der Informationen einschließlich der personenbezogenen Daten, die für eine Entscheidung über das Aufenthaltsrecht maßgeblich sind. Umfasst sind dabei also nicht nur Vorgänge, des unmittelbaren Grenzübertritts, sondern auch Fragen, die den Aufenthalt im Bundesgebiet betreffen.

Zu Nummer 2

Zu den wesentlichen Aufgaben des Staates gehören der Erhalt seiner Handlungsfähigkeit, der Schutz seiner Bevölkerung und Institutionen sowie die Verteidigung seines Territoriums gegen Angriffe und Bedrohungen von außen. Entsprechend handelt es sich bei der Bündnis- und Verteidigungsfähigkeit der Bundesrepublik um ein besonders gewichtiges Rechtsgut.

Die Bündnisfähigkeit sichert die Teilhabe der Bundesrepublik Deutschland an der internationalen Zusammenarbeit und ist dem Grundgesetz als Ziel immanent (vgl. BVerfG, Urteil vom 15. Juli 2025, 2 BvR 508/21, Rn. 105). Die Verteidigungsfähigkeit als die Gewährleistung der äußeren Sicherheit der Bundesrepublik Deutschland ist ebenso eine staatliche Kernaufgabe, so dass insbesondere die Aufgabe der Landesverteidigung und die Bündnisverpflichtungen Deutschlands uneingeschränkt und zu jeder Zeit wahrgenommen werden müssen. Der Bundesnachrichtendienst unterstützt durch seine Aufgabenerfüllung maßgeblich die seitens der Bundesregierung definierten sicherheitspolitischen Ziele, Interessen und Prioritäten der Bundesrepublik Deutschland, die eine voll einsatzbereite Bundeswehr sowie die Erfüllung der Fähigkeitsziele im Rahmen des Nordatlantikvertrages mit der Übernahme von mehr Verantwortung im internationalen Rahmen vorsehen (vgl. BT-Drs. 20/1410, S. 1 und 8).

Die Verteidigungsfähigkeit umfasst zwei Komponenten, die militärische sowie die zivile Verteidigung, die als Gesamtverteidigung in einem unauflösbaren Zusammenhang und in teilweise direkter Abhängigkeit stehen. Das Prinzip der Gesamtverteidigung gilt in gleicher Weise im nationalen und europäischen Bereich wie in der gemeinsamen Bündnisverteidigung (vgl. dazu auch die Rahmenrichtlinien für die Gesamtverteidigung vom 5. Juni 2024).

Das Rechtsgut der Bündnis- und Verteidigungsfähigkeit umfasst die Funktionsfähigkeit und Sicherheit der Bundeswehr sowie die von verbündeten Streitkräften (auch außerhalb des

Nordatlantikbündnisses). Die Bundeswehr und die ihr verbündeten Streitkräfte sichern Verteidigungsinteressen der Bundesrepublik Deutschland sowie Verteidigungsinteressen internationaler Bündnisse bzw. Systeme gegenseitiger kollektiver Sicherheit, an denen die Bundesrepublik Deutschland beteiligt ist.

Zu Nummer 3

Ein Wesenselement staatlicher Souveränität ist das Vertreten eigener Interessen insbesondere gegenüber anderen Völkerrechtssubjekten. Um die Stellung der Bundesrepublik als Völkerrechtssubjekt zu anderen Staaten auszufüllen, muss die Bundesregierung außenpolitisch handlungsfähig sein. Auf die Befähigung der Regierung hierzu zielt der Auftrag des Bundesnachrichtendienstes (vgl. Gusy, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 1 BND-Gesetz Rn. 28: „Es geht um die Aufklärung der Bedingungen eigener Handlungsmöglichkeiten der Bundesrepublik wie auch möglicher Handlungen Anderer.“). Die Versorgung der Bundesregierung mit Erkenntnissen des Bundesnachrichtendienstes für ihre außen- oder sicherheitspolitischen Entscheidungen hilft dieser, sich im machtpolitischen Kräftefeld der internationalen Beziehungen zu behaupten, und kann folgenreiche Fehlentscheidungen verhindern.

Die Herausforderungen der globalisierten, multipolaren Welt, die von neuen Gestaltungsmächten zunehmend bestimmt wird und in der Grundsätze bestehender Bündnisse in Frage gestellt werden, schaffen neue Rahmenbedingungen und Gefährdungspotenziale. Die Bundesrepublik Deutschland muss außenpolitisch handlungsfähig sein und bleiben, um sich im internationalen Wettbewerb, welcher zunehmend (wieder) von Hegemonialansprüchen und Anarchie geprägt ist, behaupten zu können. Der Schutz dieser außenpolitischen Handlungsfähigkeit der Bundesrepublik Deutschland, ihrer auswärtigen Belange, ist deshalb ein besonders gewichtiges Rechtsgut, das mit Hilfe der Auftragserfüllung des Bundesnachrichtendienstes als einzigem Auslandsnachrichtendienst der Bundesrepublik Deutschland zu schützen ist.

Bei der außenpolitischen Handlungsfähigkeit geht es nicht nur um völkerrechtlich geregelte Materien, sondern auch um die generellen Außenbeziehungen des deutschen Staates. Auch Vorgänge im Ausland, deren Urheber nicht ausländische Staaten sind, können Bedeutung für die Zusammenarbeit deutscher mit ausländischen Stellen haben, wenn außenpolitische Reaktionen erforderlich sind oder sie besondere Relevanz für die Sicherheit der Bundesrepublik Deutschland aufweisen (Beispiele bei *Dietrich* in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 6 BND-Gesetz Rn. 24). Die nachrichtendienstliche Aufklärung hat für die Handlungsfähigkeit der Bundesrepublik Deutschland in der Außen- oder Sicherheitspolitik seit jeher eine erhebliche, in jüngerer Zeit aber spezifisch gewachsene Bedeutung gewonnen (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17 (154, 152), Rn. 106). Der Bundesnachrichtendienst soll dazu beitragen, frühzeitig Bedrohungen zu erkennen, um die Handlungsfähigkeit der Bundesrepublik zu wahren und die Bundesregierung in außen- und sicherheitspolitischen Fragen mit Informationen zu versorgen (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17 (154, 152), Rn. 144). Dabei muss die nachrichtendienstliche Aufklärung im Interesse der Handlungsfähigkeit und Sicherheit der Bundesrepublik Deutschland insbesondere auch an Informationen gelangen können, die ihr – möglicherweise in nachteiliger Absicht – gezielt vorenthalten und in der Hoheitssphäre des Drittstaats geheim gehalten werden. Es besteht daher ein überragendes öffentliches Interesse an einer wirksamen Auslandsaufklärung (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17 (154, 152), Rn. 161).

Das Bundesverfassungsgericht hat das überragende Gewicht dieses Rechtsguts anerkannt und sieht in der außenpolitischen Handlungsfähigkeit der Bundesrepublik Deutschland auch als Voraussetzung der Bündnisfähigkeit und Teilhabe an der internationalen Zusammenarbeit ein dem Grundgesetz immanentes Ziel (BVerfG, Urteil vom 19.°Mai 2020, 1°BvR°2835/17 (154, 152), Rn.°248ff.; BVerfG, Urteil vom 15. Juli 2025, 2 BvR 508/21, Rn. 105).

Zu Nummer 4

Die freiheitliche demokratische Grundordnung, insbesondere auch die freie politische Meinungsbildung, bildet als ein Grundpfeiler der Bundesrepublik Deutschland deren Wesenskern und konstitutive Grundlage für ein Leben in Freiheit und Sicherheit. Sie kann z.B. durch die systematische, zielgerichtete Verbreitung von Fake-News und Desinformationen beeinträchtigt werden, deren Ziel die Störung des gesamtgesellschaftlichen und politischen Gefüges eines Staates in freiheitlicher demokratischer Grundordnung durch die Anwendung konventioneller oder nicht konventioneller Mittel ist. In der Folge kann eine möglicherweise einsetzende Destabilisierung der Gesellschaft von anderen Staaten für eigene, insbesondere machtpolitische Zwecke genutzt werden.

Der Schutz dieser Grundordnung muss also ebenfalls eine vordringliche Aufgabe des Bundesnachrichtendienstes sein.

Zu Nummer 5

Nummer 5 enthält zwei Alternativen: Zum einen werden gewichtige Rechtsgüter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, erfasst. Zum anderen stellen auch Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, ein besonders gewichtiges Rechtsgut dar.

Das Bundesverfassungsgericht hat die „überragend wichtige“ Bedeutung von „Rechtsgütern der Allgemeinheit, deren Grundlagen die Existenz der Menschen berührt“ ausdrücklich anerkannt (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07 u.a., Rn. 247). Zur Konkretisierung dieses besonders gewichtigen Rechtsguts werden nachfolgend für das Tätigkeitsfeld des Bundesnachrichtendienstes beispielhaft typische Ausprägungen dargestellt, deren Verletzung regelmäßig schwere Schäden für den äußeren und inneren Frieden oder der Existenz Einzelner bzw. hochrangiger Gemeinschaftsgüter hervorrufen kann und bei denen daher die besondere Gewichtigkeit anzunehmen ist.

Bei der *Funktionsfähigkeit des inländischen und europäischen Wirtschafts- und Wissenschaftsstandorts* (bisher § 11b Nummer 9) handelt es sich um eine Ausprägung dieses besonders gewichtigen Rechtsguts. Ein Leben in Freiheit und Sicherheit bedarf der wirtschaftlichen Absicherung. Diese Grundlage ist durch Wirtschaftsspionage und anderen Formen der Einflussnahme oder der Beeinträchtigung zunehmend Angriffen ausgesetzt. Der Umstand, dass die Bundesrepublik Deutschland einer der weltweit führenden Wirtschafts- und Wissenschaftsstandorte ist, gehört zu ihrem ökonomischen Wesenskern. Die Bundesrepublik Deutschland ist eng in internationale Handels- und Finanzströme eingebunden. Gesicherte Versorgungswege, stabile Märkte sowie funktionierende Kommunikationsströme sind hierfür unerlässlich. Um als wettbewerbsfähiger Standort bestehen zu können, müssen Innovationen, Forschung und Wirtschaft im Kontext strategischer Ressourcen geschützt werden. Durch einen solchen Schutz soll insbesondere die Schädigung von Unternehmen in der Europäischen Union durch Wirtschaftsspionage und die Fälle des Diebstahls geistigen Eigentums verhindert werden. Im Rahmen von Investitionsprüfungen sind bei Unternehmensübernahmen oder ausländischen Direktinvestitionen Kenntnisse über die ausländischen Akteure erforderlich. Dies gilt insbesondere im Bereich sogenannter Schlüsseltechnologien.

Eine Beeinträchtigung der Geldwertstabilität im Euro-Währungsraum führt in der Regel ebenfalls zu einer Gefährdung der Funktionsfähigkeit des inländischen oder europäischen Wirtschaftsstandorts. Dies kann sich beispielsweise aus im Ausland begangenen Geldfälschungen ergeben. Zwar ist dem Tatbestand der Geldfälschung der Auslandsbezug nicht inhärent, er stellt sich aber jedenfalls dann dar, wenn die Geldfälschung unter Beteiligung ausländischer Staaten geschieht oder aufgrund ausländischer (auch nicht-staatlicher) Aktivitäten ein Ausmaß annimmt, das die Geldwertstabilität im Euro-Währungsraum bedroht, so dass sie mit den Mitteln der inländischen Strafverfolgung nicht ausreichend bekämpft

werden kann, sondern außenpolitische Reaktionen erforderlich macht (BVerfG, Urteil vom 14. Juli 1999, 1 BvR 2226/94, Rn. 205).

Die *Sicherheit von informationstechnischen Systemen in Fällen von herausgehobener Bedeutung für die Allgemeinheit* (bisher § 11b Nummer 8) ist ebenso einem der Rechtsgüter des Absatz 2 zuzuordnen, typischerweise der Nummer 5 Alternative 1. Die Sicherheit von informationstechnischen Systemen, d.h. deren Integrität, Vertraulichkeit und Verfügbarkeit, stellt ein besonders gewichtiges Rechtsgut im Sinne der Rechtsprechung des Bundesverfassungsgerichts dar. Dies gilt für solche informationstechnischen Systeme, die in sich bereits von herausgehobener Bedeutung für die Allgemeinheit sind (z.B. Kritische Infrastrukturen). Bedrohungen für diese Ausprägung eines geschützten Rechtsguts können aber beispielsweise auch durch weiträumig orchestrierte Cyberangriffe oder -kampagnen entstehen, die eine Vielzahl von informationstechnischen Systemen bedrohen und dadurch eine herausgehobene Bedeutung für die Allgemeinheit haben. Informationstechnischen Systemen kommt heute, unabhängig davon, ob sie staatlich oder privat betrieben werden, für die Wahrnehmung von persönlichen, bürgerlichen und wirtschaftlichen Freiheiten eine zentrale und unverzichtbare Bedeutung zu. Zugleich sind solche Systeme in immer stärkerem Maße Angriffen, namentlich auch durch fremde Mächte, mit dem Ziel ausgesetzt, diese Freiheiten zu verletzen und dadurch dem für ihren Schutz verantwortlichen Staat Schaden zuzufügen. Der Schutz vor Cyberangriffen in Fällen von herausgehobener Bedeutung für die Allgemeinheit besitzt deshalb für ein Leben in Freiheit und Sicherheit systemische Bedeutung. Cyberangriffe bergen in sich ein solch immenses Gefährdungspotential, so dass bereits ohne Ansehung des im Einzelfall konkret betroffenen informationstechnischen Systems die Sicherheit der informationstechnischen Systeme als besonders gewichtiges Rechtsgut anzusehen ist; jedenfalls dann, wenn es sich um die Aufklärung von terroristischen, staatlichen oder weiträumig orchestrierten Angriffen handelt. Cyberangriffen ist die Gefahr des Eintritts von Großschadenslagen immanent. Angriffe auf informationstechnische Systeme oder eine Störung der Verfügbarkeit von informationstechnischen Systemen, können insbesondere bei einer Vielzahl betroffener informationstechnischer Systeme oder der Betroffenheit von Kritischen Infrastrukturen erhebliche Auswirkungen auf die öffentliche Sicherheit und Ordnung, bis hin zu einer Gefährdung von Leib und Leben oder des Bestandes oder der Sicherheit des Bundes oder eines Landes bewirken. Es können durch Cyberangriffe Ereignisse eintreten, die das Leben oder die Gesundheit einer großen Anzahl von Menschen, die lebensnotwendige Unterkunft sowie Versorgung der Bevölkerung, wesentliche Sachwerte oder die Umwelt erheblich gefährden oder beinträchtigen. Das Ziel der Aufklärung von Cyberbedrohungen ist dementsprechend auch in der Nationalen Sicherheitsstrategie der Bundesregierung für die Bundesrepublik Deutschland (Stand Juni 2023, Seite 61) verankert worden.

Das Bundesverfassungsgericht hat gleichermaßen den Schutz von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, ausdrücklich als besonders gewichtiges Rechtsgut eingeordnet (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 243). Als regelgebendes Beispiel („Gemeint sind etwa“) nennt das Bundesverfassungsgericht dabei wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen. Die Subsumtion unter Nummer 5 Alternative 2 muss sich dementsprechend an diesem Beispiel orientieren, dabei ist ein enges Verständnis geboten (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 243). Der Regelung kommt eine Auffangfunktion zu, die zum Beispiel bedeutende Gegenstände von kulturellem Wert betreffen kann.

Zu Nummer 6

Leib, Leben und Freiheit der Person sind die unverzichtbaren Grundlagen jeder individuellen Existenz und zählen damit zu den besonders gewichtigen Rechtsgütern.

Der Begriff der körperlichen Unversehrtheit findet sich, um den Bezug im Vergleich zu dem antiquierten Begriff „Leib“ klarer transparent zu machen. Da die Begriffsbestimmung als

Anknüpfung für Schutzaufgaben dient, wird der Individualrechtsgüterschutz erweitert, indem einerseits auch die sexuelle Selbstbestimmung einbezogen wird (vgl. BVerfG, Beschluss vom 1. Dezember 2020, 2 BvR 916/11, Rn. 277) Eine weitergehende Öffnung für gleichgewichtige Schutzerfordernisse (beispielsweise Gesundheit, BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 203; auch komplexere Rechtsgüter wie das Kindeswohl können u.U. berührt sein) ist durch die Öffnung des Katalogs ebenfalls denkbar. .

Entsprechend der Regelungssystematik sind lediglich Rechtsgüter benannt, nicht Eingriffsmodalitäten. Der bisherige Bezug auf „eine erhebliche Gefährdung im Einzelfall“ entfällt daher, zumal die Formulierung eher missverständlich war (der Bezug auf eine „Gefährdung im Einzelfall“ ist als konkrete Gefahr missdeutbar, was im nachrichtendienstlichen Kontext nicht gemeint sein kann). Die Regelung kommt daher auf die in der Gesetzespraxis übliche Regelungsweise zurück, die auch in der Verfassungsrechtsprechung abgesichert ist (vgl. BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 298f., 311). Ist bei einem Eingriffssachverhalt im Eingriffszeitpunkt damit zu rechnen, dass die anlassgebende Situation das zu schützende Rechtsgut der körperlichen Unversehrtheit oder Freiheit nur unerheblich gefährdet, bleibt dies unter Anwendung der Verhältnismäßigkeitsschranke zu würdigen.

Zu § 3 (Erhebliche Bedrohungen)

Die Regelung des § 3 dient als erste Qualifikationsstufe für Maßnahmen des Bundesnachrichtendienstes.

Zu Absatz 1

Absatz 1 legt fest, welche Aufklärungsziele des Bundesnachrichtendienstes von erheblicher Bedeutung für die Bundesrepublik Deutschland sind. Der qualifizierende Umstand der Erheblichkeit liegt also bei Erfüllung des Tatbestandsmerkmals der Beeinträchtigung der Rechtsgüter im Sinne des § 2 Absatz 2 in besonderem Maße vor. Das Tatbestandsmerkmal verschließt sich aufgrund der Vielgestaltigkeit des Aufklärungsauftrags des Bundesnachrichtendienstes und der zur Erfüllung dieses Auftrags notwendigen Flexibilität einer abschließenden Definition. Eine besondere Beeinträchtigung kann und wird regelmäßig etwa dann anzunehmen sein, wenn eine qualifizierte oder quantifizierte Schwere der Beeinträchtigung plausibel erscheint.

Zu Absatz 2

Zur Erleichterung der praktischen Handhabung und im Interesse der Normenklarheit enthält Absatz 2 als Auslegungshilfe zudem die Regelung, dass die in den Absätzen 3 und 4 näher ausgeführten Bedrohungsziele und Bedrohungsfelder (im weiteren Verlauf z.T. auch vereinfacht als „Bedrohungen nach“ bezeichnet) bei der Prüfung einer Bedrohung auf ihre Qualifikation von erheblicher außen- oder sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland besonders zu berücksichtigen sind. Liegt eine der dort genannten Varianten vor, so entfaltet dies eine starke Indizwirkung für die Annahme der Erheblichkeit einer Bedrohung – erforderlich bleibt indes weiterhin eine Prüfung im Einzelfall.

Der gesetzliche Indizienkatalog der Absätze 3 und 4 steuert die durch die Fachbehörde im Einzelfall vorzunehmende Gesamtbetrachtung der Potenzialität seines Aufklärungsziels. Die indizielle Ausgestaltung dieser Regelung beruht auf der Erwägung des Bundesverfassungsgerichts, dass gerade in dem vom Bundesnachrichtendienst aufzuklärenden Vorfeldbereich Bewertungen aufgrund geringer Tatsachendichte in besonderem Maße von Erfahrung, Fachwissen und nachrichtendienstlichen Erkenntnislagen abhängig sind, über die der Bundesnachrichtendienst verfügt (BVerfG, Beschluss vom 17. Juli 2024, 1 BvR 2133/22, Rn. 149). Der Bundesnachrichtendienst trifft hierbei im Einzelfall eine prognostische Risikoabschätzung von hoher Komplexität, sowohl hinsichtlich der Bedrohung als auch ihrer Wirkung auf hochrangige Rechtsgüter.

Hierbei ist zu beachten, dass an die Tätigkeit des Bundesnachrichtendienstes mit dem Ziel der Auslandsaufklärung passende verfassungsrechtliche Maßstäbe angelegt werden müssen, insbesondere die Tätigkeit des Bundesnachrichtendienstes zur Auslandsaufklärung der Tätigkeit der Verfassungsschutzbehörden nicht gleichgesetzt werden kann. Insofern können (und müssen) die Regelungen im BND-Gesetz, die eine erhebliche (oder auch nach § 4 herausgehobene) Aufklärungsbedürftigkeit begründen, von den gesetzlichen Grundlagen der Verfassungsschutzbehörden abweichen. Das Eingriffsgewicht nachrichtendienstlicher Maßnahmen hängt davon ab, welche Nachteile den Grundrechtsberechtigten drohen oder von ihnen befürchtet werden müssen (vgl. dazu u.a. BVerfG, Beschluss vom 17. Juli 2024, 1 BvR 2133/22, Rn. 89). In diesem Sinne ist typischerweise das Eingriffsgewicht der nachrichtendienstlichen Maßnahmen des Bundesnachrichtendienstes in Erfüllung seines Auslandsaufklärungsauftrages für die betroffene Person geringer als bei der nachrichtendienstlichen Tätigkeit der Verfassungsschutzbehörden. Die Informationsgewinnung des Bundesnachrichtendienstes ist typischerweise nicht darauf ausgerichtet, operative Anschlussmaßnahmen mit konkreten Auswirkungen für die durch die Informationsgewinnung betroffenen Personen im Inland oder solchen mit deutscher Staatsangehörigkeit im Ausland zu generieren. So sind Maßnahmen des Bundesnachrichtendienstes nicht darauf ausgerichtet, mit den erlangten Informationen z.B. ein Vereins- oder Betätigungsverbot in der Bundesrepublik Deutschland zu erwirken. Selbst wenn die Informationsgewinnung des Bundesnachrichtendienstes im Inland oder bei einem deutschen Staatsangehörigen im Ausland erfolgt, zielt diese dennoch immer auf die Erlangung von Erkenntnissen, die von außen- oder sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, also die Auslandsaufklärung, ab. Die nach Maßgabe des Verfassungsrechts normierten ausdifferenzierten Übermittlungsvorschriften stellen ferner sicher, dass mit dieser Zielrichtung gewonnene Informationen sich nicht unausgewogen zum Nachteil von einzelnen Grundrechtsberechtigten auswirken. Selbst wenn die Zielrichtung der Aufklärung des Bundesnachrichtendienstes doch zur Erhebung von Informationen führt, die geeignet sind, betroffene Personen in ihrer eigenen Lebensführung zu beeinträchtigen, in dem z.B. Informationen erlangt werden, die eine Teilnahme an internationalen terroristischen Bedrohungen von außen- oder sicherheitspolitischer Bedeutung nahelegen, wird durch die Übermittlungsvorschriften (vgl. Abschnitt 6) sichergestellt, dass die betroffenen Personen Nachteile durch eingriffsintensive Folgemaßnahmen lediglich in verfassungsrechtlich zulässigen Fällen ereilen. Das für betroffene Personen und insbesondere auch für deutsche Staatsangehörige oder sich im Bundesgebiet aufhaltende Personen gegenüber der Verfassungsschutztätigkeit regelmäßig geringere Eingriffsgewicht der Auslandsaufklärung des Bundesnachrichtendienstes sowie die Bedeutung dieser originär ausschließlich durch den Bundesnachrichtendienst wahrgenommenen Tätigkeit für die Handlungsfähigkeit und Sicherheit der Bundesrepublik Deutschland mit Blick auf aus dem Ausland wirkende Bedrohungen ist bei der Fassung der gesetzlichen Grundlagen für die Tätigkeit des Bundesnachrichtendienstes entsprechend zu berücksichtigen.

Ferner ist zu beachten, dass sollte trotz des Vorliegens eines der in § 4 Absatz 3 bis 5 genannten Indizien im Einzelfall keine Bedrohung von herausgehobener Bedeutung anzunehmen sein, diese Indizien auch (erst recht) im Rahmen der Prüfung nach § 3 Absatz 1 besonders zu berücksichtigen sind und so ihre Indizwirkung auch zugunsten der Annahme einer erheblichen Bedrohung entfalten können. Dienen sie nach gesetzgeberischer Wertung bereits als Indizien für die zweite Qualifikationsstufe, entfalten sie ihre Indizwirkung naturgemäß auch für die erste Qualifikationsstufe.

Zu Absatz 3

Dieser Absatz enthält Bedrohungsziele. Richtet sich eine Bedrohung gegen eines der genannten Ziele, so liegt aufgrund der jeweiligen Besonderheiten dieser Ziele ein maßgebliches Indiz vor, dass eine Beeinträchtigung in besonderem Maße zu besorgen steht. Da eine Einzelfallprüfung zu erfolgen hat, bleibt freilich immer auch Raum für atypische Sonderfälle. Durch die (offene) Prüfung des Absatz 1 bleibt spiegelbildlich zugleich auch Raum

für gesetzgeberisch nicht bedachte sonstige Sachverhalte, die das Merkmal der Beeinträchtigung der Rechtsgüter im Sinne des § 2 Absatz 1 in besonderem Maße erfüllen können.

Sollte eine der genannten Bedrohungslagen im Einzelfall nicht als erhebliche (oder nach § 4 herausgehobene) Bedrohung zu charakterisieren sein, bleibt eine Aufklärung durch den Bundesnachrichtendienst auf Grundlage des § 2 Absatz 1 und im Rahmen seiner Befugnisse unbenommen.

Der Katalog der qualifizierten Bedrohungsziele dient der näheren Bestimmung und als Auslegungshilfe des Rechtsbegriffs der Beeinträchtigung in besonderem Maße.

Zu Nummer 1

Gefährdungen des inländischen oder europäischen Wirtschafts- und Wissenschaftsstandortes und diesem zugeordneter Wirtschaftssubjekte können immensen volkswirtschaftlichen Schaden begründen und in der Folge sogar eine Gefährdung der Sicherheit der Bundesrepublik Deutschland oder von Mitgliedstaaten der Europäischen Union bedeuten, wie etwa solche durch ausländische nachrichtendienstliche Aktivitäten mit Blick auf den Wissenschaftsstandort Deutschland oder Europa. Eine staatlich gelenkte Beeinträchtigung kann dabei nicht nur auf die Verschaffung eines rein ökonomischen Vorteils ausgerichtet sein, sondern auch dem Ziel dienen, in wichtigen Wirtschafts- und Technologiefeldern durch die Zerstörung bzw. den Aufkauf ausländischer Konkurrenz eine eigene Monopolstellung zu erreichen, die nicht nur einen volkswirtschaftlichen Vorteil erbringt, sondern darüber hinaus andere Staaten in Bezug auf diese Felder und insbesondere deren kritische Infrastruktur in eine Abhängigkeit zwingt.

Erforderlich ist eine „erhebliche Beeinträchtigung“ – dies ist ein auslegungsoffener Begriff, der lediglich sicherstellen soll, dass nicht gänzlich untergeordnete Betroffenheiten des Wirtschafts- und Wissenschaftsstandorts die Indizwirkung entfalten. Rechtssystematisch ist dieser Zusatz rein klarstellend, da ohnehin eine Einzelfallprüfung erfolgen muss und untergeordnete Betroffenheiten bereits nicht geeignet sind, die besonders gewichtigen Rechtsgüter „in besonderem Maße zu beeinträchtigen“.

Zu Nummer 2

Veränderungen der Versorgung mit wesentlichen Rohstoffen, Gütern, Energien sowie kritischen Technologien im Ausland können sich auf die Bundesrepublik Deutschland in dem Zusammenhang auswirken, dass die Bundesrepublik Deutschland als rohstoffarmes Land mehr als andere Länder auf den freien grenzüberschreitenden Handel mit Energie und Rohstoffen oder kritischen Technologien angewiesen ist. Diese Bedrohungslage umfasst – ebenso wie die anderen Bedrohungslagen – nur solche Beeinträchtigungen, die in ihrer Wirkung eine außen- oder sicherheitspolitische Bedeutung entfalten. Rohstoffe und Güter umfassen in diesem Zusammenhang beispielsweise auch Lebensmittel oder Medikamente. Beeinträchtigungen in diesem Bereich in Form von Lieferengpässen oder -ausfällen haben erhebliche Folgen für die Versorgung der Bevölkerung und die deutsche Volkswirtschaft. Teilweise setzen staatliche Akteure die Zurückhaltung von Rohstoff- und Güterexporten gezielt als politisches Druckmittel gegen andere Länder ein. Die Aufklärung solcher Beeinträchtigungen ist für die Auftragserfüllung des Bundesnachrichtendienstes von besonderer Bedeutung, da die Bundesrepublik z.B. Rohöl für deutsche Raffinerien oder Erdgas in erheblichem Umfang aus dem Ausland bezieht, teilweise über Pipelines, die ihrerseits durch mehrere Länder verlegt sind. Einseitige Maßnahmen der Lieferstaaten oder Auseinandersetzungen zwischen Liefer- und Transitstaaten können die Energieversorgung der Bundesrepublik gefährden. Bei rechtzeitiger Warnung hätte die Bundesregierung beispielsweise die Möglichkeit, diplomatisch aktiv zu werden und vermittelnd einzugreifen bzw. Maßnahmen zur Aufrechterhaltung der Energieversorgung einzuleiten. Auch die Beeinträchtigung der Versorgung von Mitgliedstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages können eine erhebliche Bedrohung für die

Außen- und Sicherheitspolitik der Bunderepublik Deutschland darstellen. Die Versorgung dieser Länder kann insbesondere Auswirkungen auf den freien grenzüberschreitenden Handel mit Energie und Rohstoffen oder kritischen Technologien haben, weshalb dies gleichermaßen wie die nationale Versorgung ein gewichtiges Interesse der Bundesrepublik Deutschland darstellt.

Zu Nummer 3

Bedrohungen der Sicherheit der Infrastruktur im Weltraum sind im Interesse der Bundesrepublik ebenfalls frühzeitig zu erkennen und aufzuklären. Die militärische und nachrichtendienstliche Nutzung von Weltraumsystemen (insbesondere Satelliten), Antisatellitensystemen oder im Weltraum stationierter Waffen können die Sicherheit der Bundesrepublik Deutschland und ihrer Verbündeten beeinträchtigen oder sogar gefährden. Hier sind nur solche Bedrohungen erfasst, welche das Bedrohungsziel „Weltraum“ in einer Weise betreffen, welche erhebliche Auswirkungen auf die Bundesrepublik Deutschland haben kann. Dies können dabei sowohl unmittelbare als auch mittelbare Beeinträchtigungen sein; so wäre etwa die Beeinträchtigung des GPS-Satellitennetzwerkes (oder eines global agierenden Satelliten-Internetproviders) auch dann erfasst, wenn dies die Bundesrepublik Deutschland nicht unmittelbar in geographischer Hinsicht betreffen würde, da durch die entstehenden Folgen mittelbar erhebliche Auswirkungen drohen.

Zu Absatz 4

In Absatz 4 sind Bedrohungsfelder erfasst; d.h. Bereiche aus denen Bedrohungen erwachsen können, bei denen ebenfalls eine starke Indizwirkung besteht, dass die Bedrohungen die besonders gewichtigen Rechtsgüter in erheblichem Maße beeinträchtigen können.

Zu Nummer 1

Nummer 1 erfasst den Bereich des Terrorismus und Extremismus, der entweder durch Gewaltbereitschaft charakterisiert wird, oder auf die planvoll verborgen betriebene Durchsetzung politscher, religiöser oder ideologischer Ansichten ausgerichtet ist. Die Bedrohungslage durch den internationalen gewaltbereiten Terrorismus ist unverändert hoch.

Gewalttätige und extremistisch ausgerichtete Organisationen haben häufig Verbindungen nach Deutschland und Europa und betreiben von dort aus anschlagsvorbereitende Maßnahmen der Finanzierung und Rekrutierung. Dabei erfolgt auch eine Nutzung europäischer Staaten als Flucht- und Ruheraum für Mitglieder der Organisationen.

Darüber hinaus hat der gewaltbereite, international vernetzte Extremismus an Bedrohungspotenzial gewonnen. Gerade im Bereich des gewaltbereiten Rechtsextremismus bieten insbesondere soziale Netzwerke Möglichkeiten zum Austausch bzw. zur Kooperation mit entsprechenden Gruppierungen im Ausland. Hieraus erwächst die Gefahr, dass sich Radikalisierungen vollziehen. Transnationale Netzwerke verfolgen das Ziel einer weltweiten Durchsetzung ihres extremistischen Gedankengutes. Nicht in allen Fällen wird hierzu auf das Mittel der Gewalt gesetzt. Die Netzwerke sind bestrebt, auch in Deutschland Grundwerte der freiheitlichen Demokratie zu unterminieren und schlussendlich zu beseitigen.

Die – regelmäßig – erhebliche Bedrohung in dieser Ausgestaltungsform des Terrorismus/Extremismus erfordert insbesondere auch die Aufklärung von Finanzströmen, welche der Finanzierung dieser Aktivitäten dienen. Dabei wird es insoweit häufig nicht um einzelfallbezogene Finanzierungen von Aktivitäten gehen, sondern um die Aufklärung von Finanzierungswegen, -strukturen und -strategien, mit denen der (internationale) Terrorismus und Extremismus gefördert wird.

Zu Nummer 2

Unter hybriden Einflussmaßnahmen ist die interessensgeleitete Einflussnahme auf Staaten oder Staatenverbünde, insbesondere zentraler Akteure, deren Netzwerke und der von ihnen genutzten Instrumente, zu verstehen. Ziel ist die interessengeleitete Einflussnahme auf staatstragende Strukturen, wie z.B. Gesellschaft, Politik, unabhängige Presse etc., unter Inkaufnahme der Verletzung etablierter Normen, Ordnungen und Werte. Hybride Einflussmaßnahmen sind gekennzeichnet durch die Anwendung konventioneller oder nicht konventioneller Mittel durch staatliche oder nichtstaatlich gelenkte Akteure. Die Verschleierung der tatsächlichen Urheberschaft stellt in der Regel ein wesentliches Merkmal hybrider Einflussmaßnahmen dar.

Hybride Einflussmaßnahmen sind häufig nicht per se illegal, aber durchaus illegitim. Die Aufklärung von hybriden Einflussmaßnahmen sowie deren Hintergründen und Auswirkungen durch den Bundesnachrichtendienst ist von erheblicher außen- oder sicherheitspolitischer Bedeutung. Hybride Aktivitäten müssen frühzeitig erkannt sowie ihre Verbreitungsmethoden und -wege nachvollzogen und ihre Wirkung beobachtet werden, um die Reaktionsfähigkeit der Bundesrepublik Deutschland auf solche Einflussnahmen zu verbessern. Von besonderer Herausforderung ist hierbei die ständige Wandlung und dynamische Entwicklung von hybriden Einflussmaßnahmen, die häufig erst im Nachgang als solche erkannt werden. So können oft erst nachträglich alltägliche Vorkommnisse, wie z.B. Unfälle oder größere Unglücke, als Sabotageakte ausländischer Akteure identifiziert werden.

Die Auswirkungen hybrider Einflussnahmen auf den freiheitlich demokratischen Diskurs einer Gesellschaft können für eigene, insbesondere machtpolitische Zwecke des handelnden Akteurs genutzt werden, unabhängig davon, ob dieser die Beeinträchtigung selbst herbeigeführt hat oder nicht. Die Identifizierung der eingesetzten Instrumente, des Modus Operandi sowie des Grundes für den Einsatz hybrider Instrumente ist mit Blick auf den Aufklärungsauftrag des Bundesnachrichtendienstes essentiell. Die Auswirkungen der hybriden Einflussnahmen müssen dabei „erheblich“ sein, sodass nicht jedwede untergeordnete Tätigkeit hierunterfällt. Dies wäre etwa bei singulären Nachrichten in sozialen Netzwerken der Fall, solange die betreffende Nachricht nicht von einem besonders reichweitenstarken Account ausgeht. Die Auswirkungen müssen zudem nicht „unmittelbar“ sein; mittelbare Auswirkungen (etwa durch Verunsicherung der Gesellschaft oder Störung des außenpolitischen Verhältnisses mit anderen Staaten durch Einflussnahmen in diesen ausländischen Staaten) sind erfasst.

Da bei hybrider Einflussnahme häufig verdeckt mit Mittelsmännern und Institutionen im jeweiligen Zielland sowie insbesondere unter Nutzung von sozialen Medien gearbeitet wird, sind ebendiese erster und regelmäßig einziger Ansatzpunkt für die nachrichtendienstliche Aufklärung hybrider Einflussmaßnahmen durch den Bundesnachrichtendienst. Die Nummer erfasst damit sowohl mittelbare, als auch unmittelbare Steuerungen durch fremde Mächte.

Erforderlich ist, dass die Einflussnahme „erhebliche Auswirkungen“ auf die Bundesrepublik Deutschland haben kann. Dies soll sicherstellen, dass nicht gänzlich untergeordnete Einflussnahmen die starke Indizwirkung des Bedrohungsfeldes entfalten. Möglich sind hier mittelbare wie unmittelbare Auswirkungen – so hat etwa eine staatlich gelenkte hybride Einflussnahmekampagne auf ein anderes Land regelmäßig ebenfalls erhebliche Auswirkungen auf die Bundesrepublik, beispielsweise wenn hierdurch gesellschaftliche Instabilität oder politische Umwälzungen beabsichtigt sind. Klarstellend ist zudem aufgenommen, dass jede durch eine fremde Macht gelenkte Einflussnahme eine solche ist, die erhebliche Auswirkungen haben kann.

Zu Nummer 3

Die illegale Weiterverbreitung von Kriegswaffen sowie von Waren und technischen Unterstützungsleistungen mit ziviler und militärischer Verwendung in Fällen von erheblicher Bedeutung trägt zur Destabilisierung von Staaten und ganzen Regionen bei und begünstigt die Entstehung neuer Krisen- und Konfliktlagen. Die Umsetzung des Kriegswaffenkontrollgesetzes dient der Friedenssicherung und Kriegsverhütung. Die Aufklärung von Proliferation von Kriegswaffen in diesem Sinne soll friedensstörende Handlungen verhindern, das friedliche Zusammenleben der Völker schützen sowie die Gefahren für den Völkerfrieden und die internationale Sicherheit abwehren. Artikel 26 Absatz 2 des Grundgesetzes normiert zu diesem Zweck, dass Kriegswaffen nur mit Genehmigung der Bundesregierung hergestellt, befördert und in den Verkehr gebracht werden dürfen. Neben den Kriegswaffen stehen auch Rüstungsgüter im Fokus der Aufklärung, um eine destabilisierende Anhäufung konventioneller Rüstungsgüter in Krisenregionen oder einen Missbrauch zur internen Repression zu verhindern.

Der Bundesnachrichtendienst betrachtet neben der illegalen Verbreitung von Kriegswaffen auch legale Geschäfte mit Kriegswaffen in Staaten, in denen der Erwerb zur Destabilisierung anderer Länder oder Regionen beitragen kann oder wenn zu befürchten ist, dass Waffen im Empfängerstaat zwar legal erworben werden, jedoch aufgrund der dortigen Strukturen die Gefahr der Weitergabe der Waffen an Akteure besteht, von denen internationales Gefährdungspotential ausgeht. Eine solche Situation kann insbesondere in Staaten eintreten, die im Auftragsprofil der Bundesregierung als durch den Bundesnachrichtendienst als priorisiert aufzuklären deklariert wurden.

Umfasst von der Regelung ist darüber hinaus aufgrund des besonderen Gefährdungspotentials auch die Aufklärung von Programmen nuklearer, biologischer und chemischer Waffen und ihrer Trägersysteme sowie deren Weiterverbreitung. Da in diesem Bereich regelmäßig unter Einsatz erheblicher Verschleierungsbemühungen agiert wird, werden auch Vor- und Umfeldaktivitäten wie Zulieferungen zu solchen Programmen aufgeklärt. Dies gilt auch dann, wenn noch keine konkrete Proliferationsabsicht nachweisbar ist.

Die Aufklärung solcher Programme für die Proliferation von Massenvernichtungswaffen ist für die Auftragserfüllung des Bundesnachrichtendienstes von herausragender Bedeutung. Ziel ist es, eine Bedrohung Deutschlands oder seiner Bündnispartner durch Massenvernichtungswaffen zu verhindern. Zur Erreichung dieses außen- und sicherheitspolitischen Ziels richtet sich die Aufklärung vorrangig gegen Länder, die sich um Massenvernichtungswaffen bemühen. Daneben können auch nicht-staatliche Akteure im Fokus stehen. Die Proliferation strategischer Güter in solche ABC-Programme und Trägersysteme wird oft durch Tarnfirmen, Zwischenhändler und gezielt komplizierte Handels(um)wege und entsprechend verschleierter Finanzströme ermöglicht.

Auch die Aufklärung des unerlaubten Außenwirtschaftsverkehrs mit Waren und technischen Unterstützungsleistungen ist wesentliche Aufgabe des Bundesnachrichtendienstes, dies umfasst auch den Verkehr mit sog. Dual-Use-Gütern. Erfasst sind nur Sachverhalte von erheblicher Bedeutung, die Aufklärung rein regionaler Sachverhalte mit beschränktem Risikopotential ist nicht möglich.

Erforderlich ist eine „erhebliche Beeinträchtigung“ – dies ist ein auslegungsoffener Begriff, der lediglich sicherstellen soll, dass nicht gänzlich untergeordnete Warenverkehre die starke Indizwirkung des Bedrohungsfeldes entfalten. Rechtssystematisch ist dieser Zusatz rein klarstellend, da ohnehin eine Einzelfallprüfung erfolgen muss und untergeordnete Betroffenheiten bereits nicht geeignet sind, die besonders gewichtigen Rechtsgüter „in besonderem Maße zu beeinträchtigen“.

Zu Nummer 4

Organisierte Kriminalität ist die von Gewinn- oder Machtstreben bestimmte, planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, und bei der mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken.

Straftaten von erheblicher Bedeutung sind solche, die zumindest dem mittleren Kriminalitätsbereich zuzuordnen und geeignet sind, den Rechtsfrieden empfindlich zu stören sowie das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen (vgl. BVerfG, Urteil vom 14. Dezember 2000, 2 BvR 1741/99, Rn. 52).

Die Bedrohungslage durch die internationale organisierte Kriminalität ist insbesondere in ihrer Ausprägung des internationalen Rauschgifthandels unverändert hoch. Rauschgiftkriminalität ist seit Jahren das Hauptbetätigungsfeld von organisierter Kriminalität in Deutschland. Konspirativ agierende kriminelle Organisationen bedienen sich dabei eng verzweigter, internationaler Transport- und Logistikwege. Typischerweise stellen Erpressungs- und Tötungsdelikte, Eigentumskriminalität sowie Waffenhandel und -schmuggel zugleich Nebenaktivitäten im Bereich der organisierten Rauschgiftkriminalität dar.

Darüber hinaus ist die Aufklärung von internationalen Geldwäscheaktivitäten für die Auftragserfüllung des Bundesnachrichtendienstes von herausragender Bedeutung, da legal einsetzbare Gewinne, beispielsweise zum Erwerb von Luxusgütern, eine wichtige Voraussetzung für das Handeln organisierter krimineller Strukturen darstellen. Ohne Aussicht auf diese, müssten die kriminellen Strukturen komplett in ihrem eigenen Milieu verbleiben. Zudem erlauben legalisierte Gelder den Aufbau wirtschaftlichen und politischen Einflusses. Bedrohungen mit Auswirkungen auf die Bundesrepublik Deutschland gehen dabei sowohl von nationalen kriminellen Strukturen, die internationale Geldwäschestrukturen zur Legalisierung ihrer inkriminierten Gelder nutzen, als auch von internationalen Akteuren aus. Durch die Aufklärung erlangt der Bundesnachrichtendienst insbesondere Erkenntnisse über die klandestinen Methoden der entsprechenden Akteure betreffend die Einschleusung inkriminierter Gelder in den legalen Wirtschaftskreislauf.

Fest verankert in der organisierten Kriminalität ist ferner der Menschenhandel. Der Begriff des „Menschenhandels“ bezeichnet die Anwerbung, Beförderung, Verbringung, Beherbergung oder Aufnahme von Personen durch die Androhung oder Anwendung von Gewalt oder anderen Formen der Nötigung, durch Entführung, Betrug, Täuschung, Missbrauch von Macht oder Ausnutzung besonderer Hilflosigkeit oder durch Gewährung oder Entgegennahme von Zahlungen oder Vorteilen zur Erlangung des Einverständnisses einer Person, die Gewalt über eine andere Person hat, zum Zweck der Ausbeutung. Ausbeutung umfasst mindestens die Ausnutzung der erzwungenen Prostitution anderer oder andere Formen sexueller Ausbeutung, Zwangsarbeit oder Zwangsdienstbarkeit, Sklaverei oder sklaverei-ähnliche Praktiken, Leibeigenschaft oder die Entnahme von Organen. Insbesondere flüchtende Personen geraten in die Fänge von Menschenhändler-Strukturen. Dies führt regelmäßig zu Zwangsprostitution und zu sonstiger Zwangs-/Schwarzarbeit, woraus auch Gefahren für Gesundheit, Leib und Leben dieser Personen erwachsen. Durch die Aufklärung erlangt der Bundesnachrichtendienst insbesondere Erkenntnisse zu relevanten Personen und Personenzusammenschlüssen sowie deren Modi Operandi. Die Aufklärung dieses Phänomenbereichs ist für die Auftragserfüllung des Bundesnachrichtendienstes daher ebenfalls von besonderer Bedeutung.

Darüber hinaus unterfällt die Aufklärung krimineller Strukturen zur Ermöglichung der illegalen Migration regelmäßig dem Phänomenbereich der organisierten Kriminalität. Illegale Migration bezeichnet die Einreise nach und den Aufenthalt in Staaten unter Verstoß gegen die dort geltenden gesetzlichen Bestimmungen. Sie ist regelmäßig nur unter Zuhilfenahme

krimineller Strukturen (Schleuser, Dokumentenfälscher, Menschenhändler etc.) möglich. Für die kriminellen Akteure steht dabei die Profitmaximierung im Vordergrund. Für die irregulären Migrantinnen und Migranten ist der Weg nach Deutschland dagegen mit erheblichen Gefahren für Leib und Leben verbunden. Lukrativstes Geschäft für die internationale organisierte Kriminalität ist in diesem Zusammenhang die Ausbeutung irregulär migrierter Arbeitskräfte in vielfältiger Form („Abarbeiten“ von Vermittlungsgebühren oder vorgestreckter Reisekosten, Vorenthalten von Arbeitslohn etc.). Illegale Migrationsbewegungen können zudem die Grenzsicherheit und damit die Ausübung staatlicher Souveränitätsrechte entlang der EU-Außengrenze gefährden. Durch die Aufklärung erlangt der Bundesnachrichtendienst insbesondere Erkenntnisse zu relevanten Personen und Personenzusammenschlüssen sowie die jeweiligen Modi Operandi. Nur auf der Basis aktueller Lagebilder können illegale Migrationsbewegungen antizipiert bzw. nachvollzogen werden.

Zu Nummer 5

Durch den Bundesnachrichtendienst aufzuklärende Bedrohungen sind auch solche durch wehrtechnisch nutzbare Technologien und dazugehörige Programme sowie aufkommende disruptive Technologien. Diese Bedrohungslage umfasst – ebenso wie die anderen Bedrohungslagen – nur solche Beeinträchtigungen, die in ihrer Wirkung eine außen- oder sicherheitspolitische Bedeutung entfalten. Zur Aufklärungsaufgabe des Bundesnachrichtendienstes gehört auch das Beobachten (wehr-)technischer Forschung und Entwicklung auf dem Gebiet neuartiger Waffentechnik und nicht-letaler Systemtechnik, die z.B. zur Förderung hybrider Bedrohungen genutzt werden kann. Aufklärungsziel des Bundesnachrichtendienstes ist ferner die Entwicklung fundamental bedeutsamer Technologien, die gegebenenfalls zur Verschiebung von staatlichen Machtgefügen oder Wirtschaftsstrukturen führen können. Bei solchen sogenannten disruptiven Technologien handelt es sich um Innovationen, die die Erfolgsserie einer bereits bestehenden Technologie, eines bestehenden Produkts oder einer bestehenden Dienstleistung ersetzen oder diese vollständig vom Markt verdrängen und die Investitionen der bisher beherrschenden Marktteilnehmer obsolet machen (so die Definition Disruptiver Technologien nach Clayton Christensen (The Innovator's Dilemma, Hrsg.: Harvard Business School Press. Boston, S. 1997; engl.: to disrupt „unterbrechen“ bzw. „stören“). Es handelt sich also um wissenschaftliche oder technische Entwicklungen, von denen erwartet wird, dass sie innerhalb der kommenden Dekaden einen prägenden oder revolutionären Einfluss, insbesondere auf Streitkräfte, Sicherheitsbehörden oder Volkswirtschaften haben werden. Aktuelle Beispiele sind Systeme maschinellen Lernens (z.B. Chat-GPT), Künstliche Intelligenz und Quantencomputing. Da „disruptive Technologien“ denkbarerweise weit zu verstehen sind, sind diesbezüglich nur Sachverhalte erfasst, die (mittelbar oder unmittelbar) erhebliche Auswirkungen auf die Bundesrepublik haben können. Dies können auch Entwicklungen in anderen Ländern, wenn hierdurch Auswirkungen – auch wirtschaftlicher Natur – für Deutschland erwachsen können (etwa durch gesellschaftliche oder wirtschaftliche Veränderungen).

Die technologischen Entwicklungen der vergangenen (wenigen) Jahre im Bereich der „Künstlichen Intelligenz“ („KI“) – hier der allgemeinen, untechnischen Terminologie folgend – zeigt bereits jetzt, dass auch aus (grundsätzlich neutralen) technischen Entwicklungen Ereignisse erwachsen können, welche die nach § 2 Absatz 2 zu schützenden Rechtsgüter erheblich bedrohen können. So können weitere Entwicklungen im Bereich KI auch mit beträchtlichen wirtschaftlichen oder gesellschaftlichen Umwälzungen (etwa durch den Wegfall einer unübersehbaren Vielzahl von Arbeitsplätzen und den hieraus erwachsenden gesellschaftlichen Spannungen) einhergehen. Sollte es zu einer exponentiellen Steigerung der Fähigkeiten von Systemen der Künstlichen Intelligenz (bis hin zu dem Einsatz von autonomen „KI-Agenten“) kommen, sind die möglichen Folgen letztlich nicht abschätzbar. KI kann als Schlüssel- und Querschnittstechnik wirken, die insbesondere die Entwicklung und Nutzung nahezu aller aufkommenden und disruptiven Technologien signifikant beschleunigt.

Da sich die technologischen Entwicklungen zum Großteil in fremden Staaten vollziehen, zum Teil in solchen Staaten, in denen eine (grund-)rechtsschonende Umsetzung kaum oder

nicht gewährleistet wird, ist das Erkennen und das Aufklären dieses Bedrohungsfeldes durch den Bundesnachrichtendienst von existenzieller Wichtigkeit, um die Handlungs- und Verteidigungsfähigkeit der Bundesrepublik Deutschland zu gewährleisten.

Zu Nummer 6

Krisenhafte Entwicklungen im Ausland können rasch zu einer Destabilisierung von Staaten oder sogar ganzen Regionen führen und damit auch Sicherheitsinteressen Deutschlands bedrohen, weshalb sie von besonderer Relevanz für die Auftragserfüllung des Bundesnachrichtendienstes sind. Multipolarität und geopolitische Machtverschiebungen sind u.a. das Resultat aus dem wachsenden politischen, wirtschaftlichen und militärischen Einfluss von Schlüsselstaaten. Die damit einhergehenden dynamischen Prozesse sind hinsichtlich der Sicherheitsinteressen Deutschlands und seiner Verbündeten insbesondere vor dem Hintergrund derer langfristigen Folgewirkungen mit krisenhaftem Entwicklungspotential, wechselseitigen Verstärkungen und Interdependenzen ein besonderes Aufklärungsziel. Krisenhafte Entwicklungen können auch langzeitige bzw. dauerhafte Krisen sein.

Der Bundesnachrichtendienst gewinnt durch unterschiedliche Aufklärungsmaßnahmen Erkenntnisse über sich zum Teil schnell zuspitzende politische Spannungen, beispielsweise aufgrund strategischer Absichten einer dominierenden militanten Opposition, über soziale Unruhen und/oder bewaffnete Auseinandersetzungen, die zu einer Änderung der politischen, gesellschaftlichen, wirtschaftlichen oder militärischen (Kräfte-)Verhältnisse führen können und daher zur Gefahr für deutsche oder europäische Einrichtungen, Staatsbürger sowie Interessen werden.

Weiterhin kann der Bundesnachrichtendienst durch Aufklärungsmaßnahmen Erkenntnisse über potentiell grenzüberschreitende Entwicklungen (Chemieunfälle, Krankheitsausbrüche, etc.) erlangen, deren Existenz oder Ausmaß nationale Regierungen unter Umständen nicht oder nur zögerlich einräumen. Dies kann auch zivile oder militärische Auseinandersetzungen zwischen zwei Staaten betreffen. Nur in Kenntnis solcher Lagen kann die Bundesregierung rechtzeitig Maßnahmen zum Schutz deutscher Staatsbürger im Ausland bzw. – je nach Reichweite des Ereignisses – der Bevölkerung in Deutschland ergreifen (z.B. Warn- und Reisehinweise, Evakuierungen oder Ausgabe von Medikamenten).

Darüber hinaus gewinnt der Bundesnachrichtendienst auch Informationen über Entwicklungen, deren Fortgang schwerste Verbrechen, die die internationale Gemeinschaft als Ganzes berühren (Völkermord, Verbrechen gegen die Menschlichkeit, Kriegsverbrechen), erwarten lassen. So entzünden sich Konflikte im Rahmen von Wahlkämpfen, Kämpfen um Ressourcen (Weideland, Zugang zu Wasser, zu staatlichen Geldern etc.) oder Kämpfen um größere Autonomie oft entlang ethnischer oder religiöser Zugehörigkeiten, was zu ethnischen Vertreibungen, bewaffneten Angriffen auf die Zivilbevölkerung etc. führen kann. Die frühzeitige Erkennung solcher Verbrechen kann auch dazu beitragen, diese zu verhindern, indem entsprechende Gegenmaßnahmen ergriffen werden. Dies liegt im Interesse der Bundesrepublik Deutschland sowie der internationalen Staatengemeinschaft. Auf Basis der Übermittlung von Erkenntnissen zu derartigen Entwicklungen und den involvierten Akteuren kann die Bundesrepublik Deutschland auf diplomatischem, politischem und wirtschaftlichem Wege Einfluss auf die Konfliktparteien nehmen. Zudem kann sie ihre Mitgliedschaft in internationalen Organisationen nutzen, um über die nationale Ebene hinaus einzuwirken.

Durch seine Aufklärungsmaßnahmen gewinnt der Bundesnachrichtendienst ferner Erkenntnisse über die Auswirkungen krisenhafter Entwicklungen im Ausland, insbesondere auch über krisenbedingte illegale Migrationsbewegungen in Richtung der Bundesrepublik Deutschland bzw. von Staaten der Europäischen Union, soweit diese nicht in organisierten kriminellen Strukturen erfolgt.

Erforderlich ist, dass die krisenhafte Entwicklung „erhebliche Auswirkungen“ auf die Bundesrepublik Deutschland haben kann. Dies soll sicherstellen, dass nicht solche

Entwicklungen die starke Indizwirkung des Bedrohungsfeldes entfalten, die in keinem Zusammenhang mit der Bundesrepublik stehen. Erfasst sind sowohl mittelbare wie unmittelbare Auswirkungen, sodass solch untergeordnete Fälle (auch infolge der Globalisierung, Entwicklungshilfe und anderer Faktoren) praktisch kaum vorstellbar sind.

Zu § 4 (Bedrohungen von herausgehobener Bedeutung)

Die Regelung des § 4 dient als zweite Qualifikationsstufe für die Durchführung besonders eingriffsintensiver Maßnahmen des Bundesnachrichtendienstes.

Zu Absatz 1

In Absatz 1 sind die tatbestandlichen Voraussetzungen der Qualifikationsstufe geregelt. Hier findet sich die Vorgabe, dass eine Bedrohung von herausgehobener Bedeutung zwei materielle Komponenten hat: Einerseits muss es sich um eine erhebliche Bedrohung handeln und zusätzlich muss dieser erheblichen Bedrohung ein erhöhtes Gefährdungspotenzial innewohnen. Dabei verschließt sich das Kriterium eines erhöhten Gefährdungspotenzials einer schematisch abschließenden Definition.

Die herausgehobene Bedeutung kann sich einerseits etwa aus der (auch und insbesondere im Vergleich zu einer erheblichen Bedrohung) besonderen qualitativen und/oder quantitativen Schwere des drohenden Schadens ergeben – vgl. Nummer 1 – sowie andererseits aus einem besonderen Ausmaß der Verdichtung der Bedrohung (Konkretisierung) – vgl. Nummer 2.

Zu Absatz 2

In den Absätzen 3 bis 5 werden durch den Gesetzgeber Bedrohungen (Bedrohungsziele, Bedrohungsfelder, Bedrohungslagen) skizziert, bei denen es nahe liegt, dass sie eine herausgehobene Gefährdung für den äußeren und inneren Frieden oder die Rechtsgüter Einzelner zur Folge haben. Die aufgeführten Bedrohungen bieten entsprechend einen Katalog starker Indizien und damit zugleich einen Rahmen, welcher als Auslegungshilfe zugleich die Bestimmtheit des Absatz 1 sicherstellt.

Die Indizien der Kataloge bezeichnen Vorgänge, welche eine herausgehobene außen- oder sicherheitspolitische Bedeutung typisieren. Dabei handelt es sich um Vorgänge, bei denen das Schadenspotential der in § 3 aufgeführten Bedrohungen oftmals derart erhöht ist, dass dies in der Gesamtbetrachtung der Umstände des Einzelfalls besonders zu berücksichtigen ist und schon alleine zu einer herausgehobenen außen- oder sicherheitspolitischen Bedeutung für die Bundesrepublik Deutschland führen kann, die auch besonders eingriffsintensive nachrichtendienstliche Maßnahmen erfordert und rechtfertigt (vgl. BVerfG, Beschluss vom 17. Juli 2024, 1 BvR 2133/22, Rn. 149). Auch diese Kriterienkataloge dienen als starke Indizien für die herausgehobene Potenzialität von Vorgängen und ist als solcher nicht abschließend, d.h. die Verwaltungspraxis bleibt offen für eine sachgerechte Einstufung anderer insbesondere auch atypischer Sachverhalte in Einzelfällen. Wie bei der Aufklärung des Bundesnachrichtendienstes insgesamt genügt für die Gewichtung der Bedrohung bereits ein auf tatsächlichen Anhaltspunkten beruhender Verdacht für die herausgehobene Bedeutung.

Zu Absatz 3

Zu Nummer 1

Unter das Bedrohungsziel der Gesamtverteidigung der Bundesrepublik wie auch der verbündeten Staaten fallen nationale Verteidigungsinteressen der Bundesrepublik Deutschland wie auch die Interessen verbündeter Staaten sowie auch Bündnisverpflichtungen in internationalen Bündnissen, an denen die Bundesrepublik Deutschland beteiligt ist, darunter insbesondere die des Nordatlantikvertrags. Insgesamt muss hier von einem weiten

Verständnis des Begriffs der Gesamtverteidigung ausgegangen werden; umfasst ist insbesondere auch die Stärkung der Fähigkeiten zur Gesamtverteidigung.

Die Gesamtverteidigung kann bei sich entwickelnden Bedrohungen der territorialen Integrität Deutschlands sowie eines Bündnispartners, bei zwischenstaatlichen Konflikten, durch fragile Staatlichkeit, durch weltweite Aufrüstung, durch Gefährdung der Informations-, Kommunikations-, Transport- und Handelslinien, durch Unsicherheiten der Rohstoff- und Energieversorgung sowie bei der Aufklärung von Gefahren aus dem Cyber- und Informationsraum betroffen sein. Auch Aufklärungsmaßnahmen fremder Staaten und insbesondere von deren Nachrichtendiensten, die ihrerseits die Maßnahmen der Bundesrepublik Deutschland und ihrer internationalen Bündnispartner aufzuklären versuchen, um anhand der erlangten Erkenntnisse Strategien zur Schwächung und bzw. oder Umgehung der vorgenannten Verteidigungsinteressen entwickeln zu können, sind Bestandteil entsprechender Bedrohungen.

Eine vergleichbare Interessenlage liegt bei Einsätzen der Bundeswehr oder verbündeter Streitkräfte im Ausland vor, z.B. bei Ausbildungsmissionen oder bei humanitären Einsätzen. Die Bundeswehr leistet im Rahmen von Einsätzen im Ausland einen wertvollen Beitrag zur weltweiten Sicherheit und Stabilität. Der Bundesnachrichtendienst ist als einziger aufklärender Auslandsnachrichtendienst der Bundesrepublik Deutschland auch zuständig für die militärische Auslandsaufklärung (vgl. auch die Ausführungen zu § 1 Absatz 1). Er kann beispielsweise Erkenntnisse unmittelbar zur Sicherheitslage und zu besonderen, situativ verschärften Bedrohung der gesundheitlichen Versorgung vor Ort und der Peripherie des Einsatzlandes gewinnen und trägt damit zur Sicherheit der eingesetzten deutschen Soldatinnen und Soldaten bei. Besonders nützlich ist die Erhebung von Einblicken in Interna von ausländischen Militär- und Sicherheitsbehörden. Lagerelevante Informationen werden regelmäßig sehr zeitnah an Vorgesetzte weitergegeben. Im Gegensatz zu offiziellen Mitteilungen, in denen Gefahren häufig verharmlost und die eigenen Erfolge in den Vordergrund gestellt werden, haben Aufklärungsmaßnahmen des Bundesnachrichtendienstes zum Ziel, einen weitgehend unverfälschten Einblick in die tatsächliche Einsatzbereitschaft und die Leistungsfähigkeit der Sicherheitskräfte sowie deren Operationsführung bzw. Vorgehen zu erlangen. Zum Schutz deutscher Soldatinnen und Soldaten ist vor allem auch die Gewinnung von Erkenntnissen zu Techniken, Taktiken und Vorgehensweisen militanter Gruppierungen, die auch gegen die Einsatzkräfte der Bundeswehr agieren können, erforderlich. Die Sicherstellung des Schutzes der Soldatinnen und Soldaten im Rahmen der sogenannten Force Protection durch Gewinnung nachrichtendienstlicher Erkenntnisse über das jeweilige Einsatzland ist eine der wesentlichen Aufgaben des Bundesnachrichtendienstes. Dies inkludiert die Aufklärung des offenen und verdeckten Wirkens staatlicher- und nichtstaatlicher Akteure im Einsatzland, deren Handlungen geeignet sind, Leib- und Leben der eingesetzten Soldaten zu gefährden, z.B. durch die Unterstützung verbündeter Gruppierungen (sogenannter Proxies), aber auch durch Maßnahmen im hybriden Spektrum, die gezielt gegen den Auftrag der deutschen und verbündeten Kräfte einschließlich der körperlichen Unversehrtheit der eingesetzten Soldatinnen und Soldaten gerichtet sind und somit das Erreichen des Einsatz- bzw. Missionszieles gefährden.

Ein weiterer Aspekt zum Schutz von Leib und Leben der im Einsatz befindlichen Soldaten und Soldatinnen ist die Aufklärung der Leistungs- und Einsatzbereitschaft der Sanitätsdienste fremder Streitkräfte sowie deren Fähigkeiten. Dieser Faktor ist für die Sicherheits- und Bedrohungslage im Einsatzgebiet maßgeblich. Hier steht zum einen die eigene medizinische Versorgung im Vordergrund. Zum anderen gehört aber auch die wehrmedizinische Forschung staatlicher und nichtstaatlicher Akteure im Ausland zu den Zielen von Aufklärungsmaßnahmen.

Auch der Schutz von Auslandseinsätzen anderer deutscher Behörden, zum Beispiel polizeilicher Einsätze im Ausland, ist eine wesentliche Aufgabe des Bundesnachrichtendienstes. Ferner übermittelt der Bundesnachrichtendienst sicherheitsrelevante Erkenntnisse zur Unterstützung der deutschen Entwicklungshilfe im Ausland, die in der Regel nur aufgrund einer Vereinbarung mit dem Einsatzland erfolgen kann. Entsprechende Einsätze finden

häufig weitab der Hauptstädte in Gebieten mit besonderen Sicherheitsrisiken statt. Auch hier liefern oftmals allein die durch die Aufklärungsmaßnahmen erlangten Erkenntnisse ein wirklich zutreffendes und hinreichend aktuelles Bild der Sicherheitslage vor Ort, welches erforderlich ist, um deutsche Entwicklungshelfer keinen unnötigen Gefahren auszusetzen bzw. notfalls Evakuierungen zu ermöglichen.

Zuletzt sind auch die in der Rahmenrichtlinien für die Gesamtverteidigung vom 5. Juni 2024 genannten Dauereinsatzaufgaben als Teil der militärischen Verteidigung in der Gesamtverteidigung (und auch im Begriff des „Einsatzes“) enthalten.

Zu Nummer 2

Bedrohungen der Funktionsfähigkeit staatlicher Einrichtungen sowie von staatlichen Einrichtungen von Mitgliedstaaten der Europäischen Union und von Bündnispartnern sind hochgradig aufklärungsbedürftig. Diese Einrichtungen sichern die Funktionsfähigkeit des Staates und schaffen damit die Voraussetzung für ein funktionierendes Gemeinwesen. Zugleich sind sie in besonderem Maße von Angriffen von ausländischen Nachrichtendiensten und fremden Mächten betroffen. Zuletzt sind sie – schon aufgrund ihrer Verzweigungen und der Begrenzungen ihrer Ressourcen – oft besonders vulnerabel. Dies gilt auch für Einrichtungen der Europäischen Union, der Vereinten Nationen oder vergleichbarer internationaler Organisationen, wobei diese zudem oftmals in besonderem Maße in Krisenregionen tätige und deshalb besonders bedroht sind.

Unter die staatlichen Einrichtungen der Bundesrepublik fällt auch der Bundesnachrichtendienst. Sicherung dieser Funktionsfähigkeit und seiner wesentlichen Fähigkeiten für die Wahrnehmung des gesetzlichen Auftrags sind insbesondere vorbereitende und absichernde Tätigkeiten des Bundesnachrichtendienstes erforderlich, wie die Herstellung, der Erhalt und der Ausbau der zur Auftragserfüllung notwendigen Methoden, Gegenstände und Instrumente – entsprechend beinhaltet die Funktionsfähigkeit explizit auch die „Eigenbefähigung“. Die Eigenbefähigung beinhaltet vorbereitende bzw. vorgelagerte Maßnahmen für den Einsatz nachrichtendienstlicher Mittel, hierunter fällt auch die Ertüchtigung von Mitarbeitenden oder die Tippgewinnung und -aufbereitung. Es handelt es sich somit um die Beschaffung von Informationen, die nicht unmittelbar der Aufgabenerfüllung im Sinn der Früherkennung von Bedrohungen dienen. Durch die notwendigen Vorbereitungs-, Begleit- und Nachbereitungsmaßnahmen erhält und weitet der Bundesnachrichtendienst sein Fähigkeitsprofil und wird in die Lage versetzt, dieses Fähigkeitsprofil nicht nur initial zu begründen und zu erhalten, sondern erforderlichenfalls auch auszubauen.

Die Bundesregierung ist auf einen modernen und innovativen Auslandsnachrichtendienst angewiesen, wobei sich die Bedingungen der Aufklärung angesichts der Fortentwicklung der Technik schnell wandeln und der Bundesnachrichtendienst vorbereitet sein muss (Kaltstartfähigkeit, Löffelmann/Zöller, Nachrichtendienstrecht, 2022, C 7). Die Eigenbefähigung stärkt somit die Ertüchtigung des Dienstes in technischer und personeller Hinsicht (vgl. Gusy, in Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 1 Rn. 39). Von der Eigenbefähigung erfasst ist daher auch die Erhebung von Informationen einschließlich personenbezogener Daten, die nicht unmittelbar der Gewinnung von Informationen mit außen- oder sicherheitspolitischer Bedeutung dient, wie zum Beispiel im Bereich Kryptologie/ Verschlüsselungstechnologien mit dem Ziel der Verbesserung der Entzifferungsfähigkeit des Bundesnachrichtendienstes: Im Bereich der Entzifferung wird anhand verschlüsselter Daten geforscht und es werden Entschlüsselungsmöglichkeiten gesucht. Gelingt es dem Bundesnachrichtendienst, erstmals eine bestimmte Verschlüsselungsmethodik zu entschlüsseln, sind die vorhandenen Daten häufig (bereits) nicht mehr relevant, sie dienen nur dazu, die Verschlüsslungsmethodik zu erkennen. Das Schritthalten mit technischen Fortentwicklungen umfasst hierbei auch die Bereitstellung und den Einsatz von digitalen Zahlungsmitteln in einem operativen Kontext. Von besonderem Interesse sind hier Kryptowährungen, insbesondere solche, die einen hohen Grad der Verschleierung zulassen.

Ebenso erfasst werden auch interne Vorbereitungen z.B. die Vorbereitung einer Maßnahme im Zusammenhang mit der Führung menschlicher Quellen (sog. HUMINT), insbesondere auch solche, die der Suche nach geeigneten Personen dienen.

Unter die Eigenbefähigung fällt ferner die Informationsgewinnung zu Forschungs- und Entwicklungszwecken. Hier liegt das rein technische Erkenntnisinteresse nicht in der Verarbeitung des einzelnen Datums, sondern in der Verarbeitung der Testdaten oder des Datentyps als solchen (vgl. hierzu auch die Begründung zu § 60). Werden für Forschungszwecke Daten erhoben, für die Verarbeitungsbeschränkungen bestehen (z.B. Daten Minderjähriger), muss eine technische Trennung der Datenhaltung von derjenigen der sonstigen Aufgabenerfüllung erfolgen, um zu gewährleisten, dass diese Daten nicht für andere Zwecke genutzt werden. Die Erhebung solcher Daten ist auch vor dem Hintergrund wichtig, dass Filter stetig weiterentwickelt und verbessert werden müssen (vgl. die entsprechenden gesetzlichen Pflichten). Will der Bundesnachrichtendienst beispielsweise ein technisches System darauf trainieren Bilder von bestimmten Personengruppen automatisch auszusortieren, so muss das System aus technischen Gründen an Echt-Daten von diesen Personengruppen trainieren.

Kritische Infrastrukturen sind Einrichtungen oder Organisationen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere gravierende Folgen eintreten würden. Hierzu zählen also alle für die Funktionsfähigkeit der Gesellschaft bedeutsamen Basisdienste. Verdeutlichend kann hier das KRITIS-Dachgesetz und die Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) herangezogen werden.

Zu Absatz 4

Zu Nummer 1

Nummer 1 betrifft die Gefährdungslage von Personen im Ausland, damit also erwartbare oder bevorstehende Gefährdungen von Leib, Leben oder Freiheit einer natürlichen Person. Die Regelung ist nicht auf deutsche Staatsangehörige begrenzt. Der Schutz der körperlichen Unversehrtheit, des Lebens und der Freiheit natürlicher Personen muss vordringlichste Aufgabe aller staatlichen Stellen sein. Die Aufklärung einer Gefahr für Leib, Leben oder Freiheit im Zuständigkeitsbereich des Bundesnachrichtendienstes kann beispielsweise bei Entführungsfällen im Ausland gegeben sein. Hier können Erkenntnisse, die aus der nachrichtendienstlichen Aufklärung erlangt werden, zusammen mit dem Erkenntnisaustausch mit anderen Nachrichtendiensten und deren Unterstützung durch eigene nachrichtendienstliche Zugänge ganz wesentlich zur Lösung solcher Fälle und damit zur unmittelbaren Rettung von Menschenleben beitragen.

Erforderlich ist, dass durch die Belange der Bundesrepublik Deutschland in besonderer Weise berührt sind. In Abgrenzung zum bisherigen § 8 Absatz 1 des Artikel 10-Gesetzes ist dabei bereits tatbestandlich angelengt, dass eine solche „Berührung“ auch mittelbar erfolgen kann; erforderlich ist also nicht, dass die Gefährdungslage das Leben von deutschen Staatsangehörigen betrifft.

Zu Nummer 2

Der Schutz der Mitarbeiterinnen und Mitarbeiter, Einrichtungen, Gegenstände oder nachrichtendienstlichen Verbindungen des Bundesnachrichtendienstes u.a. gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten (Eigensicherung) ist grundsätzlich von erheblicher Bedeutung.

Die in besonderem Maße gesteigerte Gefährdung folgt dabei aus einer ganzen Reihe von Aspekten: So sind die Mitarbeiter, Einrichtungen, Gegenstände oder nachrichtendienstlichen Verbindungen des Bundesnachrichtendienstes in gesteigertem Maße gefährdet, da

sie unmittelbar mit den Aufgaben und Erkenntnissen des Bundesnachrichtendienstes in Berührung stehen. Darüber hinaus ist gerade hier ein besonders hohes Interesse maliziöser Akteure zu erwarten, da der potentielle Erkenntnisgewinn besonders vielversprechend ist. Weiter bedingt auch die Tätigkeit des Bundesnachrichtendienstes in Krisenregionen und im Zusammenhang mit rivalisierenden Mächten eine besondere Gefährdungslage, da rechtsstaatliche Prinzipien für potentielle Angreifer ohne Belang sind. So geht von einer erfolgreichen Infiltration oder Unterwanderung des Bundesnachrichtendienstes, im Rahmen derer die Identität von Mitarbeiterinnen und Mitarbeitern oder nachrichtendienstlichen Verbindungen aufgedeckt wird, eine unmittelbare Gefahr für Leib und Leben der betroffenen Personen aus. Soweit es sich nach den Umständen eines Einzelfalls a-typischerweise um einen minderschweren Fall im Kontext der Eigensicherung handelt, ist dieser im Stufensystem dieses Gesetzes ausnahmsweise der Grundstufe der nachrichtendienstlichen Auslandsaufklärung zuzuordnen (ferner kann es sich aber natürlich auch um eine Fallkonstellation handeln, die nicht nur ein besondere Beeinträchtigung beinhaltet, sondern sogar ein erhöhtes Gefährdungspotenzial mit sich bringt und damit unter § 4 subsumiert werden kann).

Die effektive Eigensicherung des Bundesnachrichtendienstes ist somit unabdingbare Voraussetzung zur Erfüllung seines gesetzlichen Auftrags. Zugleich gebietet es die Schutzpflicht des Bundesnachrichtendienstes gegenüber seinen Mitarbeiterinnen und Mitarbeitern, alle ihm zur Verfügung stehenden, gesetzlichen Befugnisse auszuschöpfen, um einen wirksamen Schutz zu gewährleisten.

Zu Nummer 3

Nummer 3 betrifft Cyberangriffe, wobei – dies ergibt sich bereits aus der Regelungssystematik des Absatz 1 – Sachverhalte mit rein regionalem Bezug und eingeschränkter Bedeutung als Aufklärungsziele ausscheiden.

In diesem Bereich agiert eine Vielzahl von Akteuren. Auch kriminelle Angriffe durch nicht staatliche Cyberangreifer größeren Ausmaßes sind umfasst. Diese können staatlichen Angriffen in Qualität und Schadenspotential ähnlich sein. Auch gezielt gesteuerte Angriffe von staatlicher Seite sind nicht auszuschließen. Darüber hinaus werden organisierte Cyberangriffe auch zur gezielten Destabilisierung relevanter Infrastrukturen durchgeführt (sogenannter „Hacktivismus“). Ziele können dabei nicht nur die informationstechnischen Systeme staatlicher Stellen sein, sondern auch informationstechnische Systeme von Unternehmen, die etwa zum Zweck der Erzielung von Wettbewerbsvorteilen (Wirtschaftsspionage) angegriffen werden. Dabei zielt der Angriff nicht zwingend immer im engeren Sinne auf die Funktionsfähigkeit informationstechnischer Systeme, sondern kann auch die Verfügbarkeit von solchen Systemen betreffen (sog. Denial-of-Service-Attacken oder Distributed Denial-of-Service-Attacken).

Die Risiken von Cyberangriffen gewinnen in einer immer enger digital vernetzten Gesellschaft weiter an Bedeutung, weshalb der Früherkennung von Cyber-Bedrohungen ebenfalls wachsende Bedeutung zukommt. Informationstechnische Systeme besitzen in der digital vernetzten Gesellschaft, unabhängig davon, ob sie staatlich oder privat betrieben werden, für die Wahrnehmung von persönlichen, bürgerlichen und wirtschaftlichen Freiheiten eine zentrale und unverzichtbare Bedeutung. Zugleich sind solche Systeme in immer stärkerem Maße Angriffen, auch durch ausländische staatliche Akteure, mit dem Ziel ausgesetzt, diese Freiheiten zu verletzen und dadurch dem für ihren Schutz verantwortlichen Staat Schaden zuzufügen. Cyber-Angriffe terroristischer Gruppen und staatlicher Akteure – einschließlich fremder Nachrichtendienste – können auch die Störung oder Zerstörung kritischer, ziviler Infrastruktur zum Ziel haben, um die sich gegebenenfalls daraus ergebende destabilisierende Wirkung für eigene Zwecke nutzen zu können.

Cyberangriffe bergen in sich ein immenses Gefährdungspotential, so dass bereits ohne Ansehung des im Einzelfall konkret betroffenen informationstechnischen Systems der Sicherheit der informationstechnischen Systeme vor dem Hintergrund der Aufklärung von

internationalen terroristischen, staatlichen oder weiträumig orchestrierten Angriffen ein besonderes öffentliches Interesse an der Früherkennung und Aufklärung einer solchen Bedrohung zukommt. Cyberangriffen ist die Gefahr des Eintritts von Großschadenslagen immanent. Angriffe auf, ggf. sogar eine Störung der Verfügbarkeit von informationstechnischen Systemen, können insbesondere bei einer möglicherweise Vielzahl betroffener informationstechnischer Systeme oder der (Mit-)Betroffenheit von gesellschaftlich wichtigen oder sogar kritischen Infrastrukturen erhebliche Auswirkungen auf die öffentliche Sicherheit und Ordnung, bis hin zu einer Bedrohung von Leib und Leben oder des Bestandes oder der Sicherheit des Bundes oder eines Landes bewirken. Es können durch Cyberangriffe Ereignisse eintreten, die das Leben oder die Gesundheit einer großen Anzahl von Menschen, die lebensnotwendige Unterkunft sowie Versorgung der Bevölkerung, wesentliche Sachwerte oder die Umwelt erheblich gefährden oder beinträchtigen. Die Sicherheit der Informationstechnologie besitzt darüber hinaus für den Wirtschafts- und Wissenschaftsstandort Deutschland sowie für den Erhalt der freiheitlichen demokratischen Grundordnung überragende systemische Bedeutung. Je frühzeitiger Erkenntnisse erlangt werden, desto mehr Schäden (z.B. Vertraulichkeitsverlust, Datenveränderung, Verfügbarkeitsstörungen, Zerstörung) können im weiteren Verlauf bestenfalls abgewendet werden.

Zu Nummer 4

Spionagetätigkeiten, die durch andere Staaten mit langfristiger Perspektive begangen werden, bedrohen die Souveränität der Bundesrepublik Deutschland unmittelbar. Die Bedrohung hat zuletzt stark zugenommen. Auch das damit verbundene Schadenspotenzial ist angesichts der hinter den Angriffen stehenden staatlichen Akteure sehr hoch. Damit potenziert sich die Gefährlichkeit derartiger Spionageangriffe im Vergleich zu einem Einzeltäter bzw. einzelner Tätergruppen. Der mögliche Schaden, den erfolgreiche Spionageangriffe mit herkömmlichen Methoden der Informationsgewinnung oder mit elektronischen Angriffen verursachen, gefährden die politischen, militärischen und wirtschaftlichen Interessen der Bundesrepublik Deutschland massiv. Aufklärungen des Bundesnachrichtendienstes sorgen für eine höhere Erkenntnisdichte. Eine erhöhte Beobachtungsbedürftigkeit ist bei nachrichtendienstlichen Aktivitäten staatlicher Akteure generell gegeben. Daneben umfasst die Nummer auch sicherheitsgefährdende Tätigkeiten, die nicht einer geheimdienstlichen Tätigkeit für einen anderen Staat zurechenbar ist (z.B. das öffentliche Mitteilen dienstlich bekannt gewordener Informationen aus einer Art persönlichem Geltungsbedürfnis heraus). Mit umfasst sind auch solche Tätigkeiten, die sich primär gegen eine Einrichtung einer internationalen Organisation, in der die Bundesrepublik Deutschland Mitglied ist, richten, da davon auszugehen ist, dass damit auch Auswirkungen auf die Bundesrepublik Deutschland verbunden sind oder in der Zukunft verbunden sein können.

Darüber hinaus sind explizit auch solche Tätigkeiten erfasst, die (Primär-)Auswirkungen auf verbündete Staaten haben. Auch insoweit hat die Bundesrepublik ein ureigenes Interesse eine umfassende Aufklärung zu betreiben, um die Partner zu unterstützen und als wertvoller Informationstauschpartner relevant zu bleiben.

Der Begriff der Sicherheitsgefährdung ist dabei zwar weit, wird aber durch das ergänzende Tatbestandsmerkmal, dass die Tätigkeit/Struktur Auswirkungen auf die Bundesrepublik Deutschland oder Mitgliedstaaten der genannten internationalen Organisationen haben muss, eingegrenzt. Solche Auswirkungen setzen voraus, dass eine nicht nur untergeordnete Tätigkeit/Struktur vorliegt, sondern ein Gefährdungspotenzial für die sicherheit staatlicher Strukturen besteht.

Zu Absatz 5

Absatz 5 definiert zuletzt Bedrohungslagen, bei denen typischerweise ein erhöhtes Gefährdungspotenzial anzunehmen ist und welche im Rahmen der Prüfung der Qualifikation besonders zu berücksichtigen sind. Auch diese Vorgänge haben Indizwirkung, sodass immer auch Raum für atypische Sonderfälle bleibt, bei denen die Regelvermutung nicht erfüllt ist

oder auch für gesetzgeberisch nicht ausdrücklich bedachte sonstige Sachverhalte mit entsprechend hohem Gefährdungspotential.

Zu Nummer 1

Vorgänge und Bedrohungen, die im Zusammenhang mit nationalen Verteidigungsinteressen oder mit militärischen Mitteln geführten Auseinandersetzungen stehen, steigern das Risiko- und Gefährdungspotential der in § 3 genannten Bedrohungen in einer Weise, dass dann im Regelfall von einer herausgehobenen Bedeutung ausgegangen werden muss. So bekommt beispielsweise die Aufklärung von Bedrohungen mit Bezug zu wehrtechnischen Technologien und dazugehörigen Programmen (vgl. § 3 Absatz 4 Nummer 5) ein gegenüber Friedenzeiten gesteigertes Gefährdungspotential, wenn sie im Zusammenhang mit einer militärischen Auseinandersetzung steht. Gleiches gilt auch für die Verteidigungsinteressen oder militärischen Auseinandersetzungen insbesondere der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages und deren oder dessen Mitgliedstaaten.

Zu Nummer 2

Tritt einer Bedrohung eine Sachverhaltsebene hinzu, bei der naheliegt, dass sie tiefgreifende wirtschaftliche und gesellschaftliche Umwälzungen mit potentiell scherwiegenden Folgen befördern kann, ist im Regelfall von einer herausgehobenen Bedrohung auszugehen. Dies könnte beispielsweise bei Entwicklungen im Bereich der der „Künstlichen Intelligenz“ („KI“) – vgl. § 3 Absatz 4 Nummer 5 – der Fall sein wie etwa die potentiell weiter zunehmenden Möglichkeiten, auf selbstlernende und/oder automatisierte Systeme zurückzugreifen, um z.B. aus Gegenständen des auch zivilen und alltäglichen Gebrauchs sicherheitliche Bedrohungen erwachsen zu lassen (etwa durch autonome, bewaffnete Drohnen). Noch weitergehend steht indes auch zu befürchten, dass durch die absehbaren Fortschritte im Bereich der Forschung und Entwicklung im Bereich KI auch die Nachrichtendienste fremder Staaten großflächig befähigt werden, autonome Angriffe auf (informationstechnische) Infrastruktur zu initiieren.

Zu Nummer 3

Eine Gefährdung der wesentlichen auswärtigen Belange der Bundesrepublik Deutschland ist regelmäßig von höchster außen- oder sicherheitspolitischer Bedeutung. Das Grundgesetz hat die Bundesrepublik Deutschland in die internationale Gemeinschaft eingebunden und die deutsche öffentliche Gewalt programmatisch auf internationale Zusammenarbeit ausgerichtet. Um dies zu erreichen, ist der deutsche Staat darauf angewiesen, in der internationalen Gemeinschaft als angesehener, berechenbarer und verlässlicher Partner wahrgenommen zu werden (BVerfG, Urteil vom 15. Juli 2025, 2 BvR 508/21, Rn. 105). Sachverhalte, die eine Gefährdung wesentlicher auswärtiger Belange der Bundesrepublik Deutschland verursachen können, müssen daher auch mit nachrichtendienstlichen Mitteln aufgeklärt werden, die im Einzelfall besonders eingriffsintensiv für betroffene Personen sein können. Die Gefährdung von wesentlichen auswärtigen Belangen liegt insbesondere dann vor, wenn das friedliche Zusammenleben der Bundesrepublik Deutschland mit anderen Völkern oder die Beziehungen zu anderen Regierungen nicht nur unerheblich beeinträchtigt werden können (z.B.: durch hybride Einflussmaßnahmen zur Darstellung Deutschlands als nicht vertrauenswürdiger Partner). Es kommt dabei nicht darauf an, ob die Bundesrepublik Deutschland diplomatische Beziehungen zu dem betreffenden Staat unterhält.

Zu Nummer 4

Bedrohungen haben dann regelmäßig eine herausgehobene Bedeutung, wenn sie aus Vorgängen erwachsen, die im Zusammenhang mit Organisationen stehen, welche zur Zielverfolgung Straftaten begehen, die im Höchstmaß mit Freiheitsstrafe von mindestens fünf Jahren bedroht sind. Für die Annahme einer Organisation im Sinne dieses Absatzes ist keine feste oder regional etablierte Organisationsstruktur erforderlich.

So klärt der Bundesnachrichtendienst u.a. Gefährdungen aus den Bereichen der organisierten Kriminalität und des internationalen Terrorismus auf. Der Fokus des Bundesnachrichtendienstes liegt hierbei nicht auf der Aufklärung in der Bundesrepublik Deutschland; vielmehr beobachtet er zum Beispiel, wie sich Kriminelle über Staatsgrenzen hinweg organisieren oder welchen Einfluss sie auf ausländische Regierungen nehmen und wie sich dies auf die öffentliche Sicherheit der Bundesrepublik Deutschland auswirkt. Den Straftaten ist gemein, dass sie in der Regel weitere Straftaten nach sich ziehen, die einzeln oder zusammen genommen von erheblicher Bedeutung für die Sicherheit der Bundesrepublik Deutschland sind.

Beispiel für eine besonders schwere Straftat im Zusammenhang mit der Aufklärungsaufgabe des Bundesnachrichtendienstes ist der internationale Rauschgifthandel.

Erforderlich ist, dass jenseits der kriminellen Folgen auch die außen- oder sicherheitspolitischen Interessen der Bundesrepublik Deutschland durch die Bedrohungslage erheblich beeinträchtigt werden kann. Dies ist insbesondere bei der organisierten Kriminalität mit Auslandsbezügen oftmals dadurch der Fall, dass zugleich das internationale Verhältnis der Bundesrepublik zu dem jeweiligen anderen Staat beeinträchtigt werden kann; etwa, weil Deutschland nicht als schlagkräftiger Partner bei der Aufklärung grenzüberschreitender Kriminalität wahrgenommen wird.

Zu § 5 (Allgemeine Befugnisse)

§ 5 regelt die allgemeinen Befugnisse des Bundesnachrichtendienstes zur Erfüllung seiner Primäraufgabe der Informationsbeschaffung, d.h. zur Erhebung von personenbezogenen Daten. Hierbei ist noch keine besondere nachrichtendienstliche Tätigkeit angelegt, vielmehr handelt es sich um „reguläre“ Erhebungsbefugnisse, wie sie auch sonstigen Verwaltungsbehörden eingeräumt werden könnten. Demgegenüber wird der Einsatz nachrichtendienstlicher Mittel als besondere Befugnisse in Abschnitt 3 geregelt.

Eine Sonderregelung zum Einsatz von Legenden und der Herstellung und Nutzung der hierfür erforderlichen Tarnmittel für den allgemeinen Gebrauch typischerweise anlässlich von Verwaltungstätigkeiten des Bundesnachrichtendienstes findet sich in § 5 Absatz 4. Die Regelung des bisherigen § 2 Absatz 4 findet sich nunmehr in § 6.

Der bisherige § 2 Absatz 3 wurde gestrichen. Eine inhaltliche Änderung geht mit dieser Streichung nicht einher. Der bisherige § 2 Absatz 3 enthielt die deklaratorischen Sätze: „Polizeiliche Befugnisse oder Weisungsbefugnisse stehen dem Bundesnachrichtendienst nicht zu. Er darf die Polizei auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, zu denen er selbst nicht befugt ist.“ Satz 1 der Vorschrift war deshalb deklaratorisch, weil dem Bundesnachrichtendienst im vorliegenden Gesetz – abschließend – Befugnisse eingeräumt werden. Unter diesen Befugnissen befinden sich keine originär polizeilichen Befugnisse; insbesondere auch nicht in Abschnitt 4 (vgl. die Ausführungen dort). Der Satz 2 war insoweit überflüssig, als die dortige Bestimmung bereits als allgemeine gesetzliche Voraussetzung der Amtshilfe geregelt ist. Unberührt sind spezialgesetzliche Regelungen, bei denen Behörden zur Mitwirkung verpflichtet sind.

Zu Absatz 1

§ 5 Absatz 1 ist Rechtsgrundlage für die Erhebung personenbezogener Daten. Dies betrifft Erhebungen, die einen Grundrechtseingriff darstellen aber ohne den Einsatz besonderer Befugnisse wie etwa den Einsatz eines nachrichtendienstlichen Mittels erfolgen (allgemeine Befugnis zur Erhebung personenbezogener Daten). Erfasst sind darüber hinaus aber auch Datenverarbeitungen, die keinen Grundrechtseingriff darstellen (und damit grundsätzlich keiner gesonderten Ermächtigungsgrundlage bedürften). Dies umfasst insbesondere die Verarbeitung von Sachdaten sowie von personenbezogenen Daten aus öffentlich verfügbaren Inhalten, die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten oder kommerziell verfügbar sind, wie z.B. Zeitungen. Bei der

Verarbeitung solcher personenbezogenen Daten liegt kein Eingriff in Grundrechte vor, insbesondere nicht in das Grundrecht der informationellen Selbstbestimmung nach Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes. (vgl. BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07 / 1 BvR 595/07, Rn. 308).

Das Erheben kann auch in einem Entgegennehmen personenbezogener Daten von öffentlichen und privaten Stellen bestehen, sodass Absatz 1 auch die Befugnis zur Entgegennahme von personenbezogenen Daten von anderen Stellen umfasst. Dies schließt Vorgänge ein, bei denen dem Bundesnachrichtendienst personenbezogene Daten unaufgefordert übermittelt oder aufgedrängt werden, aber auch Fälle, in denen der Bundesnachrichtendienst solche Daten gezielt ankauft sowie Konstellationen, in denen der Bundesnachrichtendienst im Rahmen einer Zusammenarbeit etwa mit ausländischen Nachrichtendiensten personenbezogene Daten erhält, ohne selbst direkt an der Gewinnung der Information beteiligt zu sein.

Die Vorschrift ist zugleich auch eine für eine Übermittlung an den Bundesnachrichtendienst in Einzelfällen notwendige „Abrufregelung“ (BVerfG, Urteil vom 27. Mai 2020, 1 BvR 1873/13 u.a., Rn. 95 m.w.N.). Für inländische öffentliche Stellen ist diese Abrufregelung zwar in § 10 Absatz 1 enthalten; indes gilt § 10 nicht für inländische nicht öffentliche sowie für ausländische Stellen.

Die bisherig in der Aufzählung des § 2 enthaltenen Aufgaben des Bundesnachrichtendienstes werden nunmehr in diesem Absatz systemgerecht mit der „nachrichtendienstlichen Auslandsaufklärung“ gleichgestellt. Dabei enthält diese Aufgabe zugleich unmittelbar den Regelungsgehalt der ehemaligen Nummer 3 („für die Überprüfung der für die Aufgabenerfüllung notwendigen Nachrichtenzugänge“). Der bislang im Gesetz enthaltene Zusatz in § 2 Absatz 1 Nummer 4, „wenn sie nur auf diese Weise zu erlangen sind und für ihre Erhebung keine andere Behörde zuständig ist“, wurde gestrichen. Zudem wird der Verweis auf die „anzuwendenden Bestimmungen des Bundesdatenschutzgesetzes“ entfernt, da diese Bestimmungen bereits (normenklarer) in § 99 konkret aufgezählt werden.

Zu Absatz 2

Absatz 2 stellt die Ermächtigungsgrundlage für Datenerhebungen im Falle der systematischen Sammlung personenbezogener Daten zu einer Person dar. Dies ist dann der Fall, wenn die Person selbst im unmittelbarem Interesse der Aufklärung steht, vgl. § 20 Absatz 1, beispielsweise, weil diese eine herausgehobene Position in einem terroristischen Netzwerk einnimmt. Für das Eingriffsgewicht maßgeblich ist hier die personengerichtete Sammlung der Informationen. Eine Sammlung, die nicht auf eine Person bezogen ist, hat daher kein erhöhtes Eingriffsgewicht und richtet sich nach Absatz 1.

Die Vorschrift erfasst (auch) die Erhebung aus öffentlich/allgemein zugänglichen Quellen. Automatisierte (wie auch manuelle) Datenerhebungen aus allgemein zugänglichen Quellen können sich als Grundrechtseingriff, insbesondere als Eingriff in das Grundrecht auf informationelle Selbstbestimmung, darstellen. Ein solcher ist dann anzunehmen, wenn die aus allgemein zugänglichen Quellen stammenden personenbezogenen Daten durch ihre systematische Erhebung, Sammlung und Erfassung einen zusätzlichen Aussagewert erhalten (vgl. BVerwG, Urteil vom 21. Juli 2010 - 6 c 22/09-m, Rn. 17 mit Verweis auf BVerfG vom 11. März 2008, 1 BvR 2074/05 / 1 BvR 1254/07 sowie BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07 / 1 BvR 595/07, Rn. 309). Eine systematische Erhebung in diesem Sinn liegt z.B. vor, wenn öffentlich verfügbare Inhalte (z.B. bei Social Media-Inhalten) zielgerichtet nach Meldungen von oder zu einer bestimmten Person oder Personengruppe durchsucht werden. Die gesteigerte Intensität des von der Datenerhebung (ggf. auch automatisiert unter Verwendung selbstlernender Systeme), ausgehenden Grundrechtseingriffs wird dadurch kompensiert, dass die Erhebung mittels automatisierter Datenverarbeitung nur zulässig ist, wenn dies im Einzelfall erforderlich ist.

Zu den allgemein zugänglichen Quellen gehören etwa alle Bereiche des Internets, auch solche, die mittels einer vorgelagerten Zugangshürde geschützt sind. Die Grenze zum Einsatz eines nachrichtendienstlichen Mittels ist dann überschritten, wenn die eingesetzten Schutzmechanismen über rein formale Hürden hinausgehen und eine tatsächliche nicht unerhebliche Zugangsbeschränkung bewirken, welche geeignet ist, unbefugten Dritten den Zugriff spürbar zu erschweren. Allein die Verwendung individualisierter Zugangsdaten sowie auch die Möglichkeit einer Registrierung ohne reale Verifizierung stellen noch keinen Einsatz eines nachrichtendienstlichen Mittels dar. Eine wirksame Zugangshürde liegt ebenfalls nicht vor, wenn der Zugriff auf die personenbezogenen Daten allein durch die Kenntnis technischer Zugriffsinformationen, wie etwa einer URL ermöglicht wird.

Zu Absatz 3

Zur Erfüllung seiner Aufgaben darf der Bundesnachrichtendienst personenbezogene Daten auch mittels einer (automatisierten) Anwendung erheben, welche einen biometrischen Abgleich vorhandener personenbezogenen Daten mit öffentlichen Daten durchführt. Auch bei dieser Befugnis handelt es sich nicht um den Einsatz eines nachrichtendienstlichen Mittels im Sinne des Abschnitt 3. Die hier geregelte Befugnis betrifft dabei ausschließlich die Erhebung durch Abgleich mit öffentlich zugänglichen Daten. Soweit der Bundesnachrichtendienst im Rahmen seiner Befugnisse zum Einsatz nachrichtendienstlicher Mittel biometrische Daten einsetzt – etwa im Rahmen der strategischen Aufklärung – so ist dieser Einsatz durch die Befugnis zum Einsatz des jeweiligen Mittels mit umfasst.

Ausgangspunkt des Abgleichs nach diesem Absatz ist ein biometrisches Datum, beispielsweise ein Fahndungslichtbild. Dieses Ausgangsdatum kann in der Folge für einen biometrischen Abgleich mit allgemein zugänglichen, also öffentlich verfügbaren Daten aus dem Internet verwendet werden. Unter einem biometrischen Abgleich im Sinne der Vorschrift ist die technisch gestützte Überprüfung der Übereinstimmung von biometrischen Signaturen mit dem Ergebnis einer Übereinstimmungsbewertung zu verstehen. Zur Frage, wann Daten als allgemein/öffentlich zugänglich zu betrachten sind, siehe oben (zu Absatz 2). Hier ist ein spezifisches Begriffsverständnis für den Bundesnachrichtendienst anzulegen, welches sich schon aus dem Tätigkeitsschwerpunkt im Ausland ergibt.

Zweck des Abgleichs ist, dass der Bundesnachrichtendienst neue Erkenntnisse zu Personen gewinnen kann, zu denen ihm biometrische Daten – etwa Passfotos – vorliegen. Dies ist von großer Relevanz, um etwa die verdeckten Reisebewegungen von Personen aus dem nachrichtendienstlichen Umfeld (z.B. ein ausländischer Spion), der internationalen Kriminalität (z.B. ein gesuchter Kriegsverbrecher) oder dem Gefährdermilieu (z.B. ein islamistischer Terrorist) aufzuklären, die häufig auf falsche (gefälschte) Ausweispapiere zurückgreifen können.

Um sicherzustellen, dass datenschutzrechtliche Standards nicht über die Gebühr strapaziert werden, ist der Abgleich nach Satz 2 vornehmlich durch den Bundesnachrichtendienst selbst, eine inländische Stelle oder eine Stelle eines Mitgliedsstaates der Europäischen Union durchzuführen. Nur wenn dies nicht gleich effektiv möglich ist, darf auf eine öffentliche oder nichtöffentliche Stelle (bzw. auf eine Anwendung einer solchen Stelle) zurückgegriffen werden. Dabei ist es nicht erforderlich, dass der Bundesnachrichtendienst vor jedem Abgleich prüft, ob es ein für den Abgleich geeignetes Produkt einer inländischen Stelle oder einer Stelle eines Mitgliedsstaates der Europäischen Union gibt. Vielmehr ist es hinreichend, dass der Bundesnachrichtendienst turnusmäßig (etwa jährlich) überprüft, ob und inwieweit die (eigenen/inländischen/europäischen) technischen Möglichkeiten einen Verzicht auf außereuropäische Lösungen ermöglicht.

Die gesteigerte Eingriffsintensität der Datenerhebung wird einerseits dadurch kompensiert, dass in Satz 3 eine nachträgliche Einzelfallprüfung auf die Erforderlichkeit der jeweils erhobenen Daten für die nachrichtendienstlichen Auslandsaufklärung vorgeschrieben ist. Andererseits findet sich in Satz 4 die Maßgabe einer besonderen datenschutzrechtlichen Prüfung

der Erhebung durch den Unabhängigen Kontrollrat. Diese hat – insoweit eine gesetzliche Vorgabe für die anlasslose Strukturprüfung durch das administrative Kontrollorgan des Unabhängigen Kontrollrates definierend – alle zwei Jahre zu erfolgen. Zu prüfen ist dabei (nur) die Vereinbarkeit der Erhebung der jeweiligen Daten mit den hier getroffenen datenschutzrechtlichen Vorgaben, nicht die Schritte ihrer Weiterverarbeitung und/oder Übermittlung.

Zu Absatz 4

Absatz 4 Satz 1 regelt den Einsatz von Legenden und die Herstellung und Nutzung der hierfür erforderlichen Tarnpapieren (z.B. Einsatz einer Legende durch Mitarbeitende des Bundesnachrichtendienstes im Rahmen der Verwaltungstätigkeit der Behörde).

Die Nutzung einer Legende fällt auch unter diese Regelung, wenn diese nur der Verschleierung der Identität des Bundesnachrichtendienstes dient, z.B. beim Abschluss von privatrechtlichen Verträgen wie dem Ankauf von Gegenständen oder Daten, die auf dem freien Markt verfügbar sind, aber nur einem eingeschränkten Käuferkreis angeboten werden. Auch die Überwindung einer Zugangsbeschränkung bei der Nutzung von Plattformen oder sozialen Medien durch die Verwendung einer Legende ist nach Satz 1 zulässig, solange diese nur zur Öffnung des Zugangs, aber nicht zu weiteren Tätigkeiten, z.B. zur aktiven Gesprächsführung, verwendet wird.

Die Befugnisnorm beinhaltet zugleich die korrespondierende Rechtfertigung, die erforderlich ist, um etwa die Verwendung von falschen Ausweispapieren (§ 281 StGB) zu rechtfertigen. Erfasst ist auch der Einsatz zum Schutz von ehemaligen nachrichtendienstlichen Verbindungen. Satz 3 enthält eine systematische Klarstellung.

Zu § 6 (Allgemeine Vorgaben)

§ 6 enthält allgemeine Vorgaben, welche für die in den Abschnitten 2 und 3 enthaltenen besonderen Befugnisse des Bundesnachrichtendienstes zur Datenerhebung insgesamt gelten.

Zu Absatz 1 und Absatz 2

Die Absätze 1 und 2 entsprechen dem bisherigen § 2 Absatz 4, wobei in Absatz 1 klargestellt wird, dass das Gebot der Verhältnismäßigkeit im Rahmen der Aufgabenerfüllung durch den Bundesnachrichtendienst insgesamt gilt. Bei Auswahl einer Maßnahme hat der Bundesnachrichtendienst sicherzustellen, dass die Erforschung des Sachverhalts auf keine andere, die betroffene Person oder ein rechtlich geschütztes öffentliches Interesse weniger beeinträchtigende Weise mit verhältnismäßigem Aufwand und unter Wahrung operativ-sicherheitlicher Interessen möglich ist. So liegt im Vergleich zur Erforschung eines Sachverhalts mittels des Einsatzes von nachrichtendienstlichen Mitteln eine geringere Beeinträchtigung in der Regel vor, wenn die Informationen in vergleichbarer Güte auch aus allgemein zugänglichen Quellen erlangt werden können. Bei der Auswahl nachrichtendienstlicher Mittel ist weiter anzunehmen, dass auch ein Auskunftsersuchen oder -ersuchen (z.B. eine Anfrage bei nationalen Staatsanwaltschaften und Polizeien sowie andere nationalen Behörden um Übermittlung relevanter Informationen) in der Regel zu einer geringeren Beeinträchtigung führt. Dieser regelmäßige Vorrang der Auskunftsanfrage gilt dabei nur gegenüber deutschen öffentlichen Stellen, da offizielle Anfragen im Ausland ggf. möglich wären, aber einerseits im Regelfall keine Verpflichtung ausländischer Stellen zur Beantwortung besteht und andererseits dies das Interesse des Bundesnachrichtendienstes an einer aufzuklärenden Person gegenüber einem fremden Staat und damit auch dessen Nachrichtendiensten offenlegen würde.

Ergänzt wurde die Regelung um die klarstellende Vorgabe, dass die Maßnahme unverzüglich zu beenden ist, wenn ihr Zweck erreicht ist oder sich offenbart, dass er nicht oder nicht auf diese Weise erreicht werden kann.

Absatz 1 Satz 2 greift zudem die Regelung des bisherigen § 8 Absatz 2 Satz 2 BVerfSchG auf. Für die Datenerhebung mit dem verbundenen Eingriff in die informationelle Selbstbestimmung oder besondere Privatheitsrechte (wie Artikel 13 GG) begründen bereits die Erhebungsbefugnisse eine solche Befugnis zum Individualrechtseingriff. Zudem enthält § 18 Absatz 1 Satz 1 eine besondere Befugnis in Bezug auf den Sachbesitz. Dabei gilt dem Grunde nach: Soweit die an der Erfüllung des gesetzlichen Auftrags des Bundesnachrichtendienstes beteiligten Personen im Rahmen ihrer gesetzlichen Befugnisse tätig werden, handeln sie nicht rechtswidrig. Hierunter fallen alle diejenigen Tätigkeiten insbesondere von Mitarbeiterinnen und Mitarbeitern des Bundesnachrichtendienstes, die im Zusammenhang mit dem Einsatz nachrichtendienstlicher Mittel erfolgen, also auch diejenigen vorgelagerten oder nachgelagerten Tätigkeiten, die für den Einsatz des nachrichtendienstlichen Mittels notwendig sind. Dies gilt auch bei der Ausübung der Befugnis nach § 5 Absatz 4. Auch Individualrechtseingriffe sind gerechtfertigt, wenn sie im Rahmen von konkreten Befugnissen des BND-Gesetzes erfolgen, z.B. die in § 18 Absatz 1 geregelte Inbesitznahme von Sachen. Gleiches gilt für vergleichbare (auch erweiterte nach Abschnitt 4) ND-Mittel. § 6 Absatz 1 und 2 beschränkt diese Rechtfertigung mit der Verhältnismäßigkeits- bzw. Erforderlichkeitsmaßgabe und schließt sie für evident unangemessene Folgen aus. Personell gerechtfertigt handeln die am Einsatz Beteiligten.

Die Regelung in Absatz 1 Satz 2 greift den bisherigen § 8 Absatz 2 Satz 2 des Bundesverfassungsschutzgesetzes auf. Diese öffentlich-rechtliche Befugnis stellt zugleich einen umfassenden Rechtfertigungstatbestand dar und ist insbesondere bei der Kollision mit ordnungsrechtlichen Vorschriften ebenso wie für das Strafrecht bedeutsam (vgl. BT-Drs. 18/4654, S. 25), stellt aber auch unter anderem auch einen Rechtfertigungsgrund in Bezug auf öffentlich-rechtliche und zivilrechtliche (z.B. urheberrechtliche) Vorgaben dar. Soweit der Bundesnachrichtendienst sowie die an der Erfüllung des gesetzlichen Auftrags des Bundesnachrichtendienstes beteiligten Personen im Rahmen ihrer gesetzlichen Befugnisse tätig werden, handeln sie nicht rechtswidrig. Hierunter fallen alle diejenigen Tätigkeiten von Mitarbeiterinnen und Mitarbeitern des Bundesnachrichtendienstes, die insbesondere im Zusammenhang mit dem Einsatz nachrichtendienstlicher Mittel erfolgen, also auch diejenigen vorgelagerten oder nachgelagerten Tätigkeiten, die für den Einsatz des nachrichtendienstlichen Mittels notwendig sind.

Auch Individualrechtseingriffe sind gerechtfertigt, wenn sie im Rahmen von konkreten Befugnissen des BND-Gesetzes erfolgen, wie z.B. die in § 18 Absatz 1 geregelte Inbesitznahme von Sachen. Gleiches gilt für die Anwendung anderer nachrichtendienstlicher Mittel sowie auch von erweiterten nachrichtendienstlichen Maßnahmen nach Abschnitt 4. § 6 Absatz 1 und 2 beschränkt diese Rechtfertigung mit der Verhältnismäßigkeits- bzw. Erforderlichkeitsmaßgabe und schließt sie für evident unangemessene Folgen aus.

Zu Absatz 3

In Absatz 3 ist eine Ausnahme von dem diesem Gesetz inhärenten Grundsatz geregelt, dass die Datenerhebung durch Maßnahmen gegen sich im Bundesgebiet aufhaltende Personen und Personen mit deutscher Staatsangehörigkeit nur unter erhöhten Voraussetzungen zulässig ist. Dabei wird es eine absolute Ausnahme darstellen, dass eine Person mit deutscher Staatsangehörigkeit eine hoheitliche Aufgabe für einen fremden Staat ausübt. Wie der Fall eines österreichischen ehemaligen Managers, welcher später für ausländische Geheimdienste tätig wurde, zeigt, stellt die Möglichkeit einer Einreise eines Agenten mit (auch) deutscher Staatsangehörigkeit, der im Rahmen seiner Spionagetätigkeit für einen fremden Staat nicht auf den erhöhten Grundrechteschutz eines deutschen Staatsangehörigen vertrauen können soll, gleichwohl eine besonders gefährliche und damit regelungsbedürftige Konstellation dar.

Dabei beziehen sich diese „besonderen Voraussetzungen“ nicht nur auf die materiell-rechtlichen Schwellen, sondern auch auf Verfahrensvorgaben wie insbesondere auf das Erfordernis einer der Vorabkontrolle unterfallenden Anordnung – auch insoweit ist in den hier

genannten Ausnahmefällen auf die Voraussetzungen abzustellen, die gegenüber einer Ausländerin / einem Ausländer im Ausland gelten.

Dieser Grundsatz gilt dann nicht, wenn die betroffene Person hoheitliche Aufgaben einer fremden Macht wahrnimmt (womit neben ausländischen Staaten insbesondere auch quasi-staatliche Strukturen gemeint sind, die etwa im Bereich von Revolutionsregimen, Terrorstrukturen wie dem „Islamischen Staat“ (IS), „Kalifate“ und Clanstrukturen oder bei den anarchisch regierten Gebietsteilen von „failed states“ anzutreffen sind). In diesem Fall gelten stattdessen diejenigen Voraussetzungen, soweit sie in der jeweiligen Erhebungsbefugnis vorgesehen sind, die beim Einsatz des nachrichtendienstlichen Mittels gegen eine Person gelten würden, die sich nicht im Bundesgebiet aufhält.

Der Begriff der „Wahrnehmung hoheitlicher Aufgaben“ ist dabei funktional zu verstehen. Entscheidend ist nicht, ob der Person oder den Personen ein Amt übertragen wurde oder sie im formalen Staatsapparat eingebunden sind – letzteres wäre bei den hier als „fremde Mächte“ bezeichneten quasi-staatlichen Strukturen faktisch auch schwerlich möglich - vielmehr sind auch solche Personen erfasst, die typische hoheitliche Aufgaben wahrnehmen, aber aus innerstaatlichen Gründen als vermeintliche Privatperson agieren. Dies schließt insbesondere aber nicht ausschließlich private, paramilitärische Organisationen wie etwa die „Gruppe Wagner“ oder ähnliche Gruppierungen ein, die militärische Aufgaben wahrnehmen. Eine pauschale, abschließende Beurteilung, ob eine „Wahrnehmung hoheitlicher Aufgaben“ vorliegt, verbietet sich insoweit. Maßgeblich ist stattdessen eine Einzelfallbetrachtung, wobei eine Reihe von Faktoren zu berücksichtigen ist: etwa die personelle oder ausrüstungsbezogene Verstrickung mit dem betreffenden Staat, die Finanzierungsgrundlage der Tätigkeit, der Umstand, dass eine Gruppierung ausschließlich für einen bestimmten Staat tätig ist, oder ob es sich bei der Tätigkeit um eine solche handelt, die typischerweise staatlichen Organen übertragen wird. Ebenfalls erfasst wären etwa ausländische Agenten, welche in Deutschland ein Attentat auf einen Oppositionellen ausführen sollen. Da solche Fälle in der Vergangenheit sowohl in Deutschland wie auch in anderen europäischen Ländern bereits aufgetreten sind, handelt es sich hierbei keineswegs um ein bloß theoretische Möglichkeit, sondern um eine manifeste Bedrohung, der begegnet werden muss.

Im Rahmen der verfassungsrechtlichen Bewertung sind eine Reihe von Faktoren zu berücksichtigen, welche die Eingriffsintensität nachrichtendienstlicher Maßnahmen gegenüber solchen Personen mindern oder kompensieren und die Behandlung dieser Personen „wie Ausländer im Ausland“ rechtfertigen. Zunächst und zuvorderst richtet sich die Aufklärung durch den Bundesnachrichtendienst insoweit nicht auf die private Lebensführung der betroffenen Person, sondern auf die Ausübung der ihr übertragenen hoheitlichen Aufgaben. Diese Aufgaben entstammen gerade dem Pflichtenkreis einer ausländischen Staatsgewalt, sodass der Inlandsbezug insoweit bereits – jedenfalls bezüglich der aufgeklärten Tätigkeit – aufgelöst wird. Den betroffenen Personen ist zugleich in erhöhtem Maße bewusst, dass ihre Tätigkeit für andere Staaten von besonderer Relevanz ist und diese denkbarerweise auch nachrichtendienstliche Mittel einsetzen, um ihre Tätigkeit aufzuklären. Weiter ist die ohnehin bei nachrichtendienstlicher Tätigkeit gegen ausländische Personen stark eingeschränkte Gefahr operativer Folgemaßnahmen bei Personen, die hoheitliche Aufgaben wahrnehmen, in einem Maße verringert, welches über die Behandlung von „regulären“ Inländern hinausgeht. So ist es bereits aus faktisch-politischen Gründen in aller Regel nicht zu besorgen, dass der deutsche Staat unmittelbar belastende Folgemaßnahmen gegen Personen unternimmt, die hoheitliche Aufgaben wahrnehmen. Zuletzt ist zu berücksichtigen, dass das Aufklärungsinteresse des Bundesnachrichtendienstes gegenüber diesen Personen gerade mit Blick auf ihre hoheitlichen Aufgaben besonders hoch ist, da gewonnene Erkenntnisse ihrerseits in besonderem Maße für die durch die Aufklärungsarbeit des Bundesnachrichtendienstes geschützten besonders gewichtigen Rechtsgüter relevant sind.

Um sicherzugehen, dass der Einsatz von nachrichtendienstlichen Mitteln gegen solchen Personen verhältnismäßig bleibt, ist eine Aufklärung nur dann zulässig, wenn Erkenntnisse erlangt werden sollen, die im Zusammenhang mit der Ausübung der hoheitlichen Aufgaben

durch die betroffenen Personen stehen. Hierdurch ist sichergestellt, dass der Einsatz der nachrichtendienstlichen Mittel nicht auf die private Lebensführung von Personen gerichtet ist, die nicht im Zusammenhang mit der Ausübung der hoheitlichen Tätigkeit steht. Zudem ist eine Betrachtung nach dieser Maßgabe nicht starr, sondern berücksichtigt den Umstand, dass in Fällen, in denen z.B. ein autokratischer Machthaber die Geschicke eines Staates dominiert, eine deutlich engere Verquickung von Privatem und hoheitlicher Machtausübung besteht als bei einer Person mit geringerer hoheitlicher Verantwortung und/oder beherrschender Stellung.

Zu Absatz 4

In Absatz 4 ist eine weitere Ausnahme von den erhöhten Eingriffsvoraussetzungen für Personen vorgesehen, die sich im Bundesgebiet aufhalten. Anders als in Absatz 3 knüpft diese Regelung dabei schon aufgrund ihrer örtlichen Bezugnahme nicht an die Staatsangehörigkeit an, sondern betrifft Fällen der „rein örtlichen Nacheile“, bei denen also bereits eine Anordnung zur Durchführung einer nachrichtendienstlichen Maßnahme erfolgt ist, bevor die Person ins Bundesgebiet einreist.

Die erhöhten Voraussetzungen bei nachrichtendienstlichen Mitteln gelten in diesen Fällen für einen Zeitraum von höchstens 72 Stunden nicht; vielmehr gilt eine bereits bestehende Anordnung auch bei Grenzübertritt fort. In diesen Fällen – in denen häufig bloße Zwischenstopps auf deutschem Hoheitsgebiet vorliegen – ist das Näheverhältnis zur deutschen Hoheitsgewalt, insbesondere die Wahrscheinlichkeit operativer Anschlussmaßnahmen reduziert, sodass eine Behandlung der betroffenen Personen „wie deutsche Staatsangehörige“ aufgrund einer besonderen Nähe zur deutschen Staatsgewalt entbehrlich ist. Selbst wenn es zu nachrichtendienstlichen Maßnahmen kommen sollte – etwa durch technische Mittel im Transitbereich eines Flughafens – ist für die betroffene Person bereits aufgrund der faktischen zeitlichen Umstände nicht zu erwarten, dass eine nachrichtendienstliche Auswertung und anschließende Übermittlung an eine inländische Behörde mit operativen Anschlussbefugnissen rechtzeitig erfolgen wird, um die besondere Schutzbedürftigkeit, die mit der tatbestandlichen Verschärfung für sich im Bundesgebiet aufhaltende Personen einhergeht, zu begründen.

Die Fallgruppe ist erforderlich, um der Gefahr der Entsendung von Agenten fremder Mächte zu begegnen (vgl. hierzu bereits Absatz 3), welche in das Bundesgebiet nur für kurze Zeit einreisen, etwa um einen politischen Anschlag zu begehen. Der Zeitraum von 72 Stunden orientiert sich entsprechend an der wahrscheinlichen Verweildauer der mutmaßlichen Attentäter von Salisbury im Vereinigten Königreich (versuchter Mord an Sergei und Yulia Skripal). Zudem soll die Vorschrift dem Umstand begegnen, dass eine laufende Maßnahme gegenüber einem hochwertigen Ziel mit Grenzübergang unterbrochen werden muss. Dies ist insbesondere deshalb geboten, weil in diesen Fällen regelmäßig auch keine andere geeignete Stelle zur Verfügung steht, um die Maßnahme fortzuführen (insbesondere scheidet eine Übergabe des Sachverhalts an inländische öffentliche Stellen regelmäßig aufgrund der Kurzfristigkeit oder deshalb aus, weil die Maßnahme auf nachrichtendienstlichen Informationen ausländischer Partner basieren, die nicht ohne deren Einverständnis geteilt werden dürfen).

Zu Abschnitt 2 (Datenerhebung unter Mitwirkung anderer Stellen)

Die Regelung von Datenerhebungen durch den Bundesnachrichtendienst, die unter Mitwirkung anderer Stellen erfolgt, dient der weiteren Entkopplung des BND-Gesetzes vom Bundesverfassungsschutzgesetz. Normenklare Regelungen im BND-Gesetz lösen die bisher bestehenden Verweise auf das Bundesverfassungsschutzgesetz ab. Aus der Überschrift dieses Abschnitts ergibt sich jedoch nicht, dass nicht auch bei in anderen Abschnitten geregelten Befugnissen im Einzelfall andere Stellen im In- oder Ausland mitwirken dürfen.

Geregelt sind in diesem Abschnitt nunmehr sowohl die Übermittlungen an den Bundesnachrichtendienst als auch Auskunftsersuchen gegenüber öffentlichen Stellen oder gegenüber verpflichteten Dienstleistern. Dabei wurde die Systematik des Gesetzes vereinheitlicht und klarer strukturiert. Hierbei wurden auch die Begrifflichkeiten angepasst: So wird nunmehr zur Vermeidung unnötiger Differenzierungen der Begriff des „Auskunftsersuchens“ einheitlich für die vormals als Auskunftsersuchen (bei öffentlichen Stellen) und Auskunftsverlangen (bei nicht öffentlichen Stellen) verwendet, die dabei aber weiter getrennten Regelungsregimen unterliegen (vgl. Unterabschnitt 2 für die Auskunftsersuchen gegenüber öffentlichen Stellen und Unterabschnitt 3 für die Auskunftsersuchen gegenüber nicht öffentlichen Stellen).

Entsprechend der Systematik bei den neu eingefügten Befugnisnormen zu den nachrichtendienstlichen Mitteln werden unterschiedliche Voraussetzungen festgelegt, die – entsprechend der oben dargestellten Stufensystematik – an der jeweiligen Aufklärungsbedürftigkeit der Vorgänge (Qualifizierung der Bedrohungen für die zu schützenden Rechtsgüter) anknüpfen. Mit der so verbesserten Systematisierung der Befugnisse nach Eingriffsgewicht geht die erleichterte praktische Anwendung bereits bestehender gesetzlicher Möglichkeiten einher. Zudem schafft die klare Abstufung der Befugnisse ein verständliches System der Eingriffsintensität einzelner Maßnahmen.

Die bei Auskunftsersuchen bisher aufgrund der Verweisungen in den bisherigen § 3 Absatz 1 und § 4 Absatz 5 Satz 3 auf § 8b Absatz 3 Bundesverfassungsschutzgesetz bestehenden Unterrichtungspflichten an das Parlamentarische Kontrollgremium wurden nicht in diesem Abschnitt aufgenommen, sondern in die zentrale Vorschrift für Unterrichtungspflichten an das Parlamentarische Kontrollgremium in § 96 verschoben.

Zu Unterabschnitt 1 (Allgemeine Befugnisse und Vorgaben für die Datenerhebung unter Mitwirkung anderer Stellen)

Zu § 7 (Befugnis zur Datenerhebung unter Mitwirkung anderer Stellen)

In § 7 findet sich die zentrale Vorschrift für die Befugnis des Bundesnachrichtendienstes, Dritte um Übermittlung personenbezogener Daten zu ersuchen.

Zu Absatz 1

Adressat von Auskunftsersuchen nach § 7 Absatz 1 Satz 1 sind „andere Stellen“. Dieser Begriff entspricht inhaltlich dem „Dritten“ der Definition in Artikel 4 Nummer 10 der Datenschutz-Grundverordnung (EU), umfasst also jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten. Die Regelung trifft mithin allgemeine Vorgaben für die Datenerhebung sowohl bei öffentlichen wie auch nicht-öffentlichen Stellen.

Für den Bereich der öffentlichen Stellen entspricht die Regelung in Satz 1 dem bisherigen § 18 Absatz 3 Satz 1 des Bundesverfassungsschutzgesetzes, wobei die Eingriffsschwelle nunmehr der Systematik des BND-Gesetzes angepasst wurde (erforderlich zumindest zur nachrichtendienstliche Auslandsaufklärung) Die Formulierung folgt mit dem Erfordernis der Einzelfallerforderlichkeit neuerer Praxis (vgl. etwa den bisherigen § 8d des Bundesverfassungsschutzgesetzes), die eine anlasslose, nur final angeleitete und begrenzte Erhebung „ins Blaue“ bzw. „auf Vorrat“ ausschließt (vgl. BVerfG, Beschluss vom 27. Mai 2020, 1 BvR 1873/13 u.a., Rn. 218 mwN). Nicht verschlossen wird hierdurch, Ersuchen anlassbezogen auch als Dauerersuchen oder für bestimmte Anlässe generell formuliert zu stellen. Das Erfordernis der Erforderlichkeit zur Aufklärung schließt im Übrigen nicht nur Informationen über die Bedrohungen selbst ein, sondern beispielsweise auch über die der Aufklärung dienenden Informationszugänge und –mittel, etwa bei der Überprüfung der

Nachrichtenehrlichkeit einer Person in Bezug auf ihren Einsatz oder Verwendung als nachrichtendienstliche Verbindung.

Sätze 2 und 3 übernehmen den bisherigen § 8 Absatz 1 Sätze 2 und 3 des Bundesverfassungsschutzgesetzes.

Zu Absatz 2

In Absatz 2 wird im Interesse der Normenklarheit spiegelbildlich zur Erhebung zugleich die Übermittlungszulässigkeit für die „Dritten“ des Absatz 1 geregelt. Hierbei erfolgt eine Begrenzung auf inländische Stellen, da der deutsche Gesetzgeber nur für solche eine Regelung treffen kann. Soweit besondere gesetzliche Übermittlungsschranken bestehen, gehen diese dabei jedoch vor. Besondere Regelungen in diesem Sinn sind Vorschriften, die speziell die Übermittlung an den Bundesnachrichtendienst regeln (z.B. § 5 Absatz 5 Nummer 2 und 6 Satz 1 Nummer 3 des BSI-Gesetzes) oder die eine gerade abschließende Regelung (auch gegenüber Nachrichtendiensten des Bundes) treffen, indem allgemeine verfassungsrechtliche Vorgaben der Weiterverarbeitung fachrechtlich abweichungsfest umgesetzt werden (z.B. § 12 Absatz 3 des Bundeskriminalamtgesetzes). Dazu zählen auch berufliche Verschwiegenheitspflichten, die auch gegenüber Sicherheitsbehörden gelten (z.B. § 43a Absatz 2 Bundesrechtsanwaltsordnung).

Angesichts der die Übermittlung einschließenden Regelung (in der sich beide Elemente der „Doppeltür einer Übermittlung“ wiederfinden) beschränkt sich die Prüfungsverantwortung der ersuchten Stelle ebenso auf solche gesetzliche Übermittlungsregelungen ihres Fachrechts, die in der vorstehend beschriebenen Weise der Übermittlung entgegenstehen. Ist die Übermittlung von einem Ersuchen veranlasst, trägt die ersuchende öffentliche Stelle (also der Bundesnachrichtendienst) allgemein die grundsätzliche Verantwortung für die Zulässigkeit der Übermittlung, die ersuchte Stelle prüft sodann folgerichtig nur, dass im Ersuchen auf die Aufgabe des Bundesnachrichtendienstes – also auf die nachrichtendienstliche Auslandsaufklärung – Bezug genommen ist (ohne nähere Spezifizierung, die regelmäßig unter Geheimschutzerwägungen ohnehin nicht in Betracht kommt) und im Übrigen solche besonderen Rechtsvorschriften ihres Fachrechts, die ausnahmsweise der bereichsspezifischen Übermittlungsregelung des Absatzes 2 aus den dargestellten Gründen noch vorgehen (vgl. § 15 Absatz 2 Satz 2 und 3 des Bundesdatenschutzgesetzes 1990).

Das bisherige Dokumentationserfordernis nach § 18 Absatz 5 des Bundesverfassungsschutzgesetzes zu Übermittlungsersuchen an Behörden wird nicht aufgegriffen. Das Gesetz bezweckt auch Bürokratieentlastung, um dafür gebundene Ressourcen besser für die gesetzliche Aufgabenerfüllung des Bundesnachrichtendienstes einzusetzen. Eine generelle Dokumentationspflicht ist nicht geboten (vgl. BVerfG, Beschluss vom 27. Mai 2020, 1 BvR 1873/13 u.a., Rn. 218). Dass wesentliche Vorgänge aktenkundig zu machen sind, ergibt sich allgemein aus dem rechtsstaatlichen Grundsatz der Aktenmäßigkeit der Verwaltung, ohne dass dies einer fachgesetzlichen Bekräftigung bedürfte. Dies gilt gleichermaßen für das Verwaltungshandeln nach dem BND-Gesetz. Festgehalten wird hingegen an der speziellen Regelung von Dokumentationspflichten bei besonderen Fällen in den diese betreffenden Spezialregelungen.

Zu § 8 (Mitteilungs- und Benachteiligungsverbot)

Zu Absatz 1

Die Regelung übernimmt die bisher speziell in § 8b Absatz 4 und 5 des Bundesverfassungsschutzgesetzes geregelten Pflichten. Diese waren bislang auf Auskunftsersuchen gegenüber nichtöffentlichen Stellen beschränkt. Die hier geregelten Pflichten werden indes, da sie für Auskunftsersuchen allgemein gelten sollen, in den allgemeinen Teil der Datenerhebung unter Mitwirkung anderer Stellen überführt (vgl. bereits die allgemeine Regelung in § 57 Absatz 5 des Bundesdatenschutzgesetzes). Dies dient auch dem Schutz der betroffenen Person (Nummer 2), da das allgemeine Benachteiligungsverbot grundsätzlich auch für

öffentliche Stellen gelten sollte. Auch insoweit erfolgt eine Begrenzung auf inländische Stellen, da der deutsche Gesetzgeber für ausländische Stellen keine (bußgeldbewehrte) Regelung treffen kann.

Zu Nummer 1

Nummer 1 übernimmt die bisherige Regelung aus § 8b Absatz 4 Satz 2 des Bundesverfassungsschutzgesetzes und wahrt die grundsätzlich gebotene Vertraulichkeit der Tätigkeit des Bundesnachrichtendienstes allgemein. Die Regelung geht als lex specialis allgemeinen Mitteilungsregelungen wie etwa § 111 Absatz 2 Satz 3 des Bundesbeamtengesetzes vor. Der letzte Halbsatz verdeutlicht, dass dies auch gegenüber Verdachtsmeldepflichten an Behörden gilt. Ersucht der Bundesnachrichtendienst beispielsweise eine Bank um Finanzauskünfte, ist dieses Ersuchen also keine Tatsache, die die Bank zu einer Verdachtsmeldung nach § 43 des Geldwäschegesetzes veranlassen würde. Die Informationsflüsse im öffentlichen Bereich erfolgen sachgerechter zwischen den betroffenen öffentlichen Stellen nach dem dafür maßgeblichen Recht.

Zu Nummer 2

Die Nummer übernimmt verallgemeinernd (vgl. hierzu oben) das bisher speziell zu Auskunftsersuchen gegenüber nicht öffentlichen Stellen getroffene Nachteilsverbot des bisherigen § 8b Absatz 5 Satz 1 des Bundesverfassungsschutzgesetzes.

Zu Absatz 2

Absatz 2 übernimmt für Ersuchen den bisherigen § 8b Absatz 5 Satz 2 des Bundesverfassungsschutzgesetzes, d.h. die Pflicht, auf die Pflichten des Absatz 1 hinzuweisen.

Zu § 9 (Umfang von Auskunftspflichten)

§ 9 Absatz 1 gilt für Auskunftsersuchen, die zu einer Auskunftspflicht der ersuchten Stelle führen. Die Regelung stellt klar, dass durch die ersuchte Stelle keine Vorratsdatenspeicherung ins Blaue erfolgt. Gleichwohl können – dies ist in Satz 2 geregelt – Anbieter verpflichtet sein, Daten zu speichern, um dem Auskunftsersuchen zu entsprechen. Hierdurch wird sichergestellt, dass sicher der Anbieter nicht seinen Rechtspflichten dadurch entziehen kann, dass er die gewünschten Daten selbst gar nicht speichert. Es dürfen dabei nur solche Speicherpflichten entstehen, die Daten erfassen, welche von dem Anbieter vernünftigerweise gespeichert werden würden. Zulässig ist es also nicht, dem Anbieter eines Telekommunikationsdienstes aufzugeben, Lebensmittelunverträglichkeiten seiner Kunden zu erfragen, um eine Speicherpflicht eines Auskunftsverlangens zu erfüllen.

Unbeschadet dessen regelt § 9 Absatz 2, dass konkret veranlasste Ersuchen weiterhin auch zukunftsgerichtet zulässig bleiben (vgl. hierzu auch § 17 Absatz 3).

Zu Unterabschnitt 2 (Datenerhebung unter Mitwirkung öffentlicher Stellen)

Unterabschnitt 2 enthält die Regelungen über Auskunftsersuchen gegenüber öffentlichen Stellen.

Zu § 10 (Übermittlung von Daten an den Bundesnachrichtendienst durch inländische öffentliche Stellen)

Die Regelung greift die Regelung des bisherigen § 10 auf. Die Vorschrift regelt die Übermittlung an den Bundesnachrichtendienst ohne vorheriges, ausdrückliches Ersuchen und dient zugleich als allgemeine „Abrufregelung“ im Sinne der Doppeltür, soweit keine anderweitigen Bestimmungen bestehen (BVerfG, Urteil vom 27. Mai 2020, 1 BvR 1873/13 u.a., Rn. 95 mwN). Die Regelung des bisherigen § 10 Absatz 3, welche die Übermittlung

aufgrund eines expliziten Auskunftsersuchens betrifft, findet sich nunmehr in § 11. Ferner fanden Folgeanpassungen aufgrund der Neukonzeption des Gesetzes statt.

Zu Absatz 1

Die Absatz 1 enthält die allgemeine Befugnis einer Datenübermittlung durch inländische öffentliche Stellen ohne Auskunftsersuchen und ohne Übermittlungspflicht, welche zugleich die Abrufbefugnis für die Übermittlung von personenbezogenen Daten an den Bundesnachrichtendienst durch inländische öffentliche Stellen (für die Übermittlung ausländischer Stellen und/oder nichtöffentlicher Stellen ist diese Befugnis in § 5 Absatz 1 enthalten, vgl. dort) darstellt. Der ausdrückliche Einbezug von Personaldaten in Satz 1 stellt klar, dass die Übermittlungsregelung alle vorliegenden personenbezogenen Daten einschließt, also nicht nur die aus der operativen Verwaltungsaufgabe, sondern ebenso aus der Binnenverwaltung der Behörde. Hierbei können gerade Personaldaten von Bedeutung sein, insbesondere, weil es besonders wichtig ist, Mitarbeiterinnen und Mitarbeiter im öffentlichen Dienst, die entgegen den außen- oder sicherheitspolitischen Interessen der Bundesrepublik tätig sind, aufzuklären. Die Regelung stellt damit zugleich den speziellen Anwendungsvorrang der besonderen Regelung für Übermittlungen an den Bundesnachrichtendienst gegenüber allgemeinen Vorschriften des Personaldatenschutzes klar.

Zu Absatz 2

In Absatz 2 wird diese Möglichkeit einer Übermittlung durch öffentliche Stellen in bestimmten, enumerativ aufgezählten Fällen zu einer Übermittlungspflicht.

So ist es beispielsweise bei Cyberangriffen notwendig, dass der Bundesnachrichtendienst über Angriffe auf öffentliche Stellen und Organisationen in kritischen Sektoren im Sinne der NIS 2-Richtlinie unverzüglich unterrichtet wird. Die Rechtsänderung begegnet den bislang bestehenden rechtlichen Unsicherheiten hinsichtlich der Zulässigkeit und dem Umfang von Datenübermittlungen durch das Bundesamt für Sicherheit in der Informationstechnik im Kontext von Cybervorfällen an den Bundesnachrichtendienst. Nach derzeitiger Rechtslage, insbesondere nach § 8 Abs. 6 Nr. 3 des BSIG ist eine Datenübermittlung nur vorgesehen zu „Tatsachen, die einen internationalen kriminellen, terroristischen oder staatlichen Angriff mittels Schadprogrammen oder vergleichbarer schädlich wirkender informationstechnischer Mittel auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland erkennen lassen“. In der Praxis lassen sich die „Tatsachen“ die auf eine erhebliche Bedeutung des Cyberangriffs hindeuten erst in einer fortgeschrittener Phase (bspw. nicht schon beim Portknocking) zuverlässig feststellen. Für eine effektive Gefahrenfrüherkennung und Lagebewertung ist eine Informationsübermittlung jedoch regelmäßig bereits in einem frühen Stadium des Angriffs erforderlich. Durch die vorgesehene Erweiterung hin zu einer weitergehenden Übermittlungspflicht wird diese rechtliche Unsicherheit beseitigt.

Gleichzeitig wird sichergestellt, dass relevante Informationen frühzeitig ausgetauscht werden können und somit eine effektive und zeitnahe Reaktion auf Cyberbedrohungen ermöglicht wird. Das Bundesamt für Sicherheit in der Informationstechnik und der Bundesnachrichtendienst erfüllen unterschiedliche, sich jedoch ergänzende Aufgaben. Das Bundesamt für Sicherheit in der Informationstechnik überwacht insbesondere die Zugangspunkte der Bundesnetze und nimmt insoweit eine „Gatekeeper“ – Funktion wahr. Entsprechend werden dort primär Angriffe auf diese spezifische Infrastruktur erkannt. Der Bundesnachrichtendienst hingegen betreibt u.a. strategische Fernmeldeaufklärung und verfügt darüber hinaus über Befugnisse zur Durchführung von Server-Telekommunikationsüberwachung. Dadurch verfügt der Bundesnachrichtendienst über ein deutlich erweitertes Lagebild sowie über die Möglichkeit, Zusammenhänge zu erkennen, die sich aus einzelnen isolierten (dem BSI bekannten) Vorfällen nicht erschließen. Wird durch das Bundesamt für Sicherheit in der Informationstechnik beispielsweise ein Angriffsversuch festgestellt, der von einer bestimmten IP-Adresse ausgeht, kann dieser Vorfall aus Sicht des Bundesamtes für Sicherheit in

der Informationstechnik zunächst als nicht oder nur gering relevant eingeordnet werden. Dieselbe IP-Adresse kann jedoch in den Erfassungssystemen des Bundesnachrichtendienst in anderem Zusammenhang erscheinen und dort ein für den Bundesnachrichtendienst relevantes Infrastrukturobjekt in der Angriffsstruktur des Cyberakteurs betreffen. Eine isolierte Bewertung durch das Bundesamt für Sicherheit in der Informationstechnik würde in solchen Fällen die Gesamtrelevanz des Sachverhaltes nicht vollständig Aufgabenwahrnehmung sicherzustellen. Für den Bundesnachrichtendienst ist es daher von besondere Bedeutung, möglichst umfassend Informationen zu erhalten, um eine ganzheitliche Bewertung vornehmen und Zusammenhänge erkennen zu können.

Entsprechendes gilt für die durch das Bundesamt für Sicherheit in der Informationstechnik erkannten Angriffsziele. Durch seinen global ausgerichteten Aufklärungsansatz verfügt der Bundesnachrichtendienst über die Möglichkeit, laufende Angriffskampagnen etwa gegen bestimmte Behörden, Wirtschaftszweige oder Bereiche der öffentlichen Verwaltung frühzeitig zu erkennen und in einen übergeordneten Kontext einzuordnen. Derartige Angriffe erfolgen regelmäßig nicht gegen einen einzelnen Staat, sondern sind teilweise international angelegte und koordinierte Angriffskampagnen. Durch die frühzeitige Unterrichtung des Bundesamtes für Sicherheit in der Informationstechnik wird der Bundesnachrichtendienst in die Lage versetzt, Erkenntnisse mit internationalen Partner auszutauschen und dadurch einen Beitrag zur gemeinsamen Stärkung der Cyber-Sicherheit zu leisten.

Ebenso von besonderer Relevanz sind Erkenntnisse über die technische Funktionsweise von Schwachstellen in IT-Systemen. Diese ermöglichen es, die Angriffsweise von Angreifern nachzuvollziehen bzw. vorauszusehen und Muster zu identifizieren, auf die der Bundesnachrichtendienst im internationalen Telekommunikationsverkehr besonders achten muss. Derartige Informationen können einen erheblichen Beitrag zur Erhöhung der Treffgenauigkeit der Erfassungssysteme des Bundesnachrichtendienst leiten und dadurch sowohl die Effektivität der Aufklärung als auch die zielgerichtete Auswertung relevanter Kommunikationsvorgänge verbessern. Der Bundesnachrichtendienst nutzt regelmäßig Schwachstellen zur nachrichtendienstlichen Auslandsaufklärung. Die systematische Beschaffung und Suche diesen Schwachstellen stellt jedoch sowohl personell als auch aus finanzieller Sicht eine erhebliche Herausforderung dar. Zudem ist die Nutzdauer von Schwachstellen meist stark begrenzt, weshalb Aufwände dauerhaft auf einem hohen Niveau liegen.

Vor allem im Bereich der 0-Day-Schwachstellen schafft die Übermittlung einen erheblichen Mehrwert. Bis eine 0-Day-Schwachstelle nach Veröffentlichung bei den Herstellern durch das Bundesamt für Sicherheit in der Informationstechnik in Systemen durch Patches behoben wird, vergeht Zeit, die der Bundesnachrichtendienst für wichtige Arbeiten nutzen kann, welche die Grundlage für die Auftragserfüllung darstellen. Wird das Bundesamt für Sicherheit in der Informationstechnik aufgefordert, unmittelbar, beispielsweise über eine Austauschplattform, Erkenntnisse zu teilen, kann die Zeit zwischen interner Bearbeitung, Meldung an die Hersteller, Behebung des Softwarefehlers, Bereitstellung eines Patches und finaler Installation des selbigen, ausreichend lang sein, um die Schwachstellen in Wert bringen zu können. Jegliche zeitverzögernde Prozesse minimieren die Nutzungswahrscheinlichkeit drastisch. Zudem sind die Aufwände für ein solches Verfahren, z.B. bei Nutzung einer automatisierten Austauschplattform, gering und das Bundesamt für Sicherheit in der Informationstechnik wird an seinem Auftrag nicht gehindert. Zur Generierung eines Mehrwerts kann durchaus auch eine Weiterleitung des Kenntnisstands des Bundesamt für Sicherheit in der Informationstechnik über die Schwachstellen, inkl. ohnehin vorhandener technischer Parameter, ohne vorherige Aufarbeitung, hinreichend sein. Eine bloße Abfragemöglichkeit des Bundesnachrichtendienstes stellt hierfür kein gleichwertiges Mittel dar. Ohne konkrete Anhaltspunkte kann der Bundesnachrichtendienst regelmäßige keine zielgerichteten Anfragen stellen. Eine proaktive Übermittlung von Informationen ist daher erforderlich.

Das Steuergeheimnis nach § 30 der Abgabenordnung ist gemäß dessen Absatz 4 Nummer 5 Buchstabe a generell keine entgegenstehende Sondervorschrift, da die dem Ersuchen zugrunde liegende, durch den Bundesnachrichtendienst aufzuklärende Bedrohung generell das zwingende öffentliche Übermittlungsinteresse zur Abwehr erheblicher Nachteile für das Gemeinwohl begründet. Dies verdeutlicht nunmehr allgemein auch der neue § 10 Absatz 2 Nummer 6, so dass es sich erübrigt, die spezielle Regelung des bisherigen § 18 Absatz 3a des Bundesverfassungsschutzgesetzes fortzuführen.

Satz 3 stellt zudem klar, dass die Übermittlungspflicht in geeigneten Fällen technisch auch durch Einrichtung eines Abrufverfahrens umgesetzt werden kann. Geeignet sind insbesondere solche Sachverhalte, in denen die Übermittlung unter Abfrage eines Dateisystems erfolgt und im Einzelfall keine entgegenstehenden Übermittlungsregelungen zu prüfen sind (weil sie vorliegend nicht bestehen, oder ihre Beachtung im Wege der technischen Beschränkung von Zugriffsrechten zu gewährleisten ist). In diesem Fall kann das automatisierte Abrufverfahren unter Umständen die wirtschaftlichere Variante gegenüber händischer Bearbeitung sein (die hier keine inhaltliche Funktion hat) und den Zusatznutzen bieten, Bearbeitungsfehler zu vermeiden und Informationen verzögerungsfreie auch außerhalb der Bürostunden der ersuchten Behörde verfügbar zu machen. Dies stellt zudem eine datenschutzfreundliche Bearbeitung ohne menschliche Kenntnisnahme der Abfrage dar (die ansonsten möglicherweise als bemakelnd interpretiert würde und informelle negative Effekte für den Betroffenen bei der Sachbearbeitung in der ersuchten Stelle haben könnte). Die nähere Organisation, speziell die Abrufdokumentation (zur wirksamen Datenschutzkontrolle und im Interesse gesicherten Geheimschutzes vorzugsweise beim Bundesnachrichtendienst) bleibt den beteiligten Stellen überlassen.

Auch im Übrigen wird die Durchführung der Übermittlung – etwa durch Aktenübersendung oder Gewährung von Akteneinsicht – gesetzlich nicht näher geregelt, sondern bleibt angemessener Ausgestaltung im Verwaltungsvollzug unter Beachtung von Wirtschaftlichkeitserfordernissen überlassen.

Neben den hier getroffenen Regelungen bestehen auch bereichsspezifisch gestaltete Übermittlungspflichten in Fachgesetzen (wie etwa § 32 Absatz 3 Satz 1 des Geldwäschegesetzes), die weiterhin daneben anzuwenden bleiben.

Zu Absatz 3

Die Regelung des Absatz 3 greift Vorgaben des § 18 Absatz 1a des Bundesverfassungsschutzgesetzes auf. Dessen Satz 3 wird bedarfsgerecht angepasst. Der überragende Anteil der Übermittlungen des Bundesnachrichtendienstes an ausländische Stellen vollzieht sich mit Partnerländern zu deren Einschätzung der Einbezug des Bundesamtes für Migration und Flüchtlinge keinen Mehrwert bietet. Wenn der Bundesnachrichtendienst beispielsweise Informationen zu einem marokkanischen Staatsbürger an den französischen Partnerdienst übermittelt, kann das Bundesamt nicht mit besonderer Fachkunde zur Würdigung von Betroffenenbelangen beitragen. Bereits § 18 Absatz 1a des Bundesverfassungsschutzgesetzes sollte besonderer Fachkunde des Bundesamtes bei etwaigen (fernliegenden) Übermittlungen an den Herkunftsstaat Rechnung tragen. Dies kommt nunmehr in der Regelung auch zum Ausdruck.

Zu Absatz 4

Die Regelung trägt Schutzbelangen der benannten Behörden Rechnung, Daneben gilt im Übrigen der Vorrang besonderer gesetzlicher Übermittlungsregelungen nach Absatz 1, die ihrerseits die Übermittlungspflicht des § 10 beschränken. Insoweit ergibt sich ein entsprechender Übermittlungsausschluss für das BfV bereits aus § 52 BVerfSchG. Aus Gründen der Normenklarheit wird dennoch auch das BfV in Nummer 1 mit in Bezug genommen.

Zu Nummer 1

[…]

Zu Nummer 2

[…]

Zu § 11 (Verpflichtende Auskunftsersuchen gegenüber inländischen öffentlichen Stellen)

Die Einführung von § 11 löst die bestehenden Verweise im bisherigen § 10 Absatz 3 auf das Bundesverfassungsschutzgesetz auf. Die entsprechenden Vorschriften zu Auskunftsersuchen werden nunmehr direkt im BND-Gesetz geregelt. Regelt § 7 Absatz 1 die Befugnis anderer Stellen, personenbezogene Daten auf Ersuchen an den Bundesnachrichtendienst zu übermitteln und enthält § 10 Absatz 1 die eigeninitiative Übermittlung von öffentlichen Stellen (die in § 10 Absatz 2 zu einer Pflicht erwächst), so enthält § 11 die Befugnisnorm, durch die der Bundesnachrichtendienst die Übermittlung von Informationen einschließlich personenbezogener Daten mit Rechtspflicht gegenüber öffentlichen Stellen ersuchen darf. Diese war bisher § 10 Absatz 3 in Verbindung mit § 18 Absatz 3 des Bundesverfassungssschutzgesetzes geregelt.

Zu Absatz 1

§ 11 Absatz 1 entspricht § 18 Absatz 3 des Bundesverfassungssschutzgesetzes, ersetzt allerdings den Begriff der „Behörde“ gegen den Begriff, der „öffentlichen Stelle“, um den möglichen Adressatenkreis zukunftsoffen zu halten.

§ 11 Absatz 1 Satz 2 regelt die Pflicht der ersuchten Stelle, Informationen einschließlich personenbezogener Daten sowie Personaldaten im Rahmen eines Ersuchens an den Bundesnachrichtendienst zu übermitteln, soweit nicht spezialgesetzliche Übermittlungshindernisse einer Übermittlung an den Bundesnachrichtendienst ausnahmsweise entgegenstehen. Vergleich hierzu bereits die Begründung des § 7 Absatz 2.

Zu Absatz 2

§ 11 Absatz 2 entspricht dem bisherigen § 18 Absatz 4 des Bundesverfassungsschutzgesetzes. Im Vergleich zum geltenden Recht wurde die Befugnis zur Einsichtnahme darüber hinaus moderat erweitert. So ist in Nummer 2 nunmehr vorgesehen, dass der Bundesnachrichtendienst auch dann Einsicht nehmen kann, wenn dies zur Identifizierung von Personen erforderlich ist, die zur Aufklärung einer zumindest erheblichen Bedrohung beitragen können. Dies greift den Bedarf des Bundesnachrichtendienstes auf, Einsicht in das Ausländerzentralregister zu nehmen, um Personen ausfindig zu machen – sei es als mögliche Verantwortliche von (erheblichen) Bedrohungen, sei es, um potentielle nachrichtendienstliche Verbindungen zur Aufklärung solcher Bedrohungen zu identifizieren. Normativ ist ein „Zusammenhang zu dem Aufklärungsziel“ gefordert, wobei hier – da es um die Identifizierung möglicher Personen geht – der Zusammenhang nur möglich sein und gerade noch nicht feststehen muss.

Das bisherige Dokumentationserfordernis nach § 18 Absatz 5 zu Übermittlungsersuchen an Behörden wird in der allgemeinen Regelung nicht aufgegriffen. Das Gesetz bezweckt auch Bürokratieentlastung, um dafür gebundene Ressourcen besser für die Aufgabenerfüllung des Bundesnachrichtendienstes einzusetzen. Eine generelle Dokumentationspflicht ist nicht geboten (vgl. BVerfG, Beschluss vom 27. Mai 2020, 1 BvR 1837/13 u.a., Rn. 250). Dass wesentliche Vorgänge aktenkundig zu machen sind, ergibt sich allgemein aus dem rechtsstaatlichen Grundsatz der Aktenmäßigkeit der Verwaltung. Dies gilt gleichermaßen für das Verwaltungshandeln nach dem BND-Gesetz. Entsprechend findet sich nunmehr nur noch ein gesetzliches Erfordernis, die Einsichtnahme zu dokumentieren.

Zu Absatz 3

Absatz 3 regelt Ausschreibungen im polizeilichen Informationsverbund, die im nationalen Recht als „polizeiliche Beobachtung“ (vgl. § 47 Absatz 1 Nummer 1 BKAG) und im Unionsrecht als „verdeckte Kontrolle“ (vgl. Art. 36 f. EU (VO) 2018/1862) bezeichnet werden. Die polizeilichen Informationssysteme bezeichnen hier grundsätzlich alle bestehenden Informationssysteme von Polizeibehörden – in der Praxis erfolgt eine Ausschreibung im zentral beim Bundeskriminalamt geführten Informationssystem (insb. INPOL), welches eine Vernetzung mit anderen (etwa auch ländergeführten) Informationssystemen ermöglicht.

Der Sache nach handelt es sich um Ersuchen des Bundesnachrichtendienstes, beim polizeilichen Antreffen der Personen bestimmte, hierbei angefallene Erkenntnisse mitzuteilen. Die Regelung betrifft ausschließlich öffentliche Stellen und erfolgt daher in Unterabschnitt 2. Sie greift die Bestimmungen der bisherigen § 17 Absatz 2 und 3 des Bundesverfassungsschutzgesetzes auf, wobei Erkenntnisziel der Ausschreibung gemäß dem jeweiligen Aufklärungsbedarf nicht allein grenzüberschreitende Bewegungen der betroffenen Person sind. Datenschutzfreundlich erfolgt in Satz 1 Nummer 1 und 2 eine spezielle gesetzliche Regelung zu dem Personenkreis, zu dem Ausschreibungen möglich sind. Dabei ist das Tatbestandsmerkmal „im Zusammenhang mit dem Aufklärungsziel stehen“ in Nummer 2 weit zu verstehen, wobei ein Bezug zum Aufklärungszielt ggf. auch durch besondere Fähigkeiten oder Kontakte anzunehmen sein kann. Davon umfasst sind insbesondere diejenigen Personen und Sachen, von denen zu erwarten ist, dass sie zur Informationsgewinnung über das jeweilige Aufklärungsziel durch den Bundesnachrichtendienst beitragen können, insbesondere auch diejenigen Personen, die beispielsweise auf Grund ihres besonderen Wissens zu einem bestimmten Aufklärungsziel für den Bundesnachrichtendienst relevante Informationen liefern können.

Obgleich die Maßnahme weniger gewichtig eingreifend ist (BVerfG, Beschluss vom 9. Dezember 2022, 1 BvR 1345/21, Rn. 174), erfolgt für nationale Ausschreibungen eine Schwellenanhebung gegenüber dem bisherigen § 17 Absatz 2 des Bundesverfassungsschutzgesetzes, indem künftig zumindest tatsächliche Anhaltspunkte vorausgesetzt werden, dass dies zur Gewinnung von Informationen über zumindest erhebliche Bedrohungen erforderlich ist. Dies ist wertungs- und systemgerecht, da auch eine Ausschreibung (im nationalen polizeilichen Informationssystem - GFD) bei verständiger Würdigung an eine zumindest erhebliche Bedrohung geknüpft werden sollte; bereits die (im Vergleich zu Ausschreibungen in Datenverarbeitungssystemen der Europäischen Union – SIS) größere Nähe zur deutschen Staatsgewalt wiegt insoweit die regionale Begrenzung der Ausschreibungsmöglichkeit im nationalen polizeilichen Informationssystem GFB auf.

Für Ausschreibungen in Datenverarbeitungssystemen der Europäischen Union sind die unionsrechtlichen Voraussetzungen maßgeblich. Die Europäische Union besitzt zwar keine Regelungskompetenz zum Bereich der nationalen Sicherheit ihrer Mitgliedstaaten (Artikel 4 Absatz 2 Satz 3 EUV, BVerfG, Beschluss vom 8. Oktober 2024 - 1 BvR 1743/16, 1 BvR 2539/16 [BND – Cybergefahren] - Rn. 77 ff.). Sie regelt jedoch die Zwecksetzung ihrer Einrichtungen. Im Rahmen der nationalen Sicherheit können die Mitgliedstaaten autonom bestimmen, diese im Rahmen des EU-rechtlich erlaubten Zwecks auch für nachrichtendienstliche Ausschreibungen zu nutzen. Absatz 3 enthält insoweit die in Artikel 36 Absatz 4 EU (VO) 2018/1862 vorausgesetzte nationalrechtliche Erlaubnis. Dabei sind in jedem Fall tatsächliche Anhaltspunkte vorausgesetzt, dass dies zur Gewinnung von Informationen über zumindest erhebliche Bedrohungen erforderlich ist. Das Unionsrecht greift im Ergebnis nur, wo es enger ist. Der nationale Gesetzgeber kann zwar nicht darüber hinaus gehen, kann aber insoweit die Entscheidung treffen, den unionsrechtlichen Rahmen auszuschöpfen.

Zu Absatz 4

Die Regelung folgt einer Empfehlung der Innenministerkonferenz zu harmonisierten Verfassungsschutzgesetzen in Bund und Ländern (207. Sitzung am 8. Dezember 2017, TOP

29). Einige Landesverfassungsschutzgesetze enthalten bereits solche Regelungen (vgl. z.B. § 19a Absatz 1 Satz 4 BayVSG, § 21 LVerfSchG RP). Für den Bundesnachrichtendienst ist die dort getroffene Empfehlung gleichermaßen von praktischer Relevanz für seine Aufgabenerfüllung – insbesondere die Treffpunktabsicherung kann hierdurch entscheidend verbessert werden. Erfasst sind dabei allerdings ausschließlich Anlagen zur Überwachung des öffentlichen Raums. Die Regelung verpflichtet öffentliche Stellen; für nicht öffentliche Stelle vgl. § 15.

Die in Satz 2 und 3 enthaltenen Schwellenregelungen sind der Regelung in § 21 LVerfSchG RP nachempfunden und unterscheiden einerseits zwischen dem Echtzeit-Zugriff und dem hiermit verbundenen Anspruch, die Räumlichkeiten zu betreten und Einrichtungen zu nutzen. Dies ist nach Satz 2 möglich, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass es im Einzelfall zu nachrichtendienstlichen Auslandsaufklärung erforderlich ist. Andererseits ist in Satz 3 für ein Ersuchen, welches auf die Herausgabe angefertigter Aufzeichnungen gerichtet ist, die erste Qualifikationsstufe erforderlich. In diesem Fall sind ausgehändigte Aufzeichnungen zudem in Satz 4 mit einer besonderen Löschvorgabe belegt.

Zu Unterabschnitt 3 (Datenerhebung unter Mitwirkung nichtöffentlicher Stellen)

Zu § 12 (Auskunftsersuchen gegenüber nichtöffentlichen Stellen)

§ 12 regelt besondere Auskunftsersuchen zur Abfrage von – näher bestimmten – Bestandsdaten. Hierzu zählen insbesondere Vertragsdaten o.ä.. Diesen Daten ist – vor allem im Vergleich zu sog. Verkehrs- oder Inhaltsdaten – gemein, dass es sich um Daten handelt, die regelmäßig nur zu einem geringen Maß Rückschlüsse auf die private Lebensgestaltung zulassen. Eine Erhebung dieser Daten ist insoweit von herabgesenkter Eingriffsintensität. Grundlage für die Systematik des § 12 ist die bereits bestehende Rechtslage gemäß § 4 des bisherigen Rechts in Verbindung mit § 8d des Bundesverfassungsschutzgesetzes.

Zu Absatz 1

Absatz 1 regelt die Befugnis des Bundesnachrichtendienstes, Auskunft zu den Informationen über den angebotenen Dienst sowie zu den Bestandsdaten der in Absatz 2 genannten Dienste zu verlangen. Zugleich ist eine Legaldefinition des Begriffs der Bestandsdaten enthalten. Dabei ist ein entsprechendes Auskunftsersuchen (gegenüber den verpflichteten Stellen vgl. Absatz 2) regelmäßig daran geknüpft, dass die Auskunft im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist (Nummer 1).

Ergänzend darf eine Auskunft auch dann verlangt werden, wenn dies dem Schutz der betroffenen Person dient (Nummer 2). Diese Erweiterung ist praktisch in Fällen bedeutsam, in denen der Bundesnachrichtendienst betroffene Personen warnen möchte. So ist z.B. der Fall denkbar, dass eine TKG-Abfrage dazu dienen, den Anschlussinhaber zu bestimmen, um ihn davor zu warnen, dass sein Mobiltelefon von einem ausländischen Nachrichtendienst erfasst wurde. Auch wenn eine Gefährdung insoweit nicht eindeutig vorliegen sollte, liegt eine Kontaktaufnahme gleichwohl im Interesse der betroffenen Person liegt (um diese zu warnen).

Zu Absatz 2

In Absatz 2 werden die von der Auskunftspflicht erfassten Dienstleister näher bezeichnet. Dabei sind die hier geregelten nichtöffentlichen Stellen gleichermaßen auch die Adressaten der in § 13 geregelten qualifizierten Auskunftsersuchen. Nachfolgend werden dabei auch zu den „Verkehrsdaten“, welche nur im Rahmen von qualifizierten Auskunftsersuchen abgefragt werden können, Ausführungen gemacht.

Die Pflicht der ersuchten Stellen nach Absatz 2 Satz 1 Nummer 5 und 6 Auskunft zu erteilen, wird grundrechtsschonend subsidiär ausgestaltet, in dem sie nur greift, wenn die

Informationen nicht bereits im automatisierten Auskunftsverfahren von der Bundesnetzagentur nach § 173 Absatz 4 des Telekommunikationsgesetzes erlangt werden können.

Zu Nummer 1

Absatz 2 Nummer 1 wird entsprechend der Änderungen durch den Entwurf eines weiteren Gesetzes zur Reform des Nachrichtendienstrechts angepasst und damit der Verpflichtetenkreis erweitert.

Im Rahmen der ersten Alternative (Leistungen im Personenverkehr) wird die Aufklärung der Mobilität einer Person von der bisherigen Fixierung auf Luftverkehre gelöst. Künftig werden allgemein entgeltliche oder geschäftsmäßige Anbieter von Leistungen zum Transport von Personen (Personenverkehr) erfasst. Hierzu zählen insbesondere Eisenbahnverkehrsunternehmen im Sinne des § 2 Absatz 3 des Allgemeinen Eisenbahngesetzes, Unternehmen für den Linienverkehr mit Kraftomnibussen im Sinne des § 42a Satz 1 des Personenbeförderungsgesetzes sowie Unternehmen, die entgeltlich oder geschäftsmäßig Mittel für den öffentlichen Personenverkehr bereitstellen wie gewerbliche Anbieter von Mietfahrzeugen für Selbstfahrer im Sinne des § 6 Absatz 1 Nummer 14 des Straßenverkehrsgesetzes und Carsharing-Anbieter im Sinne des § 2 Nummer 2 des Gesetzes zur Bevorrechtigung des Carsharing. Mit der Regelung wird der gestiegenen und perspektivisch weiterwachsenden Bedeutung von Verkehrsträgern alternativ zum Flugverkehr (der weiterhin umfasst ist) Rechnung getragen. Neben den bereits beispielhaft aufgeführten Luftverkehren erstreckt sich die Auskunft insbesondere auch auf Schiffsverkehre.

Erfasst werden von der zweiten Alternative darüber hinaus auch die Dienstleister im Güterverkehr, wobei insoweit regelmäßig ein deutlich geringeres Eingriffsgewicht vorliegen wird, da gerade keine Bewegung von Personen (sondern von Dingen) in den Blick genommen wird.

Die erfassten Datenkategorien enthalten dabei insbesondere die zur Kundenidentifikation sowie – im Rahmen von qualifizierten Auskunftsersuchen – die zur Inanspruchnahme und zu den Umständen von Leistungen, insbesondere dem Zeitpunkt einer Abfertigung und zum Buchungsweg gespeicherten Daten.

Zur Auskunft sind auch diejenigen Dienstleister verpflichtet, die geschäftsmäßig an der Leistungserbringung im Personen- oder Güterverkehr mitwirken. Daraus folgt, dass auch Betreiber von Computerreservierungssystemen und globalen Distributionssystemen weiterhin verpflichtet werden können (entsprechend der bisherigen Aufzählung im bisherigen § 8a Absatz 1 Nummer 1 des Bundesverfassungsschutzgesetzes), ohne dass dies insoweit einer weiteren speziellen Regelung bedarf.

Zu Nummer 2

Die Neuregelung zielt darauf ab, dem Bundesnachrichtendienst die Aufklärung über die von verschiedenen Akteuren genutzten Kraftfahrzeuge zu ermöglichen und hierfür vorhandene Bestandsdaten – sowie im Rahmen von qualifizierten Auskunftsersuchen nach § 13 auch Standort- und Nutzungsdaten – bei Kraftfahrzeugherstellern, oder, wenn dies nicht oder nicht ohne Gefährdung des Zwecks der Maßnahme möglich ist, von Kraftfahrzeugwerkstätten, abrufen zu können. Darüber hinaus ist auch die beim Hersteller registrierte Fahrzeugidentifikationsnummer (FIN) erfasst, über welche eine Zuordnung des genutzten Kraftfahrzeuges möglich ist.

Bei modernen Kfz-Modellen erfassen Kfz-Hersteller umfassende Daten, die Rückschlüsse auf das Nutzungsprofil, die Intensität der Nutzung oder auch die Anzahl der Fahrer erlauben. Gespeichert werden z.B. gefahrene Strecken, GPS-Daten oder auch Gurtstraffungen. Die im Fahrzeug verbauten Steuergeräte können durch Kfz-Werkstätten im Rahmen eines Werkstattbesuchs mit Zustimmung des Fahrzeugbesitzers ausgelesen werden. Die Abfragemöglichkeit durch den Bundesnachrichtendienst kann weitere operative Maßnahmen im

Bereich der nachrichtendienstlichen Auslandsaufklärung ergänzend unterstützen. Darüber hinaus könnten durch das Abfragen von Nutzungsdaten (z.B. GPS-Daten, Statusdaten wie Kilometerstand, Anzahl der Fahrtstrecken, Abstellposition) Rückschlüsse auf konkrete Aktivitäten beteiligter Personen ermöglicht werden.

Zu Nummer 3

Absatz 2 Satz 1 Nummer 3 wird neu eingefügt und ermöglicht dem Bundesnachrichtendienst, auch bei den nach § 2 Absatz 1 des Geldwäschegesetzes verpflichteten Stellen Auskünfte zu den dort vorhandenen Daten zu verlangen, die in der Qualität mit den Bestandsdaten bei den zu ersuchenden Stellen nach Nummern 1 und 2 vergleichbar sind.

Entsprechend der niedrigen Eingriffsintensität darf der Bundesnachrichtendienst solche Daten ebenfalls abfragen, wenn tatsächliche Anhaltspunkte vorliegen, dass dies zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist. Die Aufnahme der Regelung optimiert die nachrichtendienstlichen Möglichkeiten im Bereich der Finanzermittlungen, da hierdurch der Adressatenkreis durch die Abfragemöglichkeit nach erweitert wird. Die nach § 2 Absatz 1 des Geldwäschegesetzes verpflichteten Stellen können allesamt Auskunft geben über die Personen, für die sie geschäftsmäßig Leistungen erbringen sowie zu den Daten, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines von ihnen betreuten Vertragsverhältnisses erforderlich sind (sog. Vertragsrahmendaten). Die Angaben zur Person umfassen die vom Unternehmen zur Identifizierung und Kontaktierung seiner Kundschaft gespeicherten Daten. Der Begriff der Kennung erfasst etwa Konto- oder Depotnummern. Die Abfrage ermöglicht dem Bundesnachrichtendienst, weitere Erkenntnisse im Bereich der Finanzermittlungen zu erzielen.

Die Einfügung ist erforderlich, da insbesondere großvolumige Transaktionen mittlerweile auch außerhalb des regulären Bankensystems durchgeführt werden. Insofern ist der Blick auf nach dem GWG-Verpflichtete, die nicht dem originären Finanzsektor zuzurechnen sind (in diesem Fall also z.B. Immobilienmakler), umso wichtiger. Dieser Personenkreis kann neben der Annahme von Bargeld auch mit der Gründung und Strukturierung von Firmen und Gesellschaften sowohl national als auch international befasst sein.

So verschleiern beispielsweise Extremisten aktiv ihre Geldflüsse; finanzstarke Geldgeber bleiben oft im Hintergrund, mit dem Ziel, unerkannt zu bleiben. Sind mehr Akteure nach GWG verpflichtet, hier Auskunft gegenüber dem Bundesnachrichtendienst zu geben, so erhöht dies die Möglichkeiten, extremistische Finanzstrukturen und Geldflüsse zu erkennen und aufzuklären.

Im Bereich der Aufklärung des Rechtsextremismus kann es vorkommen, dass einem international agierenden Akteur aus der rechtsextremistischen Szene die regulären Bankkonten gekündigt wurden und dieser sich daher auf anderen Wegen finanziell unterstützen lässt. Beispielsweise durch das Einsammeln von Spenden vor Ort bei seinen Veranstaltungen, deren Zahlungen anschließend über Online-Bezahldienstleister oder durch Überweisung auf ein Konto bei einer ausländischen Bank erfolgen. Andere Zahlungen können beispielsweise auch über Kryptowährungen erfolgen. Um die Natur solch diverser Finanzströme aufzuklären (rein privat oder doch Szene relevant), werden die Auskunftsmöglichkeiten des Bundesnachrichtendienstes durch Ergänzung der GWG-Verpflichteten, die auch Online-Finanzdienstleister oder auch Kryptowährungsbörsen umfassen, verbessert.

Der mögliche Erwerb von Immobilien spielt zudem für die rechtsextremistische Szene im In- und Ausland eine große Rolle. Eigene Immobilien ermöglichen das ungestörte Ausleben der extremistischen Gedankenwelt und bieten so die Möglichkeit, das Gemeinschaftsgefühl der Szene zu stärken. Zugleich dienen die Immobilien der Finanzierung der Szene, insbesondere durch den Verkauf von Getränken und Merchandise-Artikeln bei Gemeinschaftsabenden, Kampfsport-Events und Konzerten. Staatliche Akteure haben hier nur begrenzte

Möglichkeiten, derartige Veranstaltungen zu verhindern. Zugleich kann dabei erwirtschaftetes Kapital erneut in die Finanzierung von Immobilien fließen.

Mögliche Szenarien, in denen der Bundesnachrichtendienst in anderen Bereichen auf spezielle Auskünfte angewiesen sein könnte, betreffen die Phänomenbereiche Geldwäsche, Sanktionsumgehungen, Terrorismusfinanzierung und hybride Einflussnahme.

Die Abfragemöglichkeit nach § 13 bezieht sich bezüglich der in § 12 Absatz 2 Nummer 3 genannten Dienstleister auf qualifizierte, über Bestandsdaten bzw. Vertragsrahmendaten hinausgehende Daten, die aufgrund der gesteigerten Eingriffsintensität eine höhere Schwelle (Erste Qualifikationsstufe) erfordert. Eine Verkehrsdatenauskunft ermöglicht dem Bundesnachrichtendienst auch eine Abfrage zu Vermögensstand und Vermögensbewegungen. Der Begriff der Vermögensbewegungen umfasst beispielsweise auch die Übertragung und den Handel von Kryptowerten, der im Bereich der illegalen Finanzgeschäfte zunehmend an Bedeutung gewinnt.

Die erfassten Datenkategorien betreffen hier neben den bereits genannten Vermögensständen und-bewegungen (z.B. Kontostand, Zahlungsein- und -ausgänge) insbesondere Daten zu Konten, Kontoinhabern und sonstigen Berechtigten sowie weiteren am Vermögensverkehr beteiligten Personen.

Zu Nummer 4

Die Neuregelung zielt darauf ab, eine Aufklärung der von verschiedenen Akteuren genutzten Sendungswege von Post- und Warenverkehrssendungen zu ermöglichen.

Der Standort Deutschland beherbergt eine Vielzahl marktführender Unternehmen der internationalen Logistikbranche, deren Dienstleistungen auch von nicht-legitimen Akteuren genutzt werden. Diese Dienstleistungen werden z.B. im Phänomenbereich Proliferation/Sanktionsumgehung häufig von Zwischenhändlern in Drittstaaten genutzt, deren Geschäftsmodell maßgeblich auf systematischer Umgehung von Sanktionen gegen einen anderen sanktionierten Drittstaat beruht. So werden beispielsweise sanktionierte Produkte (z.B. Dual-Use-Güter) in einem nicht-sanktionierten Staat durch einen Zwischenhändler in einem anderen, ebenfalls nicht-sanktionierten Staat, erworben. Dieser Zwischenhändler leitet die Ware dann, ggf. über weitere Umwege, an einen Endverwender der Rüstungsindustrie eines sanktionierten Staates weiter.

Im Bereich Terrorismus spielen Versandwege zudem häufig eine entscheidende Rolle zur Vorbereitung von Anschlägen und können somit zur Aufklärung der Anschlagsvorbereitungen genutzt werden. Beispielsweise könnten Anhaltspunkte für Anschlagsplanungen gewonnen werden, indem Sendungen mutmaßlich terrorverstrickter Personen systematisch daraufhin ausgewertet werden, ob Lieferungen bekannter Hersteller z.B. von zur Herstellung von Sprengstoff geeigneten Chemikalien erfolgt sind. Genauso könnten Anhaltspunkte für Unterstützer eines Terrornetzwerks gewonnen werden, indem Lieferungen bekannter Hersteller z.B. von zur Herstellung von Sprengstoff geeigneten Chemikalien systematisch daraufhin ausgewertet werden, wohin Lieferungen abgesetzt wurden.

Die Regelung ermöglicht die Auskunft zu den bei der ersuchten Stelle gespeicherten Daten, u.a. zu Namen und Anschriften von Absendern und Empfängern, sowie – ggf. unter Rückgriff auf § 13 – zu der Art des in Anspruch genommenen Post- und Warenverkehrsdienstes, zu Maßen und Gewicht der jeweiligen Post- und Warensendung, zu vom Absender angegebene Informationen zum Inhalt der jeweiligen Post- und Warensendung, zu zugeteilten Sendungsnummern, zu Zeit- und Ortsangaben des jeweiligen Post- oder Warensendungsverlaufs sowie zu Bild- und Röntgenaufnahmen von der Post- oder Warensendung, die zu Zwecken der Erbringung der Post- oder Warenverkehrsdienstleistung erstellt wurden.

Nicht umfasst sind Daten, die lediglich durch Öffnung der Post- oder Warensendung erlangt werden können, wie z.B. der konkrete Inhalt der jeweiligen Sendung.

Da es sich bei den vom Auskunftsersuchen erfassten Daten regelmäßig um solche handelt, die dem Schutz des Artikel 10 Absatz 1 des Grundgesetzes unterfallen, ist insoweit eine vorherige Anordnung und Vorabkontrolle durch den Unabhängigen Kontrollrat erforderlich.

Zu Nummer 5 und Nummer 6

Nummer 5 und Nummer 6 entsprechen der aktuellen Rechtslage im derzeitigen § 3 in Verbindung mit § 8a des Bundesverfassungsschutzgesetzes.

Absatz 2 Satz 1 Nummer 5 und 6 entsprechen bereits der geltenden Rechtlage nach § 4 Absatz 1 Nummer 1 und Nummer 2. Danach kann der Bundesnachrichtendienst bei Telekommunikationsdiensten und digitalen Diensten Bestandsdaten abrufen, wenn tatsächliche Anhaltspunkte vorliegen, dass dies zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist.

Bei qualifizierten Auskunftsersuchen nach § 13 sind bezüglich der hier genannten Dienstleister insbesondere Verkehrsdaten nach § 9 Absatz 1 Satz 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes sowie Standortdaten nach § 13 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes, erfasst (Nummer 5). Für den Bereich der digitalen Dienste (Nummer 6) sind dies insbesondere Merkmale zur Identifikation des Nutzers eines digitalen Dienstes, zu Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung eines digitalen Dienstes und Angaben über die vom Nutzer in Anspruch genommenen digitalen Dienste.

Zu Nummer 7

Nach § 2 Absatz 1 Nummer 9 des Zahlungsdiensteaufsichtsgesetzes sind technische Dienstleister, die zwar zur Erbringung der Zahlungsdienste beitragen, jedoch zu keiner Zeit in den Besitz der zu übertragenden Gelder gelangen, keine Zahlungsdienste. Entsprechend fallen die hiervon umfassten Stellen auch nicht unter Nummer 3. Es handelt sich hierbei z.B. um Betreiber von Zahlungsverkehrssystemen wie den Kreditkartenunternehmen Mastercard und VISA, die aufgrund ihrer weltweiten Verbreitung von besonderer Relevanz für die nachrichtendienstliche Auslandsaufklärung sind. Dies gilt insbesondere deshalb, weil die Auskunft bei diesen Dienstleistern auch dann möglich ist, wenn ein Auskunftsersuchen gegenüber der kartenausgebenden Bank aus operativen Gründen nicht in Betracht kommt.

Zu Absatz 3

Absatz 3 enthält die vormals in § 2 Absatz 2 Satz 2 und 5 des Artikel 10-Gesetzes enthaltenen Regelungen, deren Reihenfolge dabei aus rechtssystematischen Gründen umgekehrt wurde.

Zu Absatz 4

Absatz 4 entspricht im Wesentlichen dem bisherigen § 4 Absatz 4 BND-Gesetz.

Neu eingefügt wird die Möglichkeit, das Auskunftsersuchen auch anhand der genutzten Zahlungsmittel (wobei es sich nicht nur um die „Art“ des Zahlungsmittels handelt – also etwa Kreditkarte, Online-Bezahlkonto etc. – sondern auch um die konkrete Kartennummer, den „Account“, usw.) oder sog. technische Identifikatoren (wie etwa Anmeldedaten, Zahlungsdaten) zu stellen. Die Identifikatoren sind neben der Internetprotokoll-Adresse auch solche sekundären technischen Merkmale, die durch Diensterbringer genutzt werden, um den Zugang zu ihren Diensten zu ermöglichen, z.B. persistente Cookies oder MAC-Adressen. Hierdurch soll z.B. im Fall eines Cyberangriffes über einen gemieteten Server ein schnelles Handeln ermöglicht werden. Solche Server werden häufig mit einer E-Mail-Adresse und einem konkreten Zahlungsmittel angemietet. Bisher unbekannte, durch denselben Cyberakteur angemietete IT-Infrastruktur kann dadurch schneller identifiziert werden.

Zu Absatz 5

Absatz 5 entspricht im Wesentlichen dem bisherigen § 4 Absatz 5 und § 8d Absatz 3 des Bundesverfassungsschutzgesetzes. Die in der letztgenannten Vorschrift enthaltene spezielle Verfahrensregelung erübrigt sich, da der allgemeine Verweis auf die gesetzlichen Voraussetzungen auch Verfahrensvoraussetzungen einschließt. Wenn die durch das Auskunftsersuchen vorbereitete Maßnahme einer unabhängigen Vorabkontrolle unterliegt, muss diese Vorabkontrolle – dies wird durch den Verweis auf die gesetzlichen Voraussetzungen für die Nutzung der Daten sichergestellt – mithin bereits für das entsprechende Auskunftsersuchen zur PIN/PUK erfolgen (BVerfG, Beschluss vom 24. Januar 2012, 1 BvR 1299/05, Rn. 185). Eine zusätzliche, von der vorbereiteten Maßnahme unabhängige Verfahrensregelung ist aus diesem Grund nicht erforderlich.

Zu Absatz 6

Absatz 6 entspricht dem bisherigen § 8a Absatz 2 Satz 2 des Bundesverfassungsschutzgesetzes. Durch die Änderung des § 93 Absatz 8 der Abgabenordnung, in der nun der Bundesnachrichtendienst explizit aufgeführt ist, bedarf es insoweit (nur) noch der Feststellung der Nichtanwendbarkeit des § 93 Absatz 9 der Abgabenordnung.

Zu § 13 (Qualifizierte Ersuchen gegenüber nicht öffentlichen Stellen)

Zu Absatz 1

§ 13 regelt solche Auskunftsersuchen, die über die Auskunft der in § 12 geregelten Informationen und Bestandsdaten hinausgehen, insoweit also sowohl hinsichtlich der Daten als auch bezüglich der Eingriffsintensität und -kompensierung „qualifiziert“ sind. Auch insoweit ist eine Beauskunftung nach § 16 Absatz 1 für die ersuchte Stelle verpflichtend.

Es werden die bisher in § 3 Absatz 1 in Verbindung mit § 8a des Bundesverfassungsschutzgesetzes enthaltenen Regelungsgehalte aufgenommen, wobei auch hier die materielle Schwelle angepasst wurde, um ein einheitliches, in sich konsistentes Schwellensystem innerhalb des BND-Gesetzes sicherzustellen. Bislang mussten Tatsachen die Annahme rechtfertigen, dass schwerwiegende Gefahren für die in § 5 Absatz 1 Satz 3 Nummern 1 bis 4 und 6 Artikel 10-Gesetz genannten Gefahrenbereiche vorliegen. Nunmehr müssen – soweit deutsche Staatsangehörige, sich im Bundesgebiet aufhaltende Personen oder inländische juristische Personen betroffen sind – tatsächliche Anhaltspunkte vorliegen, dass durch das Auskunftsersuchen Informationen zu zumindest erheblichen Bedrohungen erlangt werden können (Erste Qualifikationsstufe). Dies betrifft lediglich den Fall der Übermittlung von personenbezogenen Daten – für Sachinformationen ohne Personenbezug gilt die erhöhte Schwelle nicht (da es hier ohnehin bereits an einem qualifizierten Inlandsbezug fehlt). Satz 1 regelt hiervon abweichende materielle Voraussetzungen, soweit sich das Auskunftsersuchen auf Ausländerinnen oder Ausländer im Ausland oder auf reine Sachinformationen bezieht. Die Ausgestaltung der gesetzlichen Befugnis in diesem Absatz trägt in verfassungsrechtlicher Hinsicht dem Umstand Rechnung, dass die Maßnahme gegenüber einer Ausländerin oder einem Ausländer im Ausland ein geringeres Eingriffsgewicht aufweist. Diese Personengruppe unterliegt typischerweise nicht dem Zugriff deutscher Behörden und ist damit in deutlich verringertem Ausmaß Folgemaßnahmen ausgesetzt. Vgl. BVerfG vom 19. Mai 2020, 1 BvR 2835/17 (154, 152), Rn. 186. Es ist insoweit maßgeblich, wer die betroffene Person des Auskunftsersuchens ist.

Die Prüfung der normativ verankerten Tatbestandsvoraussetzungen liegt dabei – dem o.g. allgemeinen Grundsatz folgend – ausschließlich in der Verantwortung des Bundesnachrichtendienstes. Für die adressierten nicht öffentlichen Stellen besteht insoweit Rechtssicherheit, dass sie auf Ersuchen des Bundesnachrichtendienstes zu übermitteln haben und die Voraussetzungen des Ersuchens allein vom Bundesnachrichtendienst zu prüfen sind.

Die Pflicht zur Übermittlung der ersuchten Informationen an den Bundesnachrichtendienst bezieht sich auf die für die Geschäftszwecke vorhandenen (oder in der Zukunft anfallenden) Informationen. Weder besteht eine Pflicht zur Vorsorgespeicherung noch eine Pflicht, über die Speicherung bei zukunftsgerichteten Auskunftsersuchen hinaus Informationen zur Auskunftserteilung zu beschaffen.

Zu Absatz 2

Nach Absatz 2 gilt das bereits vorhandene Verursacherprinzip fort (zur bisherigen Rechtslage vgl. den derzeitigen § 3 Absatz 2 in Verbindung mit § 8a Absatz 3 des Bundesverfassungsschutzgesetzes). Die Regelung wurde dabei sprachlich angepasst, da sich Auskunftsersuchen nicht „gegen“ eine Person richten, sondern auf eine Person bezieht.

Bei den in Nummer 1 – für den dort geregelten „Primärverantwortlichen“ – verwandten Begriff der „Verantwortlichkeit“ nicht um ein subjektives Merkmal, sondern um ein rein kausalobjektives – erforderlich ist insbesondere kein Vorsatz der betroffenen Person im strafrechtlichen Sinne. Vielmehr können auch vorsatzlose Werkzeuge für eine Bedrohung „verantwortlich“ sein, da insoweit nur auf die Kausalität abzustellen ist. Vergleichbar zum geltenden Recht ist zudem ein „Unterstützen“ der erheblichen Bedrohung durch die betroffene Person hinreichend, um ein Auskunftsersuchen gegen sie zu richten. Hierbei wird von dem bisherigen Begriff („nachdrücklich fördern“ – vgl. § 8a Absatz 3 Nummer 1 des Bundesverfassungsschutzgesetzes) insbesondere insoweit abgewichen, als dass ein besonderer „Nachdruck“ nicht länger vorgesehen ist. Dieses Merkmal war mit erheblicher Rechtsunsicherheit verbunden. Im Unterschied zur „Verantwortlichkeit“ für eine erhebliche Bedrohung setzt ein Unterstützen keinen (maßgeblichen) Beitrag voraus, sondern kann schon bei geringeren Mitwirkungshandlungen vorliegen.

Auch Nummer 2 wurde im Vergleich zum bisherigen Recht (§ 8a Absatz 3 Nummer 2 des Bundesverfassungsschutzgesetzes) modifiziert. Insoweit wurde klargestellt, dass die in den Buchstaben a bis d (für bestimmte Auskunftsersuchen) genannten Fallkonstellationen lediglich Beispiele dafür darstellen, dass die betroffene Person in einem (hinreichenden) Zusammenhang mit dem Aufklärungsziel des Auskunftsersuchens stehen. Der erforderliche Zusammenhang wird dabei bereits tatbestandlich näher konturiert; er muss gerade Grund zu der Annahme geben, dass durch den Zusammenhang Erkenntnisse zu der aufzuklärenden Bedrohung gewonnen werden können. Nicht hinreichend ist also ein völlig entfernter Zusammenhang bloß terminologischer Natur. Die Regelung soll das Gesetz insoweit flexibilisieren, dass es in – den Buchstaben a bis d in ihrer Intensität vergleichbaren – Situationen möglich ist, etwa eine in Deutschland lebende enge Kontaktperson eines ausländischen Generals mit einem Auskunftsersuchen aufzuklären. Gleichermaßen würden neben den in den Buchstaben a bis d „insbesondere“ genannten personellen Zusammenhängen indes auch „vorhabenspezifische“ Verbindungen zu dem Aufklärungsziel hinreichend sein; etwa die Zugehörigkeit zur gleichen Gruppierung oder einem sanktionsrelevanten Unternehmen.

Um eine Aufklärung von Netzwerken zu ermöglichen, die dem Zweck dienen, eine erhebliche Bedrohung zu unterstützen, darf der Bundesnachrichtendienst insbesondere auch Auskunftsersuchen durchführen, die sich gegen Teile eines solchen Netzwerkes richten (Buchstabe d). Der im Rahmen von Nummer 2 erforderliche „Bedrohungszusammenhang“ lieg hier in der von dem Netzwerk als solchem ausgehende Bedrohung. Der Bundesnachrichtendienst darf insoweit Auskunftsersuchen durchführen, um die Mitglieder dieses Netzwerks insgesamt aufzuklären, solange tatsächliche Anhaltspunkte dafür bestehen, dass diese das Netzwerk ausschließlich oder ganz überwiegend nutzen, um die erhebliche Bedrohung zu unterstützen. Eine solche Nutzung ist insoweit anzunehmen, wenn das Netzwerk ganz überwiegend dafür genutzt wird, eine Bestrebung zu unterstützen, oder das Netzwerk mit dem expliziten Ziel geschaffen wurde, als Kommunikationsbasis für eine Gruppe von Personen zu dienen, welche sich der Verwirklichung oder Förderung einer erheblichen Bedrohung verschrieben haben.

Absatz 3 Satz 2 stellt klar, dass auch eine Funkzellenabfrage zulässig ist. In Absatz 3 Satz 3 ist klargestellt, dass Auskunftsersuchen jenseits der in den Nummern 1 bis 3 enthaltenen Verantwortlichkeitszurechnung auch gegenüber solchen Personen zulässig sind, deren Einsatzfähigkeit als nachrichtendienstliche Verbindung (entweder initial oder im Verlauf ihrer Tätigkeit) geprüft wird. Dies ist zwingend erforderlich, um sicherheitliche Risiken zu vermeiden, die sich aus der Verpflichtung einer nachrichtendienstlichen Verbindung ergeben würden, welche z.B. für ein fremde Macht tätig ist.

Zu Absatz 3

In Absatz 3 ist eine besondere Befugnis des Bundesnachrichtendienstes im Rahmen von Auskunftsersuchen gegenüber Dienstleistern, die geschäftsmäßig Leistungen im Güterverkehr oder geschäftsmäßig Post- und Warenverkehrsdienste erbringen, vorgesehen. Die Ermächtigungsgrundlage befähigt den Bundesnachrichtendienst, auch ungezielt Sendungsdaten zu erheben, um Beschaffungswege und Transportrouten aufzuklären. Hierdurch soll die Möglichkeit geschaffen werden, z.B. für Beschaffungsnetzwerke von Proliferationsakteuren genutzte, illegale Warenströme ausfindig zu machen.

Die Befugnis ist für die Aufgabenerfüllung des Bundesnachrichtendienstes von großer Bedeutung. Der Standort Deutschland beherbergt eine Vielzahl marktführender Unternehmen der internationalen Logistikbranche, deren Dienstleistungen von vielfältigen, aufklärungsrelevanten Akteuren genutzt werden. Eine systematische Auswertung der zugrundeliegenden Metadaten erfolgt bisher nicht. Dabei ließen sich so nachrichtendienstliche Erkenntnisse über eine große Bandbreite von Aufklärungsschwerpunkten erlangen.

Im Phänomenbereich „Proliferation“ versenden Zwischenhändler häufig in und an Drittstaaten, deren Geschäftsmodell maßgeblich auf der systematischen Umgehung von Sanktionen beruht. Aber auch militärische Güter, die keiner Sanktionierung unterliegen, werden über den internationalen Transportweg an den Endverwender verbracht. Ein Beispiel hierfür bildet der Kauf eines sanktionierten Produkts in einem EU-Staat durch einen Zwischenhändler in einem nichtsanktionierten Drittstaat. Dieser leitet die Ware dann, ggf. über weitere Umwege, an einen Endverwender im sanktionierten Staat weiter. Aus dem Metadatenmuster können sich tatsächliche Anhaltspunkte für Sanktionsumgehung durch die beteiligten Stellen ergeben, die sodann als Einzelfall genauer betrachtet werden können.

Im Bereich der Wirtschaft sind private und staatliche Unternehmen zur Erschließung von ausländischen Absatzmärkten auf robuste Lieferketten angewiesen. Internationale Logistikdienstleister spielen hierbei eine maßgebliche Rolle. Aus der Auswertung der durchgeführten Transporte lassen sich Rückschlüsse auf wirtschaftliche Interessen und strategische Bemühungen einzelner Staaten ableiten.

Zur Aufklärung des internationalen Terrorismus ist eine strategische Aufklärung von Lieferwegen gleichsam von großer Bedeutung. Dies betrifft beispielhaft den Online-Versandhandel bzgl. chemischer Komponenten, welche für Sprengvorrichtungen genutzt werden können. Liefern z.B. mehrere ausländische Hersteller gemäß Sendungsdeklaration eine bestimmte Chemikalie an eine noch unbekannte Person in einem Drittland, worauf hin diese Person in engen zeitlichem Zusammenhang im Vorfeld eines Großereignisses ein Visum für den Schengenraum beantragt, so können sich aus diesem Muster tatsächliche Anhaltspunkte für eine von der Person ausgehende Bedrohung ergeben.

Internationale Lieferketten sind zuletzt auch vermehrt Ziel von Sabotageakten ausländischer Akteure geworden. Die gezielte Aufklärung dieser Bemühungen erfordert die Analyse der zugrundeliegenden Versandvorgänge mithilfe der einschlägigen Metadaten.

Im Phänomenbereich der „Aufklärung fremder Dienste“ greifen Entitäten, die sich fremden Nachrichtendiensten zuordnen lassen, im Rahmen ihrer eigenen Lieferkette häufig auf Versanddienstleister zurück. Darüber hinaus erhalten Geheim- und Nachrichtendienste, sowie diplomatische Vertretungen im Ausland regelmäßig nachrichtendienstlich relevante

Versendungen von bisher unbekannten Personen oder Unternehmen, die sich mit der hier geschaffenen Befugnis ebenfalls aufklären ließen.

Zuletzt nutzen auch im Phänomenbereich „Organisierte Kriminalität / Rauschgifthandel“ einschlägige Akteure den internationalen Transportweg zur Verbringung von Rauschgift in ausländische Absatzmärkte. Die Aufklärung der Lieferwege erlaubt Rückschlüsse auf mögliche Kooperationspartner im europäischen Markt.

Zu Absatz 4

In Absatz 4 finden sich die bislang in § 2 Absatz 1 des Artikel 10-Gesetzes enthaltenen Pflichten von Anbietern von Post- (und Warenverkehrs-)Dienstleistern. Dabei wurde (wie auch im nachfolgenden Absatz 5) eine systematische Vereinheitlichung dergestalt vorgenommen, dass die jeweiligen „Pflichten“ (bei denen es sich im Kern um Auskunfts- und Mitwirkungspflichten handelt) nunmehr einheitlich in Abschnitt 2 geregelt werden.

Dies bedeutet im Ergebnis, dass der Bundesnachrichtendienst einerseits die in § 12 Absatz 2 Satz 1 Nummer 4 genannten Stellen ersuchen kann, ihm nach Maßgabe der §§ 12, 13, 16 und 17 Auskunft zu Bestands- und Verkehrsdaten zu erteilen. Andererseits kann er (muss er, wenn es um die Erhebung von Artikel 10-geschützten Inhaltsdaten geht) aber auch ein nachrichtendienstliches Mittel (etwa eine Maßnahme bei Post- und Warensendungen nach § 28) durchführen. Macht er von der letztgenannten Möglichkeit Gebrauch so ist er regelmäßig (zumal im Inland) gleichwohl auf die Mitwirkung der in § 12 Absatz 2 Satz 1 Nummer 4 genannten Stellen angewiesen, welche ihm z.B. die jeweilige Postsendung aushändigen müssen (Nummer 2). In diesen Fällen bedarf es zugleich – dies ist in § 17 geregelt – keiner „erneuten“ Anordnung, da bereits das nachrichtendienstliche Mitteln nach § 28 anordnungsbedürftig war. Der Inhalt der Mitwirkungspflichten entsprich in seinem Umfang dem bisherigen § 2 Absatz 1 des Artikel 10-Gesetzes.

Zu Absatz 5

Die zu Absatz 4 beschriebene Systematik setzt sich – mutatis mutandis – in Absatz 5 auch für die in § 12 Absatz 2 Satz 1 Nummer 5 genannten Stellen und bezüglich von Maßnahmen der Telekommunikationsüberwachung, der strategischen Aufklärung und des Eingriffs in informationstechnische Systeme fort. Dabei entsprechen die Mitwirkungspflichten denen des bisherigen § 2 Absatz 1a des Artikel 10-Gesetzes, wobei in Nummer 4 eine Anpassung dahingehend erfolgt ist, dass eine Mitwirkungspflicht zur Einbringung von technischen Mitteln nicht nur bei der (vormaligen) Quellen-Telekommunikationsüberwachung besteht, sondern bei Eingriffen in informationstechnische Systeme insgesamt.

Zu Absatz 6

Absatz 6 enthält die vormals in § 2 Absatz 2 Satz 1 und 3 bis 4 des Artikel 10-Gesetzes enthaltenen Bestimmungen.

Zu § 14 (Besondere Auskunftsersuchen bei informationstechnischen Angriffen)

Mit der Vorschrift soll insbesondere die Aufklärung von komplexen Angriffen (sogenannte Advanced Persistent Threats, APT) ermöglicht werden, bei denen einzelne informationstechnische Systeme gezielt als Teil einer komplexeren Angriffsinfrastruktur eingesetzt werden. Die neue Befugnis für Auskunftsersuchen in diesem Bereich soll dem Bundesnachrichtendienst eine wirksame und verbesserte Früherkennung von entsprechenden Bedrohungen (vgl. § 4 Absatz 4 Nummer 3) ermöglichen. Der Angriff muss „möglich“ sein, womit sowohl ein Angriff in der Zukunft wie in der Vergangenheit gemeint sein kann. Zudem ist ein prognostisches Element erhalten, da der Bundesnachrichtendienst nur höchst ausnahmsweise sichere Kenntnis davon haben wird, ob ein entsprechender Angriff wirklich vorlag. Die Aufgabenwahrnehmung anderer Sicherheitsbehörden bleibt hiervon unberührt. Dies gilt gleichermaßen für die nachrichtendienstliche Aufklärung von Bedrohungen durch

das Bundesamt für Verfassungsschutz und Bundesamt für den Militärischen Abschirmdienst wie auch polizeiliche Ermittlungen oder ebenso die Cyberverteidigung der Streitkräfte.

Zu Absatz 1

Absatz 1 Satz 1 enthält die allgemeine Befugnis für den Bundesnachrichtendienst, um Auskunft zu ersuchen. Dabei ist die tatbestandliche Eingriffsschwelle – insoweit von der übrigen Systematik des Gesetzes abweichend – spezieller und auf die Zielrichtung der Befugnis zugeschnitten: Nicht die nachrichtendienstliche Auslandsaufklärung (oder eine der Bedrohungs-Qualifikationsstufen) ist hier eingriffsrechtfertigend, sondern tatsächliche Anhaltspunkte für einen „Cyber-Angriff“. Angriffe in diesem Sinne sind solche, die darauf gerichtet sind, die Integrität, Authentizität, Vertraulichkeit oder Verfügbarkeit von Telekommunikations- und Datenverarbeitungssystemen zu beeinträchtigen, insbesondere mit Programmen und sonstigen informationstechnischen Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten zu nutzen oder zu löschen oder die dem Zweck dienen, unbefugt auf sonstige informationstechnische Abläufe einzuwirken (Schadprogramme i.S.d. § 2 Absatz 5 BSIG).

Die zur Aufklärung dieser Angriffe nötige, spezielle Auskunftspflicht ist (gesetzlich) beschränkt auf Diensteanbieter, die Telekommunikationsanlagen oder sonstige informationstechnische Systeme Dritten zur Nutzung überlassen beispielsweise kommerzieller Hostinganbieter. Die vorgesehene Auskunftspflicht soll in diesem Zusammenhang ermöglichen, vorrangig ohne systeminvasive Maßnahmen notwendige Informationen zur weiteren Aufklärung zum Angriff und zu Angriffszielen zu erlangen. Die Auskunftspflicht ist auf die Übermittlung der beim Betreiber vorhandenen und verfügbaren technischen Informationen begrenzt. Eine Pflicht zur Speicherung begründet die Vorschrift nicht. Der Bundesnachrichtendienst kann den Provider bei der Erfüllung der Auskunftspflicht etwa durch die Bereitstellung notwendiger Hardware unterstützen.

In Satz 2 werden die Auskunftspflichten mit den Hauptanwendungsfällen näher konkretisiert. Satz 3 erstreckt die Auskunftspflicht über die nach Satz 1 zu beauskunfteten technischen Informationen hinaus auch auf Beutedaten, die der Angreifer in der genutzten Angriffsstruktur im Rahmen der Angriffsverschleierung womöglich zwischengespeichert hat. Auch diese Informationen sind zur Klärung der Beschaffungsziele des Angreifers wertig.

Zu Nummer 1

Absatz 1 Satz 2 Nummer 1 bezieht sich auf Auskünfte zu Verkehrs- und Steuerdaten, die vom Diensteanbieter zur Verkehrsanalyse oder Kapazitätsplanung für die eigene Qualitätssicherung verarbeitet und dokumentiert werden. „Verkehrsfluss“ ist der Fachbegriff für solche Datenbasis betrieblicher Qualitätssicherung. Er wird betreiberseitig mit Standardprodukten, verbreitet beispielsweise im sog. Netflow-Format (proprietärer Standard der Firma Cisco), erhoben. Die gespeicherten Informationen sind abhängig vom jeweiligen Speicherformat und enthalten im Falle von Netflow typischerweise unter anderem Quell- und Ziel-IP-Adressen, Zeitstempel und den jeweiligen Protokolltyp. Damit werden auch die im Verkehrsfluss anfallenden Verbindungen von Servern des Hosters zu dem Steuerungsserver des Angreifenden protokolliert.

Anhand von technischen Parametern, die nicht gleichermaßen über eine Verkehrsdatenauskunft zu erheben sind, kann geprüft werden, ob es sich bei diesen weiteren Verbindungen ebenfalls um Kommunikation des Akteurs handelt. So können Infrastrukturnetzwerke von Cyberspionagegruppen und bisher nicht sichtbare Angriffe aufgeklärt werden. Je nach Zeitpunkt des Zugriffs ließen sich auch Ausspähversuche auf bestimmte IP-Adressen identifizieren.

Die Speicherung von Verkehrsflussdaten bei Providern variiert deutlich, da es diesbezüglich keine verpflichtenden Vorgaben gibt. Auch diese gesetzliche Regelung soll

ausschließlich auf der betrieblichen Praxis aufsetzen und enthält keinerlei Verpflichtung zu besonderen Vorsorgemaßnahmen speziell für solche Abfragen. Beispielsweise wird in bekannten Implementierungen auf eine vollständige Abdeckung des Verkehrs verzichtet und der Verkehrsfluss mit vorabdefinierten Raten gespeichert. (z.B. 1 von 5.000 Verbindungen). Mangels verpflichtender Vorgaben ist auch die Speicherdauer variabel und abhängig vom Bedarf des Betreibers. Regelmäßig wird die betriebliche Speicherung lediglich für einen Zeitraum von wenigen Tagen erfolgen. Die Auskünfte nach Satz 2 Nummer 1 beziehen sich allein auf diese aus betrieblichen Gründen beim Unternehmen vorhandene Dokumentation des Verkehrsflusses.

Parameter zur Bestimmung des relevanten Verkehrsflusses kann beispielsweise eine bestimmte IP-Adresse sein, die der Angreifende für den Angriff nutzt (maliziöse Kennung). Die Auskunftspflicht dient zunächst auch der Klärung des genutzten Providers, wenn – etwa aus der Zusammenarbeit mit anderen Nachrichtendiensten – IP-Adressen bekannt werden, für die tatsächliche Anhaltspunkte dafür bestehen, dass diese zu Angriffskampagnen genutzt werden, ohne dass zunächst bekannt ist, welche IT-Infrastruktur in Deutschland dafür genutzt wird.

Zu Nummer 2

Nummer 2 bezieht sich auf Angriffswerkzeuge, die im System des Diensteanbieters vorliegen. Spuren, die technisch mit dem Angriff verbunden sind, sind eingeschlossen, beispielsweise genutzte Prozesse und Verweisungen auf Speicherorte für erbeutete Informationen. Darüberhinausgehende Inhalte der Kommunikation werden von Satz 2 nicht erfasst. Das Bundesamt für Verfassungsschutz kann den Provider bei der Erfüllung der Auskunftspflicht etwa durch die Bereitstellung notwendiger Hardware unterstützen. Erfasst sind hier auch weitere technische Informationen, die beim Diensteanbieter vorliegen. Von Bedeutung sind etwa Spuren, die technisch mit dem Angriff verbunden sind, beispielsweise genutzte Prozesse und Verweisungen auf Speicherorte für erbeutete Informationen.

Zu Absatz 2

In Absatz 2 ist sodann der Fall geregelt, dass der Verpflichtete das Auskunftsersuchen nach Absatz 1 Satz 2 Nummer 2 nicht erfüllen kann, weil ihm dies technisch nicht möglich oder zumutbar ist. In diesem Fall kann der Bundesnachrichtendienst nach entsprechender Mitteilung durch den Verpflichteten von diesem, stattdessen die Herausgabe einer Kopie der Teile des informationstechnischen Systems verlangen, deren Auswertung zum Aufspüren der verlangten Informationen erforderlich ist. Da dieses letztgenannte Herausgabeverlangen potentiell zu einer Aushändigung von einer großen Vielzahl von Daten mit denkbarerweise sehr schützenswerten Inhalten führen kann, ist in diesen Fällen eine vorherige Anordnung sowie eine Vorabkontrolle durch den Unabhängigen Kontrollrat erforderlich.

Zu Absatz 3

Absatz 3 enthält spezifische Vorgaben, um den Eingriff auf den erforderlichen Umfang begrenzt zu halten. Die nach Satz 2 nötige Auswertung der Kopien einzelner Teile eines informationstechnischen Systems orientiert sich dabei immer an technischen Parametern. Es gilt in einem ersten Schritt Logdateien und Verzeichnisstrukturen zu analysieren um beispielsweise die Frage zu klären, was auf dem System geschehen ist. Dabei können verschiedene Werkzeuge des Angreifers, wie Skripte, Exploits und Malware, identifiziert werden. In Bezug auf die Trennbarkeit von Daten findet § 56 Absatz 4 Anwendung.

Zu Absatz 4

Absatz 4 stellt klar, dass der Anbieter seine Vertragspflichten nicht verletzt, wenn er Malware oder erbeutete Daten löscht. Durch eine Sicherungskopie wird die Reversibilität gewährleistet, ebenso wie die weitere Aufklärung des Angriffs. Dazu ist die Sicherungskopie an den Bundesnachrichtendienst herauszugeben.

Zu § 15 (Ersuchen gegenüber privaten Einrichtungen der Videoüberwachung)

Zu Absatz 1

Die Regelung ermöglicht – parallel zu den in § 11 Absatz 4 geregelten Ersuchen gegenüber öffentlichen Stellen – Ersuchen gegenüber privaten Einrichtungen der Videoüberwachung.

Zu Nummer 1

Die Anlagenbetreiber haben die Mitnutzung der Überwachungseinrichtung zu dulden. Dies schließt dazu notwendige Vorbereitungen wie den Zutritt zu den betreffenden Räumlichkeiten ein.

Zu Nummer 2

Nummer 2 eröffnet auch den Zugriff auf vorhandene Aufzeichnungen. Eine Verpflichtung, dafür vorsorgende Aufzeichnungen anzufertigen, besteht nicht. Die Regelung erfasst nur die bereits für Zwecke des Betreibers ohnehin gefertigten Aufzeichnungen.

Zu Nummer 3

In Nummer 3 regelt die Echtzeitüberwachung, was die Signalausleitung aus der Anlage beinhaltet.

Zu Absatz 2

Absatz 2 regelt die erste Qualifiaktionsstufe als materielle Schwelle für die in Absatz 1 dargestellten Fälle. Ausgehändigte Aufzeichnungen (Nummer 2) sind zudem in Satz 2 mit einer besonderen Löschvorgabe belegt.

Zu § 16 (Pflichten bei Ersuchen an nicht öffentliche Stellen)

Zu Absatz 1

Absatz 1 entspricht der bisherigen Regelung in § 4 Absatz 1 Satz 2 BND-Gesetz und § 8a Absatz 4 des Bundesverfassungsschutzgesetzes und nennt die bei Auskunftsersuchen verpflichteten Stellen (der Begriff umfasst alle denkbaren natürlichen und juristischen Personen; „Dritte“, vgl. hierzu bereits oben). Wegen der unterschiedlichen Verpflichteten nach § 2 des Geldwäschegesetzes allerdings ohne weiterhin auf Unternehmen beschränkt zu sein.

Zu Absatz 2

In Absatz 2 sind die Mitwirkungspflichten für die privaten Einrichtungen der Videoüberwachung gesondert geregelt. Dabei ist neben dem Verpflichtetenkreis (Satz 1) insbesondere eine Regelung vorgesehen, nach der die Einrichtungen nicht gezwungen sind, über die bei ihnen vorhandenen technischen Mittel zusätzliche Gerätschaften zu beschaffen, um dem Bundesnachrichtendienst die Echtzeit-Ausleitung nach § 15 Absatz 1 Nummer 3 zu ermöglichen (Satz 2).

Zu Absatz 3

Durch Auskunftsersuchen kann grundsätzlich Auskunft zu allen bei einem Verpflichteten vorliegenden Daten ersucht werden. Um zu verhindern, dass überschießend Daten zu Personen übermittelt werden, die zu den betroffenen Personen zwar vorliegen, indes keinerlei Relevanz für die nachrichtendienstliche Aufklärung haben, haben die Auskunftsersuchen (abstrakt) diejenigen Daten zu enthalten, auf die sich das Auskunftsersuchen bezieht. Darüber hinaus findet sich in Absatz 3 auch die Vorgabe, dass der Bundesnachrichtendienst

die verpflichteten Stellen auf die in § 8 querschnittlich geregelten Mitwirkungs-/Vertraulichkeitspflichten hinzuweisen hat. Zuletzt ist (klarstellend) in Satz 4 geregelt, dass die – bereits aus Absatz 1 folgende – Pflicht der Auskunftserteilung unverzüglich und vollständig zu erfüllen ist.

Zu Absatz 4

Absatz 4 dient einerseits der Entkoppelung vom Bundesverfassungsschutzgesetz, indem eine eigene Vorschrift für die Entschädigungspflichten von privaten Stellen bei Auskunftspflichten geschaffen wird, die sich inhaltlich an § 20 des Artikel 10-Gesetzes und § 8d Absatz 6 des Bundesverfassungsschutzes orientiert. Besonderheiten von Informationsanforderungen des Bundesnachrichtendienstes kann künftig nach Absatz 4 Satz 2 durch eine zusätzliche, flexiblere Vereinbarungsoption Rechnung getragen werden, um angemessenere Ergebnisse auch in Sonderfällen zu gewährleisten. Dies orientiert sich inhaltlich an der bewährten Regelung des bisherigen § 25 Absatz 5. Damit wird ein praxisgerechter Handlungs-rahmen dafür eröffnet, insbesondere nähere Absprachen zur technischen Durchführung, speziell zu Übermittlungsformaten zu treffen.

Zu § 17 (Anordnungen)

Zu Absatz 1

Absatz 1 regelt das nunmehr eigenständige Anordnungsverfahren des BND-Gesetzes. Grundlage ist ein Anordnungserfordernis durch die Behördenleitung des Bundesnachrichtendienstes oder einer von ihr bestimmten Vertretung für Auskunftsersuchen nach § 13 Absatz 1 Satz 2, die sich gegen eine der in § 12 Absatz 2 Nummer 4 und 5 genannten Stellen richten, sowie von Auskunftsersuchen nach § 14 Absatz 2 Satz 3.

Das Erfordernis, dass (nur) bei diesen Auskunftsersuchen eine gesetzliche Regelung der Anordnung erforderlich ist, folgt daraus, dass es sich hierbei um besonders schützenswerte Daten handelt. Bei Auskunftsersuchen nach § 13 Absatz 1 Satz 2, die sich gegen eine der in § 12 Absatz 2 Nummer 4 und 5 genannten Stellen richten, sind solche Daten betroffen, die unter den Schutzbereich des Fernmeldegeheimnisses (Artikel 10 Absatz 1 des Grundgesetzes) fallen. In § 14 Absatz 2 Satz 3 folgt die besondere Schutzwürdigkeit demgegenüber vornehmlich daraus, dass hier eine potenziell große Vielzahl von Daten betroffen sein können. Ausgenommen ist das Anordnungserfordernis dann, wenn das Auskunftsersuchen lediglich der Umsetzung einer bereits mit einer eigenen, der Vorabkontrolle unterliegenden Anordnung dient, wie es etwa bei der Telekommunikationsüberwachung regelmäßig der Fall ist. In diesen Fällen würde das Erfordernis einer (weiteren) Anordnung nur eine bürokratische Förmelei darstellen.

Im formalen Verfahren selbst wurden keine Änderungen vorgenommen. Lediglich die Zuständigkeiten wurden – auch bedingt durch den Wegfall des Artikel 10-Gesetzes – harmonisiert, indem die Anordnungen der genannten Auskunftsersuchen nunmehr durch den Bundesnachrichtendienst selbst vorgenommen werden und der Unabhängige Kontrollrat die Rechtmäßigkeit der Anordnungen, die sich auf Personen mit deutscher Staatsangehörigkeit sowie Inländerinnen und Inländer beziehen, überprüft (§ 97 Absatz 1 Nummer 1 und 2). Die Anordnung zur Auskunftserteilung erfolgt im Außenverhältnis gegenüber der verpflichteten Stelle durch den Bundesnachrichtendienst schriftlich, vgl. § 16 Absatz 3. Bislang erfolgten die Anordnungen auf Antrag des Bundesnachrichtendienstes durch das Bundeskanzleramt nach dem derzeitigen § 3 Absatz 1 BND-Gesetz in Verbindung mit § 8b des Bundesverfassungsschutzgesetzes, bewilligende Stelle war die G 10-Kommission.

Zu Absatz 2

Absatz 2 regelt die inhaltlichen Vorgaben, die eine Anordnung des Bundesnachrichtendienstes erfüllen muss.

Zu Absatz 3

Absatz 3 trifft gesonderte, zeitlich beschränkende Vorgaben für den Fall, dass neben in der Vergangenheit erhobenen Daten auch solche übermittelt werden sollen, die erst in der Zukunft erhoben werden. Die zeitliche Grenze liegt hier bei 12 Monaten. Eine Verlängerung der Anordnung bleibt dem Bundesnachrichtendienst bei (andauerndem) Vorliegen der Voraussetzungen unbenommen.

Zu Absatz 4

Der Bundesnachrichtendienst kann im Zeitpunkt, in dem eine Anordnung einer Maßnahme getroffen wird, in gewissen Sachverhaltskonstellationen noch nicht abschließende Angaben zum betroffenen Personenkreis machen. Dies ist etwa dann der Fall, wenn der Bundesnachrichtendienst zwar damit rechnet, dass noch weitere Personen in einen Sachverhalt verstrickt sind, indes noch keine individualisierbaren Angaben zu diesen Personen möglich sind. Beispielsweise erfolgen Finanzierungstransaktionen nach nachrichtendienstlichen Erfahrungen zur Verschleierung im Wege von Überweisungsketten regelmäßig mit eingebundenen Strohpersonen. Um hier in gewissen Maßnahmen für eine nötige Flexibilität zu sorgen, kann der Bundesnachrichtendienst bereits in der Anordnung den Zusatz aufnehmen, dass die Maßnahme auch gegen weitere Personen gerichtet werden kann, bei denen – wie im späteren Verlauf klar wird – gleichermaßen die Voraussetzungen für ein Auskunftsersuchen vorlägen. Folge ist damit eine Entbürokratisierung und Flexibilisierung, ohne die materiellen Voraussetzungen der Maßnahmen zu unterlaufen.

Der Bundesnachrichtendienst muss in der Anordnung darstellen, weshalb er in dem jeweiligen Auskunftsersuchen den genannten Zusatz, der wie die Anordnung insgesamt der Vorabkontrolle durch den Unabhängigen Kontrollrat unterliegt, für angezeigt hält.

Zu Absatz 5

Entsprechend der Regelung in allen Anordnungsvorschriften wird auch hier eine Dokumentationspflicht hinsichtlich der Anordnungen begründet.

Zu Abschnitt 3 (Einsatz nachrichtendienstlicher Mittel)

Im Rahmen der durch die Rechtsprechung des Bundesverfassungsgerichts, insbesondere auch des Urteils des Bundesverfassungsgerichts vom 26. April 2022, 1 BvR 1619/17, sowie der Auflösung des Artikel 10-Gesetzes und der Auflösung der Verweise in das Bundesverfassungsschutzgesetz notwendigen Gesetzesänderungen wurde Abschnitt 3 neu eingefügt.

Geregelt wird in Unterabschnitt 1 zunächst eine allgemeine Befugnis zum Einsatz nachrichtendienstlicher Mittel und die grundsätzlichen Rahmenbedingungen eines solchen Einsatzes. Dabei entfällt durch die Entkopplung von den Regelungen des Bundesverfassungsschutzgesetzes die bislang übliche, unübersichtliche Verweisungstechnik. § 18 Absatz 1 enthält die allgemeine Befugnis zum Einsatz von nachrichtendienstlichen Mitteln mitsamt einer Legaldefinition.

Es finden sich in den Unterabschnitten 2 und 3 zudem besondere Regelungen für Einsätze bestimmter, jedenfalls in ihren denkbaren Ausgestaltungen potentiell eingriffsintensiver, nachrichtendienstlicher Mittel (Unterabschnitt 2) und für technische nachrichtendienstliche Maßnahmen (Unterabschnitt 3), die ein besonderes Eingriffsgewicht aufweisen und daher gesonderten Vorgaben bedürfen. So erhöht sich das Eingriffsgewicht von Maßnahmen der Aufklärung von Telekommunikation potentiell schon dadurch, dass sie auch aus dem eigenen staatlichen Hoheitsgebiet heraus und damit unter dem Schutz hoheitlicher Befugnisse der Bundesrepublik Deutschland in erheblichem Umfang Daten im Ausland erfassen können. Auch dieser Besonderheit wird durch die speziellen gesetzlichen Regelungen

Rechnung getragen. In Unterabschnitt 4 finden sich dann gesammelt die Vorschriften für die erforderlichen behördlichen Anordnungen der jeweiligen Maßnahmen.

Zu Unterabschnitt 1 (Allgemeine Befugnis und Vorgaben für den Einsatz nachrichtendienstlicher Mittel)

Dieser Unterabschnitt regelt die allgemeine Befugnis zum Einsatz nachrichtendienstlicher Mittel sowie grundlegende Rahmenbedingungen zum Einsatz solcher Mittel.

Vom Regelungsbereich dieses Unterabschnitts umfasst ist einerseits der Einsatz nachrichtendienstlicher Mittel gegenüber Personen, die sich im Bundesgebiet aufhalten oder sich durch ihre deutsche Staatsangehörigkeit – unabhängig von ihrem Aufenthalt – in einem besonderen Näheverhältnis zur deutschen Staatsgewalt befinden. Gleiches gilt auch für inländische juristische Personen, soweit grundrechtliche Gewährleistungen ihrem Wesen nach auf diese anwendbar sind. Andererseits regeln die hier getroffenen Vorgaben auch den Einsatz gegenüber ausländischen Staatsangehörigen im Ausland. Zur Erfüllung seines gesetzlichen Auftrags der Auslandsaufklärung kann der Bundesnachrichtendienst Informationen bei Ausländerinnen und Ausländern im Ausland, aber auch bei Personen, die sich im Bundesgebiet aufhalten, inländischen juristischen Personen oder deutschen Staatsangehörigen im Ausland erheben.

Für die rechtliche Einordnung der Maßnahme ist maßgeblich, gegenüber wen sich die nachrichtendienstliche Tätigkeit richtet und wo sie ihre jeweilige Wirkung entfaltet.

Zu § 18 (Einsatz nachrichtendienstlicher Mittel)

§ 18 regelt allgemein den Einsatz von nachrichtendienstlichen Mitteln. Es werden die bisherigen Verweise in das Bundesverfassungsschutzgesetz aufgehoben und die jeweils geltenden Voraussetzungen normenklar geregelt.

Zu Absatz 1

Die materielle Schwelle in § 18 Absatz 1 für allgemeine nachrichtendienstliche Mittel (im Gegensatz zu den gesondert geregelten nachrichtendienstlichen Mitteln der Unterabschnitte 2 und 3) ergibt sich aus der Entscheidung des Bundesverfassungsgerichts vom 26. April 2022, 1 BvR 1619/17, vgl. Rn. 181ff.: Hiernach müssen für allgemeine nachrichtendienstliche Mittel hinreichende tatsächliche Anhaltspunkte vorliegen, dass die Maßnahme im Einzelfall zur Auftragserfüllung – also zur nachrichtendienstlichen Auslandsaufklärung – geboten ist: Der konkrete Einsatz eines nachrichtendienstlichen Mittels durch den Bundesnachrichtendienst erfordert als grundsätzliche Eingriffsschwelle, dass die Maßnahme zur nachrichtendienstlichen Auslandsaufklärung, also der Gewinnung von Erkenntnissen über das Ausland, die von außen- oder sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind (§ 2 Absatz 1), erforderlich ist (Nummer 1). Nachrichtendienstliche Maßnahmen bewegen sich – im Gegensatz zu klassischen polizeilichen Maßnahmen – typischerweise im Rahmen der Früherkennung von Bedrohungen, was bei der Auslegung des Tatbestandmerkmals in den Befugnisnormen dieses Gesetzes im Einzelfall zu berücksichtigen ist. Die Bestimmbarkeit des Ziels der Maßnahme mittels einer Beschreibung dieses Ziels unter den Prämissen der Früherkennung ist ausreichend. Die nachrichtendienstliche Maßnahme kann auf die Aufklärung mehrerer Sachverhalte gerichtet sein.

Der Einsatz nachrichtendienstlicher Mittel – also auch jener, die in Unterabschnitt 2 oder 3 geregelt sind – ist nur dann zulässig, wenn diese der Erlangung von Informationen dienen, mit deren Aufklärung das Bundeskanzleramt den Bundesnachrichtendienst beauftragt hat (Nummer 2). Mit diesem Erfordernis wird sichergestellt, dass der Einsatz nachrichtendienstlicher Mittel im Einklang steht mit dem sogenannten Auftragsprofil der Bundesregierung, welches das Bundeskanzleramt im Einvernehmen mit den zuständigen Bundesministerien festlegt, oder mit konkreten Einzelweisungen des Bundeskanzleramtes, die den gesetzlichen Auftrag des Bundesnachrichtendienstes im Bedarfsfall ergänzen, etwa bei einer

kurzfristig entstehenden Krisenlage. Durch das Auftragsprofil der Bundesregierung legt die Bundesregierung Prioritäten fest, anhand derer der Bundesnachrichtendienst gemäß seinem gesetzlichen Auftrag Erkenntnisse von außen- oder sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland zu beschaffen hat. Das Erfordernis der Beauftragung gilt für den Einsatz sämtlicher in diesem Abschnitt geregelter nachrichtendienstlicher Mittel. Die notwendigen „Annexe“ zur eigentlichen Aufgabe (namentlich Eigensicherung und Eigenbefähigung) sind, auch soweit sie nicht Auftragsprofil der Bundesregierung enthalten sind, gleichermaßen Gegenstand der Beauftragung durch das Bundeskanzleramt. Dies folgt bereits daraus, dass es sich hierbei zwar denkbarerweise nicht (oder nur mittelbar) um eine Aufklärung des Auslands handelt, aber gleichwohl die entsprechenden Einsätze nachrichtendienstlicher Mittel zwingend erforderlich sind.

In Nummer 3 ist – klarstellend – aufgeführt, dass die in den Unterabschnitten 2 und 3 enthaltenen Befugnisse zum Einsatz besonders eingriffsgewichtiger nachrichtendienstlicher Mittel der allgemeinen Vorschrift des § 18 Absatz 1 vorgehen.

§ 18 Absatz 1 enthält keinen abschließenden Katalog einzelner nachrichtendienstlicher Mittel. Eine abschließende Positivliste zulässiger nachrichtendienstlicher Mittel würde bedingen, dass neue nachrichtendienstliche Fähigkeiten jeweils zunächst einer Gesetzesänderung bedürften. Die entsprechenden Fähigkeiten stünden damit, falls überhaupt, erst mit einem nennenswerten zeitlichen Verzug zur Verfügung. Darüber hinaus wäre dadurch bereits die Entwicklung neuer nachrichtendienstlicher Fähigkeiten begrenzt, so dass kritische Entwicklungen verpasst werden könnten. Dies entspricht auch der Empfehlung der Initiative für einen handlungsfähigen Staat für Flexibilität und Entwicklungsoffenheit (vgl. Abschlussbericht, vorgelegt am 14. Juli 2025, S. 32, 33). Gleichwohl enthält § 18 Absatz 1 erstmalig für das BND-Gesetz eine Legaldefinition des Begriffs des nachrichtendienstlichen Mittels. Danach darf der Bundesnachrichtendienst Methoden, Gegenstände und Instrumente zur heimlichen Beschaffung von Informationen einsetzen. Das Merkmal der „Heimlichkeit“ meint, dass die Informationsbeschaffung durch den Bundesnachrichtendienst eigenständig und direkt ohne Kenntnis der vom Informationsinteresse erfassten Person bzw. Stelle erfolgt.

Die Kontrolle des parlamentarischen Raums über den Umfang und den Einsatz nachrichtendienstlicher Mittel des Bundesnachrichtendienstes ist dabei durch die Unterrichtungspflicht des parlamentarischen Kontrollgremiums über die im Bundesnachrichtendienst vorhandenen nachrichtendienstlichen Mittel (siehe dazu auch § 95; abschließende Aufzählung der nachrichtendienstlichen Mittel) sowie auch über den Einsatz neuer nachrichtendienstlicher Mittel zur Erprobung umfassend gewahrt. Beim Einsatz neuer nachrichtendienstlicher Mittel unterliegen diese auch vorab der Rechtskontrolle durch den Unabhängigen Kontrollrat.

Rechtsstaatlichen Vorgaben wird auch durch einen nicht abschließenden Katalog nachrichtendienstlicher Mittel Rechnung getragen. Der Gesetzgeber schafft hier normenklare und hinreichend bestimmte Regelungen. Die Normenklarheit ist dadurch gewährleistet, dass die Regelung deutlich macht, dass der Bundesnachrichtendienst heimlich mit als Methodik benannten unterschiedlichen Vorgehensweisen zur Erfüllung seiner Aufgaben tätig wird. Hinreichend bestimmt ist die Regelung, da das staatliche Handeln klar umrissen und in einen verfassungskonformen gesetzlichen Rahmen eingebunden ist. Dies erfolgt durch auf die Behörde zugeschnittene typologische gesetzliche Ausformung der eingriffsintensiven nachrichtendienstlichen Maßnahmen (Sondernormen mit jeweils eigenen Voraussetzungen, die gegenüber der allgemeinen Befugnis des § 18 Absatz 1 vorrangig sind, Nummer 3). Zudem unterliegt jeglicher Einsatz nachrichtendienstlicher Mittel dem Verhältnismäßigkeitsgrundsatz, der gleichzeitig auch gebietet, dass der Einsatz neuer nachrichtendienstlicher Mittel insbesondere im Hinblick auf ihre Auswirkung bei Betroffenen nur unter den Voraussetzungen angewendet wird, die für nachrichtendienstliche Mittel mit vergleichbaren Auswirkungen gelten. Dies findet sich auch in der Regelung des § 19 wieder. Der Einsatz neuer nachrichtendienstlicher Mittel, die noch nicht den Eingang in eine darauf zugeschnittene,

typisierte gesetzliche Regelung gefunden haben, ist zudem durch die unabhängige Kontrolle des Unabhängigen Kontrollrates abgesichert.

In § 18 Absatz 1 Satz 2 sind – den vorstehenden Ausführungen zu dem nicht-abschließenden Charakter der Vorschrift entsprechend – beispielhaft Maßnahmenarten aufgeführt, die abhängig von ihrer Durchführungsart als nachrichtendienstliche Mittel anzusehen sein können. Dies sind etwa der Einsatz nachrichtendienstlicher Verbindungen oder technischer Mittel sowie die Inbesitznahme von Sachen zu deren heimlicher Auswertung, wobei letzteres wiederum nicht nur durch den Bundesnachrichtendienst selbst, sondern insbesondere auch durch nachrichtendienstliche Verbindungen erfolgen kann. Zudem muss die Inbesitznahme letztlich der Auswertung dienen, eine Unmittelbarkeit ist nicht verlangt. So kann etwa ein mobiles Endgerät vorübergehend heimlich in Besitz genommen und unter Beachtung der Vorgaben der § 37 ff. manipuliert werden, ohne dass eine direkte Datenauswertung erfolgt. Mittelbar dient dieses Vorgehen jedoch der Erlangung von Informationen. In Satz 3 ist eine Pflicht zur Rückgabe von Gegenständen enthalten, welche in Besitz genommen wurden. Diese Pflicht setzt voraus, dass der Eigentümer oder berechtige Inhaber der tatsächlichen Gewalt dem Bundesnachrichtendienst bekannt ist. Darüber hinaus kommt eine Rückgabe nur in Betracht, wenn die Auswertung, zu deren Zweck die Sache in Besitz genommen wurde, abgeschlossen ist. Sollte eine solche Auswertung aufgrund von technischen oder sonstigen Umständen nicht oder nicht abschließend möglich sein, so besteht eine Rückgabepflicht nicht. Gleiches gilt endlich für den Fall, dass überwiegende Sicherheitsinteressen einer Rückgabe entgegenstehen. Der Begriff der überwiegenden Sicherheitsinteressen ist dabei weit zu verstehen und umfasst die Bedeutung der Sache für die nachrichtendienstliche Aufklärung, operativ-sicherheitliche Aspekte, Geheimschutzaspekte sowie den Schutz eingesetzter Personen. Diesen Interessen ist im Rahmen einer Gesamtabwägung das Interesse des Eigentümers oder berechtigen Inhabers der tatsächlichen Gewalt an einem Rückerhalt der Sache entgegenzustellen. Dieses Rückerhaltinteresse wird dabei dadurch gemindert, dass die in Besitz genommene Sache im Zusammenhang mit einer Bedrohung Verwendung gefunden hat.

Zu Absatz 2

Absatz 2 ermöglicht zur Vorbereitung und Durchführung der Maßnahme einen heimlichen Zutritt zu Gebäuden und Räumen, was das Überwinden von Zutrittssperren einschließt. Der annexe Eingriff in die Wohnung unterliegt den in Satz 2 vorgesehenen erhöhten Voraussetzungen, welche verfassungsgerichtlich determiniert sind (BVerfGE 165, 1 – Ls. 2, Rn. 147 ff., 155). Satz 3 stellt klar, dass Voraussetzungen für besondere Maßnahmen nicht unterlaufen werden dürfen.

Zu Absatz 3

Der Begriff der konkretisierten Gefahr wurde vom Bundesverfassungsgericht 2016 in seiner Entscheidung zum Bundeskriminalamtsgesetz geprägt. In Abgrenzung zum etablierten polizeirechtlichen Begriff der konkreten Gefahr versteht das Gericht darunter eine Sachlage, bei der die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs bis zum Eintritt einer Rechtsgutsverletzung reduziert sind. Die der erforderlichen Prognose zugrundeliegenden Anknüpfungspunkte können also eine größere Unschärfe aufweisen. Im Bereich des Polizeirechts ist die konkretisierte Gefahr allgemein durch zwei Elemente gekennzeichnet: erstens die Möglichkeit eines typisierenden Schlusses auf eine Rechtsgutsverletzung („Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen“) und zweitens auf die Beteiligung bestimmter Personen, gegen die die polizeiliche Maßnahme gerichtet werden kann. In Bezug auf terroristische Straftaten reduziert das Bundesverfassungsgericht weiter die prognostischen Anforderungen an die Art und den zeitlichen Abstand der Rechtsgutsverletzung. Unverzichtbar ist dabei stets, dass die Prognose im Tatsächlichen wurzelt. Es müssen „zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen“ (BVerfG, Urteil vom 20. April 2016, 1 BvR 966, Rn. 112). In der Folge hat das Bundesverfassungsgericht diese

Rechtsprechung weiter konsolidiert und auch auf nachrichtendienstliche Sachverhalte angewendet (BVerfG, Urteil vom 19.°Mai 2020, 1°BvR°2835/17, Rn.°266,°269; BVerfG, Urteil vom 26.°April 2022, 1°BvR°1619/17, Rn.°245ff.,°261; BVerfG, Beschluss vom 28.°September 2022, 1°BvR°2354/13, Rn.°132ff.). Diese Rechtsprechung wurde schließlich von den Fachgerichten aufgegriffen und weiterentwickelt (vgl. nur BGHSt°66,°1ff.; BVerwG NVwZ°2022,°1802 Rn.°37 f.; HmbOVG, NVwZ°2022,°1219 Rn.°40 m.w.N.). Eine konkretisierte Gefahr setzt voraus, dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen (BVerfG, Beschluss vom 28.°September 2022, 1°BvR°2354/13, Rn.°134), also Anhaltspunkte, die den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Störungsgeschehen zulassen (BVerfG, Urteil vom 26.°April 2022, 1°BvR°1619/17, Rn.°158). Der Rechtsbegriff der konkretisierten Gefahr kann vor diesem Hintergrund als ausreichend durch die Rechtsprechung konturiert angesehen werden, um dem verfassungsrechtlichen Gebot der Bestimmtheit zu genügen und für den Anwender operabel zu sein.

Die „konkretisierte Gefahr“ knüpft an die Wahrscheinlichkeit eines drohenden Schadens an. Bei den – zum Teil eher abstrakten, z.B. die freiheitliche demokratische Grundordnung oder die Sicherheit des Bundes, eines Landes oder einer internationalen Organisation – Rechtsgütern des § 2 Absatz 2 ist indes selbst ein bereits eingetretener Schaden bzw. eine bereits eingetretene Störung oftmals schwierig zu bestimmen. Eindeutig ist eine Bestimmung eines Schadens jedenfalls dann, wenn bereits entsprechende Schutznormen verletzt werden. Dies ist etwa der Fall, wenn konkrete Delikte begangen werden, die bereits einen unmittelbaren Bezug zu einem besonders gewichtigen Rechtsgut im hier verwandten Sinne haben. Aber auch ein mittelbarer Bezug, der daraus entsteht, dass die tatbestandliche Verwirklichung sich gegen diese Schutzgüter richtet (praktisch indiziert durch den äußeren und inneren Zusammenhang der jeweiligen Tatbestandsverwirklichung), muss aufgrund der genannten Abgrenzungsschwierigkeiten hinreichend sein, um eine konkretisierte Gefahr zu begründen. Ein Beispiel hierfür ist etwa, die konkretisierte Gefahr einer Sachbeschädigung, die gegen eine Botschaft gerichtet ist, und sich damit (auch) auf ein besonders gewichtiges Rechtsgut im Sinne von § 2 Absatz 2 (hier die außenpolitische Handlungsfähigkeit) erstreckt. Diese instrumentelle Sicht lag bereits dem bisherigen § 9f Absatz 3 zugrunde und ist weiterhin maßgebend.

Zu § 19 (Besonderer Einsatz nachrichtendienstlicher Mittel)

Zu Absatz 1

Als Auslandsnachrichtendienst ist der Bundesnachrichtendienst auf den zügigen Einsatz neuer (insbesondere technischer oder digitaler) Fähigkeiten angewiesen, um unter oft dynamischen außenpolitischen oder sicherheitspolitischen Bedingungen seinem gesetzlichen Auftrag effektiv nachkommen zu können. Der Bundesnachrichtendienst benötigt ein breites, modernes sowie innovationsorientiertes Fähigkeitsspektrum, um die sicherheitspolitischen Ziele, Interessen und Prioritäten Deutschlands unterstützen zu können.

Um auch beim Einsatz neuer nachrichtendienstlicher Mittel zur Entwicklung und Erprobung die Verfassungskonformität umfassend zu gewährleisten, wird festgelegt, dass der Einsatz neuer nachrichtendienstlicher Mittel durch den Unabhängigen Kontrollrat kontrolliert wird (siehe zur Festlegung der Vorabkontrolle den zentralen Katalog in § 97 Absatz 1). Dieser prüft den konkreten Einsatz sowie auch die Zuordnung des neuen nachrichtendienstlichen Mittels in das mit dieser Novelle eingeführte Stufensystem. Der unabhängige Kontrollrat legt also anhand der in diesem Gesetz getroffenen gesetzgeberischen Wertungen fest, ob das neue nachrichtendienstliche Mittel unter den Voraussetzungen des § 18 Absatz 1 eingesetzt werden kann, oder ob es sich um ein eingriffsintensives nachrichtendienstliches Mittel handelt. Handelt es sich um ein eingriffsintensives nachrichtendienstliches Mittel erfolgt der Einsatz in der Entwicklungs- und Erprobungsphase unter den hier in diesem Absatz festgelegten Voraussetzungen (der höchsten Stufe). Da der Gesetzgeber diese in ihrer Entwicklungs- und Erprobungsphase noch nicht in einer Sondernorm mit spezifischen

materiellen und/oder formellen Voraussetzungen erfassen konnte, werden für diese Phase besondere materielle Voraussetzungen festgelegt, unabhängig davon, welche Festlegungen durch den Gesetzgeber später für dieses neue nachrichtendienstliche Mittel getroffen werden.

Es ist für die dauerhafte Gewährleistung der Funktionsfähigkeit des Bundesnachrichtendienstes von essentieller Bedeutung, dass neben konkreten Regeln für etablierte nachrichtendienstliche Mittel auch die Entwicklung und der Einsatz neuer nachrichtendienstlicher Fähigkeiten möglich bleiben. Von dieser Regelung umfasst sind z.B. weiterentwickelte oder neuartige Technologien zum Zwecke der Erfassung, Aufklärung, Überwachung oder Verschleierung mittels autonomer oder neuartiger prototypischer Systeme. Alle zum Zeitpunkt des Gesetzgebungsverfahrens bekannten und genutzten eingriffsintensiven nachrichtendienstlichen Mittel wurden im Rahmen von Spezialnormen berücksichtigt.

Anwendungsfälle neuer nachrichtendienstliche Mittel könnten z.B. die Verbringung neuartiger, aktiver oder passiver Materialien für Geolokalisierungen oder der Einsatz bionischer Drohnen sein.

Die nachrichtendienstlichen Fähigkeiten müssen sich an den beschleunigten technischen Fortschritt anpassen, auch insofern, als dass sie nicht bloß technische Varianten bereits vorhandener nachrichtendienstlicher Fähigkeiten darstellen. Eine Entwicklung, die zudem einer Entwicklungs- und Erprobungsphase zum Ausbau solcher Fähigkeiten bedarf, kann nur vollzogen werden, wenn die gesetzliche Befugnis zum Einsatz von nachrichtendienstlichen Mitteln keine abschließende Aufzählung der zum Zeitpunkt der Gesetzgebung bekannten und bewährten nachrichtendienstlichen Mitteln enthält.

Erst die Entwicklung und die diese begleitende Anwendung neuer nachrichtendienstlicher Mittel versetzt schließlich auch den Gesetzgeber in die Lage, neue Befugnisse mit passenden materiellen und formellen Anwendungsvoraussetzungen überhaupt treffend formulieren zu können. Die gesetzliche Regelung einer nachrichtendienstlichen Methode oder eines Mittels ist in der Regel erst möglich, wenn die relevanten Umrisse einer Fähigkeit und deren Einsatzmöglichkeiten erprobt wurden. Die Beschränkung des Bundesnachrichtendienstes auf den Einsatz lediglich gesetzlich geregelter nachrichtendienstlicher Mittel könnte damit einen unvertretbaren Verlust an nachrichtendienstlich relevanten Informationen bedeuten, der regelmäßig nicht durch den Einsatz anderer nachrichtendienstlicher Mittel kompensiert werden könnte.

Zudem dient die Entwicklung neuer nachrichtendienstlicher Mittel der effektiven Aufgabenerfüllung des Bundesnachrichtendienstes, denn das Aufklärungsziel der Gewinnung von Informationen mit außen- oder sicherheitspolitischer Bedeutung bringt die Notwendigkeit der Anpassung und Fortentwicklung der eingesetzten nachrichtendienstlichen Mittel mit sich. Gerade das Ziel der Auslandsaufklärung verlangt die Anpassung der Aufklärungstätigkeit an weltweit – insbesondere auch durch andere Staaten – vollzogene Weiterentwicklungen mit Blick auf den Schutz ihrer Informationen. Um seinem gesetzlichen Auftrag nachzukommen, ist der Bundesnachrichtendienst gehalten, seine Aufklärungsfähigkeiten kontinuierlich weiterzuentwickeln und an Lageentwicklungen anzupassen. Der Bundesnachrichtendienst hat hierzu einen Organisationsbereich eingerichtet, der sich mit Forschung und innovativen Technologien beschäftigt. Zukunftstrends werden dabei mittels projektbasierter Forschung und Entwicklung verfolgt.

Durch die in § 19 Absatz 1 enthaltenen sehr hohen materiellen Voraussetzungen wie auch durch die zeitliche Begrenzung der Erprobung wird sichergestellt, dass grundrechtsintensiv wirkende nachrichtendienstliche Maßnahmen in ihrer Entwicklungs- und Erprobungszeit nur unter adäquaten bzw. sogar besonders hohen Schwellen durchgeführt werden. Nach einer erfolgreichen Entwicklung und Erprobung eines neuen nachrichtendienstlichen Mittels kann dieses dann typisiert als neue Befugnis in das BND-Gesetz aufgenommen und ggf. entsprechend der dann erfolgten gesetzgeberischen Bewertung mit differenzierten

materiellen und formellen Voraussetzungen gesetzlich geregelt werden. Wirken neuen nachrichtendienstliche Mittel in der Regel nicht vergleichbar grundrechtsintensiv wie die in Unterabschnitt 2 geregelten Maßnahmen, fallen sie nicht unter diese Vorschrift, sondern können auf Grundlage des § 18 eingesetzt werden.

Zu Absatz 2

Durch § 19 Absatz 2 ist sichergestellt, dass die jeweilige Eingriffsintensivität einer Maßnahme berücksichtigt wird.

In Unterabschnitt 2 werden nachrichtendienstliche Maßnahmen des Bundesnachrichtendienstes geregelt, die gegenüber Betroffenen besonders eingriffsintensiv wirken und daher mit spezieller Regelung an erhöhte Voraussetzungen gebunden werden. Neben diesen speziellen Tatbeständen muss aber ergänzend auch berücksichtigt werden, dass nachrichtendienstliche Maßnahmen, die typischerweise kein erhebliches Eingriffsgewicht erlangen, unter außergewöhnlichen Umständen durchaus den in § 18 geregelten Rechtfertigungsrahmen übersteigen können.

Beispielsweise können bei Informationsgewinnung durch eine nachrichtendienstliche Verbindung, die üblicherweise vollständig von § 18 Absatz 1 getragen ist, nicht nur ungezielt auch umfassende höchstprivate Informationen über das Aufklärungsziel anfallen. Aufgrund außergewöhnlicher Umstände können solche Informationen einerseits von spezifischem Aufklärungsinteresse sein und andererseits aufgrund einer besonderen Nähebeziehung zum Aufklärungsziel systematisch abgeschöpft werden. Dies kann im Einzelfall nicht mehr angemessen nach Maßgabe der Voraussetzungen des § 18 erfolgen. Insofern enthält § 19 Absatz 2 einen Qualifikationstatbestand mit qualifizierten Voraussetzungen, sobald der Einsatz des nachrichtendienstlichen Mittels nach § 18 zu einer vergleichbar gewichtigen Eingriffsintensität führt wie der Einsatz der in Unterabschnitt 2 geregelten nachrichtendienstlichen Maßnahmen.

Da es sich hier um eine Auffangregelung für atypische Sondersachverhalte handelt, sind naturgemäß – anders als bei den in Unterabschnitt 2 genannten Mitteln – keine spezifizierten Sachverhalte tatbestandlich bezeichnet, sondern unmittelbar die Kriterien, die der Verfassungsrechtsprechung folgend (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 191) den Vorgang als im Sinne der vorgehenden Qualifikationstatbestände eingriffsintensive nachrichtendienstliche Maßnahme bestimmen. Dauerhaft persönliche Vertrauensbeziehungen beschreibt eine nachhaltig in der Privatheit aufgebaute Vertraulichkeit, in Abgrenzung etwa zu Vertrauensbeziehungen im Geschäftsverkehr oder weniger intensiven privaten Beziehungen, etwa im Vereinsleben. Die Erfassung der Persönlichkeit setzt nicht erst mit der Erstellung eines umfassenden Persönlichkeitsbildes ein, sondern bezieht bereits ein, wenn wesentliche Elemente der Persönlichkeit erfasst werden, wenn etwa verschiedene private Lebensbereiche nicht nur punktuell, sondern umfassend Gegenstand der nachrichtendienstlichen Aufklärung werden.

Zu § 20 (Einsatz nachrichtendienstlicher Mittel gegen eine Person)

In § 20 ist der Einsatz nachrichtendienstlicher Mittel geregelt, der sich gegen eine natürliche Person richtet. Die hier geregelten Voraussetzungen gelten dabei sowohl für den gegen eine Person gerichteten Einsatz allgemeiner nachrichtendienstlicher Mittel nach § 18 Absatz 1 als auch für den gegen eine Person gerichteten Einsatz der besonders geregelten nachrichtendienstlichen Mittel in Unterabschnitt 2. Die in Unterabschnitt 3 geregelten Maßnahmen der technischen Aufklärung enthalten hingegen eigene Vorgaben für den Einsatz „gegen eine Person“.

Zu Absatz 1

In Absatz 1 ist definiert, wann ein nachrichtendienstliches Mittel gegen eine Person gerichtet ist. Dies ist dann der Fall, wenn sie mit dem Ziel einer systematischen Sammlung von

Informationen zu dieser Person erfolgt, also die Person selbst in unmittelbarem Interesse der Aufklärung steht. Üblicherweise zielt der Einsatz nachrichtendienstlicher Mittel durch den Bundesnachrichtendienst demgegenüber darauf ab, Wissen und Kenntnisse von Personen zu auftragsrelevanten Themen oder Bereichen zu erlangen. Derartige Maßnahmen fallen dementsprechend nicht unter diese Norm; auch dann nicht, wenn die Aufklärung „mittelbar“ über eine Person erfolgt, etwa bei der Aufklärung einer Proliferationsbedrohung durch nachrichtendienstlichen Mitteleinsatz gegen einen Wissenschaftler.

Es ist also beispielsweise zu unterscheiden, ob eine Observation der Lageaufklärung eines Ortes dient oder im obigen Sinne gezielt gegen eine Person gerichtet ist. So ist z.B. die Observation zur Absicherung rund um einen Treffort mit einer nachrichtendienstlichen Verbindung oder die Observation eines Gebäudes, um festzustellen, wer dort ein- und ausgeht, zu unterscheiden von der Observation einer Person, bei der ihre persönlichen Lebensumstände aufgeklärt werden sollen und so über die gesamte Zeitdauer der Maßnahme dieser Person gefolgt wird, um deren Tagesablauf, Kontakte und Gewohnheiten zu erkennen. Allein die Tatsache, dass eine Person von einer nachrichtendienstlichen Maßnahme betroffen ist, bedeutet nicht, dass sich eine Maßnahme gegen diese Person richtet. Als gegen eine Person gerichtet muss eine Maßnahme des Bundesnachrichtendienstes betrachtet werden, wenn diese typischerweise dazu führt, dass die Erhebung der gewünschten Informationen mit einem tiefgehenden Einblick in die persönlichen Lebensumstände der Person verbunden ist. Dies ist in der Regel nicht der Fall, wenn der Bundesnachrichtendienst lediglich unter Mithilfe des Wissens oder der Kenntnisse einer Person, die diese beispielsweise im Rahmen ihrer beruflichen Tätigkeit erworben hat, einen Themenbereich oder eine Region aufklären möchte.

Zu Absatz 2

In Absatz 2 wird der Einsatz von nachrichtendienstlichen Mitteln gegen Personen für solche nachrichtendienstlichen Mittel geregelt, die sich – anders als etwa bei der Telekommunikationsüberwachung nach § 35, der Online-Durchsuchung nach § 37 Absatz 2 oder 3 oder der Verwendung eingriffsintensiver nachrichtendienstlicher Verbindungen nach § 24 – nicht schon aufgrund ihrer Natur gegen eine Person richten. Die Regelung greift die Rechtsprechung des Bundesverfassungsgerichts auf (vgl. mit Blick auf die Tätigkeit der Verfassungsschutzbehörden BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 206: „Ist die Maßnahme gezielt gegen bestimmte Personen gerichtet, muss insbesondere gerade die Überwachung dieser Person zur Aufklärung beitragen“).

Die Aufklärung von Personen, die im Zusammenhang mit dem Erkenntnisziel stehen, hat bei einer gegen Personen gerichteten Maßnahme Vorrang gegenüber der Aufklärung einer unbeteiligten Person. Dabei ist der Begriff des Zusammenhangs weit zu verstehen, wobei – ggf. auch durch besondere Fähigkeiten oder Kontakte der jeweiligen Person – ein Bezug zum Aufklärungsziel anzunehmen sein und so eine nicht unerhebliche Wahrscheinlichkeit bestehen muss, dass der Einsatz nachrichtendienstlicher Mittel gegen diese Person dem Erkenntnisziel dienlich sein wird (vgl. BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 212).

Es sind also gegen Personen gerichtete nachrichtendienstliche Maßnahmen auch gegen weitere Personen zulässig, wenn die Information nicht anders zu erlangen ist. Gänzlich unbeteiligte Personen können damit nur nachrangig von einer gezielt gegen eine Person gerichteten nachrichtendienstlichen Maßnahme betroffen werden, dies kann jedoch gerade bei der Auslandaufklärung zur effektiven Aufgabenerfüllung notwendig werden. Aufgrund der bei der Auslandsaufklärung erschwerten Rahmenbedingungen der nachrichtendienstlichen Tätigkeit müssen, um die Effektivität der Aufgabenerfüllung gewährleisten zu können, auch nachrichtendienstliche Mittel gegenüber Personen eingesetzt werden können, die nicht selbst Teil des Aufklärungsziels sind oder mit diesem in einem Zusammenhang zu stehen, sondern z.B. lediglich Wissensträger sind, also sich durch Kenntnisse über für den

Bundesnachrichtendienst auftragsrelevante Themen oder Regionen auszeichnen, ohne selbst Teil einer Bedrohung zu sein.

Zu Absatz 3

Richtet sich die eingriffsintensive nachrichtendienstliche Maßnahmen nach Unterabschnitt 2 gegen eine Person, gelten die zusätzlichen Vorgaben in diesem Absatz. Weniger eingriffsintensive, gezielt gegen Personen gerichtete nachrichtendienstliche Maßnahmen, sind allerdings auch gegen andere, als die in Absatz 3 genannten, deutschen Staatsangehörigen oder sich im Bundesgebiet aufhaltende Personen zulässig. Insoweit gilt Absatz 2.

Nach der Rechtsprechung des Bundesverfassungsgerichts (vgl. BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17) ist der Betroffenenkreis bei eingriffsintensiven nachrichtendienstlichen Maßnahmen einzuschränken. Diese Rechtsprechung bezieht sich auf die Tätigkeit der Verfassungsschutzbehörden und damit vornehmlich auf eine nachrichtendienstliche Inlandstätigkeit, also auf das Tätigwerden gegenüber deutschen Staatsangehörigen oder Personen, die sich im Bundesgebiet aufhalten. Danach steigen mit der Eingriffsintensität der Maßnahme die verfassungsrechtlichen Anforderungen an die Beziehung der von der Überwachung betroffenen Person zu der aufzuklärenden Aktion oder Gruppierung (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 212).

Dem wird gefolgt, indem in Absatz 3 Satz 1 bei eingriffsintensiven Maßnahmen gegen deutsche Staatsangehörige oder sich im Bundesgebiet aufhaltenden Personen der Betroffenenkreis in ihrer gezielten Anwendung gegen Personen beschränkt wird (vgl. Nummern 1 bis 2). Die Ausgestaltung der gesetzlichen Regelung in diesem Absatz mit ihrer Bezugnahme auf deutsche Staatsangehörige oder sich im Bundesgebiet aufhaltende Personen, trägt in verfassungsrechtlicher Hinsicht dem Umstand Rechnung, dass die nachrichtendienstliche Maßnahme gegenüber einer Ausländerin oder einem Ausländer im Ausland ein geringeres Eingriffsgewicht aufweist. Diese Personengruppe unterliegt typischerweise nicht dem Zugriff deutscher Behörden und ist damit in deutlich verringertem Ausmaß Folgemaßnahmen ausgesetzt, vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17 (154, 152), Rn. 186.

Zulässig ist der Einsatz von nachrichtendienstlichen Mitteln gegen Deutsche/Inländer, die für die aufzuklärende (erhebliche) Bedrohung verantwortlich ist oder diese fördert (Nummer 1). Für Nummer 2 wird auf die Begründung zu § 13 Absatz 2 Nummer 3 Bezug genommen. Auch hier gibt ein „Zusammenhang mit dem Aufklärungsziel“ insbesondere dann Grund zu der Annahme, dass Erkenntnisse gewonnen werden können, wenn sich die Maßnahme gegenüber Nachrichtenmittlerinnen oder Nachrichtenmittlern richtet, wobei insoweit auch die unbewusste oder nicht-willentliche Mitteilung entsprechender Nachrichten umfasst ist. Zulässig ist der Einsatz nachrichtendienstlicher Mittel nach Nummer 2 ferner auch gegen abgrenzbare „Netzwerke“, wobei hier nicht die Verantwortlichkeit einer einzelnen Person in Rede steht, sondern die von dem Netzwerk als solches ausgehende Bedrohung (vgl. hierzu auch die Begründung zu § 13 Absatz 2).

Richtet sich die eingriffsintensive nachrichtendienstliche Maßnahmen dagegen nicht gezielt gegen Personen (z.B. die längerfristige Observation eines Ortes zur Lageaufklärung) sind die von der nachrichtendienstlichen Maßnahme betroffenen Personen in der Regel nicht tiefgehend von der Maßnahme des Bundesnachrichtendienstes betroffen.

Zu Absatz 4

Die in Absatz 4 enthaltene Ausnahme ist erforderlich, um die Eignung einer Person als nachrichtendienstliche Verbindung im anfänglichen Forschungsprozess sowie im Verlauf der Zusammenarbeit insbesondere auch im Interesse der Sicherheit der Mitarbeitenden des Bundesnachrichtendienstes zu ermitteln und festzustellen. So sind zur Beurteilung der operativen Sicherheit für die nachrichtendienstliche Verbindung selbst, für die Mitarbeitenden des Bundesnachrichtendienstes als auch für Dritte, Erkenntnisse zur Person der

nachrichtendienstlichen Verbindung notwendig. Auch ist eine laufende Überprüfung von nachrichtendienstlichen Verbindungen erforderlich. Eine solche liegt u.a. auch im Interesse der nachrichtendienstlichen Verbindung, z.B. aus Fürsorgegesichtspunkten, um ggf. neue, aber auch laufende Risiken überhaupt erkennen und beurteilen zu können. Die Eingriffsintensität gegenüber dem Betroffenen ist in diesen Fällen geringer zu gewichten, da das nachrichtendienstliche Mittel nicht eingesetzt wird, um Informationen zu gewinnen, die in Produkte des Bundesnachrichtendienstes einfließen sollen. Auch sind Folgemaßnahmen, die bei Übermittlung der Daten an andere Behörden drohen können, in diesen Fällen nur in absoluten Ausnahmefällen denkbar.

Bei dem Einsatz eines nachrichtendienstlichen Mittels gegen eine Person bei der Prüfung ihrer Eignung und Verwendung als nachrichtendienstliche Verbindung im Rahmen des Absatzes 4 ist dabei zu beachten, dass die vom jeweiligen nachrichtendienstlichen Mittel geforderte, materielle Erhebungsschwelle nicht an die Person selbst anknüpft, sondern an den Lebenssachverhalt, der mittels ihrer Verwendung nachrichtendienstliche Verbindung aufgeklärt werden soll. Entscheidend ist also, ob die Person als nachrichtendienstliche Verbindung Verwendung findet bzw. finden soll, um z.B. eine Bedrohung von herausgehobener Bedeutung aufzuklären, und nicht, dass die Person diese Bedrohung selbst begründet.

Zu § 21 (Schutz des Kernbereichs privater Lebensgestaltung)

Der Schutz des Kernbereichs privater Lebensgestaltung ist verfassungsrechtlich geboten und erfordert spezielle Regelungen für Maßnahmen, die zur Erhebung kernbereichsrelevanter Daten führen (BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17, Rn. 278).

Der Schutz des Kernbereichs privater Lebensgestaltung gewährleistet dem Individuum einen Bereich höchstpersönlicher Privatheit und sichert einen dem Staat nicht verfügbaren Menschenwürdekern grundrechtlichen Schutzes gegenüber Überwachung. Selbst überragende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Bereich privater Lebensgestaltung nicht rechtfertigen. Dies gilt auch gegenüber Nachrichtendiensten und auch für Aufklärungsmaßnahmen im Ausland. Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge, Überlegungen und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen. Geschützt ist insbesondere die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens, die in der berechtigten Annahme geführt wird, nicht überwacht zu werden (vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17 (154, 152), Rn. 200f.).

Dies ist in § 21 umfassend in Bezug auf nachrichtendienstliche Maßnahmen umgesetzt. Der Schutz des Kernbereichs privater Lebensgestaltung wird nunmehr zusammenfassend in § 21 für die in dem Abschnitt 3 normierten Befugnisse geregelt. Die Regelungen der bisherigen §§ 22, 31 Absatz 4 Nummer 3 Buchstabe d, und § 32 Absatz 3 Nummer 2 Buchstabe a) und Absatz 4 Nummer 2, sowie § 36 gehen in dieser Regelung auf. Weiterhin findet sich demgegenüber – aufgrund der spezifischen Besonderheiten des Artikel 13 des Grundgesetzes; der Privatwohnung als „letztes Refugium und Mittel zur Wahrung der Menschenwürde“ – eine spezielle Regelung zum Schutz des Kernbereichs privater Lebensgestaltung für die Wohnraumüberwachung in der diesbezüglichen Regelung des § 29.

Zu Absatz 1

Der Schutz des Kernbereichs privater Lebensgestaltung ist strikt. Dem trägt Absatz 1 Rechnung. Nach Absatz 1 ist insbesondere die gezielte Erhebung von Informationen über den Kernbereich privater Lebensgestaltung unzulässig, vgl. BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17, Rn. 275ff. (277, 278). Gleiches gilt dann, wenn zwar keine gezielte Erhebung beabsichtigt ist, aber tatsächliche Anhaltspunkte bestehen, dass nur kernbereichsrelevante Informationen von der Maßnahmen erhoben würden. Insoweit wird der Tatbestand des bisherigen (freilich nur für die strategische Aufklärung einschlägigen) § 22 BND-Gesetz erweitert.

Absatz 1 entzieht inhaltlich intime Gedanken wie auch die nichtöffentliche Kommunikation, wenn sie in höchstpersönlichen Vertrauensbeziehungen unter besonders schutzwürdigen Umständen erfolgt, pauschal der nachrichtendienstlichen Erhebung durch den Bundesnachrichtendienst. Geschützt sind die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, sowie insbesondere die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens, die in der berechtigten Annahme geführt wird, nicht überwacht zu werden, wie es insbesondere bei Gesprächen im Bereich der Wohnung der Fall ist (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 121).

Der Kernbereich privater Lebensgestaltung ist nicht gleichbedeutend mit höchstprivaten Informationen (die kein Ausschlussgrund der Maßnahme sind, allerdings bei nachrichtendienstlichen Mitteln, die solche Informationen typisch einschließen, eine unabhängige Vorabkontrolle erfordern), vielmehr bezieht er sich auf intime oder vergleichbar engste Beziehungen oder Informationen dieser absoluten Schutzwürdigkeit.

Nicht umfasst vom Kernbereichsschutz sind Informationen mit Sozialbezug. Kommunikation hierüber ist nicht geschützt, selbst wenn sie auch Höchstpersönliches zum Gegenstand hat. Die Besprechung und Planung von Straftaten oder Gefährdungen gehört ihrem Inhalt nach nicht zum Kernbereich privater Lebensgestaltung, sondern hat Sozialbezug (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 122). Solcher Sozialbezug ist beispielsweise auch gegeben, wenn bei Aufklärungsmaßnahmen durch Verhalten und Äußerungen der Zielperson Erkenntnisse über eine psychische Störung mit resultierenden Gewaltphantasien anfallen. Hierbei sind zwar spezifische Vertraulichkeitsbeziehungen, bei denen der betroffenen Person gerade ermöglicht werden soll, fachliche qualifizierte Hilfe zu erlangen, absolut geschützt, also etwa ein Gespräch mit einem Psychotherapeuten (BVerfG, a.a.O.), nicht jedoch allgemeine persönliche Kontakte. Wenn also eine nachrichtendienstliche Verbindung solche gefährdungsqualifizierende Eigenschaften bei einer Person feststellt, dürfen diese Erkenntnisse auch dem Bundesnachrichtendienst mitgeteilt und dort zur Auslandsaufklärung genutzt werden.

Nach Satz 2 sind bereits bei einer Einsatzplanung besonders kernbereichsgeneigte Situationen möglichst zu vermeiden. Dazu ist bereits vorab zu prüfen, ob Anhaltspunkte bestehen, dass der geplante Einsatz seinem Gesamtcharakter nach kernbereichsrelevante Informationen erfassen wird. Das Bundesverfassungsgericht (BVerfG, Urteil vom 9. Dezember 2022, 1 BvR 1345/21, Rn. 111) hat dies zur Einsatzplanung bei Vertrauenspersonen und Verdeckten Bediensteten der Verfassungsschutzbehörden vorgegeben, es gilt aber gleichermaßen für andere nachrichtendienstliche Mittel, speziell optische oder akustische Überwachungen mit technischen Mitteln, und wird daher in der allgemeinen Schrankennorm aufgenommen. Je mehr der Einsatz insgesamt von einer Nähe zum Kernbereich privater Lebensgestaltung geprägt ist, desto eher muss er von vornherein unterbleiben. Den Rahmen der Risikovermeidung bilden Belange wirksamer Aufgabenwahrnehmung und wirtschaftlicher Verwaltung, die ebenso zu wahren sind.

Zu Absatz 2

Sofern dennoch im Rahmen des Einsatzes nachrichtendienstlicher Mittel Informationen aus dem Kernbereich privater Lebensgestaltung erlangt wurden, regelt Absatz 2 die Löschpflicht. In Zweifelsfällen erfolgt eine Klärung der Kernbereichsrelevanz durch den unabhängigen behördlichen Datenschutzbeauftragten (vgl. dazu insbesondere BVerfG, Beschluss vom 9. Dezember 2022 - 1 BvR 1345/21, Rn. 119). Diesem kommt im behördlichen Gefüge eine besondere – unabhängige – Stelle zu; er ist gerade nicht Teil der regulären behördlichen Hierarchie. Selbstverständlich darf der Bundesnachrichtendienst anstelle einer Vorlage auch selbst unmittelbar die erhobenen Daten löschen.

Zu Absatz 3

In bestimmten Fällen fordert das Bundesverfassungsgericht ein sogenanntes Abbruchgebot, vgl. BVerfG, Beschluss vom 9. Dezember 2022, 1 BvR 1345/21, Rn. 113ff. Entsprechend der verfassungsgerichtlichen Rechtsprechung zu einem Eingriff auf informationstechnische Systeme, welcher ausnahmsweise auch dann „zulässig ist, wenn hierbei eine Wahrscheinlichkeit besteht, dass am Rande auch höchstpersönliche Informationen miterfasst werden“ (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 286 mwN), ist auch bei der Entscheidung zur Fortführung eines Einsatzes maßgeblich, ob eine Erfassung von kernbereichsrelevanten Informationen nicht nur am Rande geschieht. Dabei meint der Begriff „am Rande“, dass lediglich punktuell und untergeordnet kernbereichsrelevante Informationen geteilt werden – die freilich gleichwohl nach Absatz 2 zu löschen sind – und diese nicht den eigentlichen Erhebungsinhalt ausmachen.

Unter Umständen kann eine gebotene Unterbrechung einer Maßnahme wegen einer Gefährdung eingesetzter Personen oder ihrer Einsetzbarkeit nicht sogleich erfolgen. In diesen Fällen kann die Maßnahme zunächst fortgeführt werden, allerdings sind etwaige operative Gestaltungsmöglichkeiten auch dahingehend zu nutzen, die Unterbrechung möglichst schnell zu ermöglichen (BVerfG, Beschluss vom 9. Dezember 2022, 1 BvR 1345/21, Rn. 114 ff.). Nach der Rechtsprechung des Bundesverfassungsgerichts rechtfertigt der Rechtsgüterschutz einer eingesetzten Person eine Ausnahme vom Abbruchgebot „jedenfalls“, wenn ansonsten Leib oder Leben der Person in Gefahr gerieten (a.a.O. Rn. 115). Die gesetzliche Regelung bezieht auch die Freiheit als ebenso besonders gewichtiges Rechtsgut (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 243) ein. Ebenso wie beim Rechtsgut Leib und Leben muss hier allerdings eine erhebliche Beeinträchtigung drohen, um die Fortsetzung der Maßnahme rechtfertigen zu können. Wenn in solchen Situationen solche Gefährdungen drohen, sind sie jedoch typischerweise erheblich. Der eingesetzten Person ist auch keine Aufopferung bei unübersichtlichen Schadensszenarien, die jedenfalls möglicherweise auch erhebliches Ausmaß annehmen, zuzumuten. Das Tatbestandsmerkmal der weiteren Einsetzbarkeit sichert gleichermaßen die Fortführung des aktuellen Einsatzes wie auch künftige andere Einsätze.

In der Regel muss beim Einsatz einer nachrichtendienstlichen Verbindungen grundsätzlich ein gewisses Maß an Nähe und Vertrauen zu den jeweiligen Aufklärungszielen bestehen, um überhaupt Informationen gewinnen zu können. In Ausnahmefällen kann es vorkommen, dass die aufzuklärende Person diese Beziehung in Anspruch nimmt, um von sich aus kernbereichsrelevante Informationen mitzuteilen, z.B. wenn sie sich in einer emotionalen Ausnahmesituation befindet. In diesen Ausnahmefällen muss es der eingesetzten Person ermöglicht sein, zu ihrem Schutz aber auch zur Sicherung ihrer weiteren Einsetzbarkeit, unter den obig beschriebenen engen Bedingungen, in der Situation zu verbleiben.

Auch beim Einsatz anderer nachrichtendienstlichen Mittel, wie z.B. bei Observationen kann es im absoluten Ausnahmefall nötig sein, in einer kernbereichsrelevanten Situation zu verbleiben. Hier ist insbesondere auch dem Umstand Rechnung zu tragen, dass seitens der im Aufklärungsinteresse stehenden Organisationen im Rahmen ihrer Tätigkeiten teilweise umfangreiche Maßnahmen ergriffen werden, um eingesetzte Personen und nachrichtendienstliche Mittel, insbesondere Observationen, zu identifizieren bzw. unwirksam zu machen. Bei einer Enttarnung einer eingesetzten Person besteht regelmäßig die Gefahr, dass die Person mit einem heute üblicherweise jederzeit verfügbaren Smartphone fotografiert und das Foto in breiten Szenekreisen – mit Warnhinweis – geteilt wird. Die eingesetzte Person ist dann weit über den konkreten Einsatz hinaus nicht mehr einsetzbar.

Bei den operativ eingesetzten Personen, wie z.B. nachrichtendienstlichen Verbindungen oder Observanten, handelt es sich regelmäßig um professionell ausgebildete oder erfahrene Personen mit besonderen Zugangslagen, die nur unter großem Aufwand ersetzt werden können. Ungleich schwieriger gestaltet sich die Ad-hoc-Kompensation einer nicht mehr einsetzbaren Person in einer laufenden Maßnahme wie z.B. einer Observation. Insofern

muss die Funktionsfähigkeit der nachrichtendienstlichen Aufklärung bzw. die Einsetzbarkeit der handelnden Personen durch die Möglichkeit eines ausnahmsweisen Verbleibens in einer kernbereichsgeschützten Situation gesichert werden. Zu berücksichtigen ist hierbei, dass es einer eingesetzten Person, die nicht als nachrichtendienstliche Verbindung agiert, wie z.B. einem Observanten, eher möglich ist, die einschlägige Situation ohne Gefährdung seiner Person oder seiner Einsatzfähigkeit zu verlassen bzw. seinen Einsatz innerhalb der Maßnahme abzubrechen.

Insgesamt ist dem Schutz der eingesetzten operativen Personen gerade im Bereich der Auslandsaufklärung eine sehr hohe Bedeutung zuzumessen. Nachrichtendienstliche Handlungen der Auslandsaufklärung stehen hierbei unter dem hohen Druck der Aufklärungstätigkeiten anderer (ausländischer) Nachrichtendienste. Werden Personen bei nachrichtendienstlichen Handlungen identifiziert, kann dies immense Folgewirkungen für die betroffene Person insbesondere bei späteren beruflichen oder sogar privaten Reisetätigkeiten bis hin zu einer Gefahr für Leib, Leben oder Freiheit haben, da solche Handlungen zum Nachteil anderer Staaten regelmäßig strafbewehrt sind.

Für den Einsatz technischer Mittel sind in Absatz 4 abweichende Vorgaben getroffen. Diese Abweichung ist dem besonderen Umstand geschuldet, dass im Rahmen der technischen Aufklärung in der Regel eine Vielzahl von personenbezogenen Daten erhoben werden und eine inhaltliche Auswertung der so erhobenen Daten erst zu einem späteren Zeitpunkt erfolgt. Da insoweit bereits Absatz 2 Satz 2 bis 4 Vorgaben enthalten, die sicherstellen, dass eine Verwendung der Daten erst nach vorheriger Prüfung erfolgt, ist es grundsätzlich zulässig, die Erhebung durch technische Mittel fortzusetzen, solange tatsächliche Anhaltspunkte dafür bestehen, dass das Eindringen in den Kernbereich lediglich vorübergehend erfolgt. Dies greift vornehmlich die Situationen auf, in denen im Rahmen einer technisch-akustischen Überwachung „live“ mitgehört wird, und der Betroffene dann mit seinem Gesprächspartner auch über höchstpersönliche Inhalte spricht. Hier ist für den Bundesnachrichtendienst nicht erkennbar, ob das Gespräch im späteren Verlauf diese Themensphäre wieder verlassen wird und möglicherweise nachrichtendienstlich relevante Inhalte besprochen werden. Der Bundesnachrichtendienst muss hier befähigt sein (bzw. bleiben), die Maßnahme zunächst fortzusetzen. Für den maßgebenden Anwendungsfall - Maßnahmen der Telekommunikationsüberwachung, die auch durch ein zeitgleiches „Mithören“ erfolgen – ist insoweit aber klargestellt (vgl. hierzu auch § 3a des bisherigen Artikel 10-Gesetzes), dass die Fortsetzung nur durch Anfertigung einer Aufzeichnung erfolgen darf, um die genannten Sicherungsvorgaben nicht unterlaufen werden. Der Verweis auf Absatz 2 Satz 2 bis 4 ist klarstellend, da eine Anwendung dieser Regelungen bereits nach dem allgemeinen Wortlaut erfolgen würde.

Zu Absatz 4

Die Regelung in Absatz 4 Satz 1 konkretisiert den Kernbereichsschutz beim Einsatz einer nachrichtendienstlichen Verbindung mit einem vorbeugenden Ausschluss der gezielten Instrumentalisierung von intimen Beziehungen, in denen geradezu zwangsläufig kernbereichsrelevante Informationen erlangt würden (BVerfG, Beschluss vom 9. Dezember 2022, 1 BvR 1345/21, Rn. 107, 110).

Eine nachrichtendienstliche Verbindung darf nicht gezielt zum alleinigen Zwecke der Informationsgewinnung eine intime Beziehung zu einer Person aufbauen oder zu diesem Zwecke fortführen. Unabhängig vom absoluten Schutz informationeller Selbstbestimmung im Kernbereich privater Lebensgestaltung ist im Lichte der grundrechtlichen Garantie der Menschenwürde auch ausgeschlossen, dass der Staat eine für ihn tätige Person zur Eingehung intimer Beziehungen (womit keine Intimität im rein physisch-sexuellen Sinne gemeint ist, sondern eine emotionale Intimität) anhält, um damit staatliche Aufklärungszwecke zu verfolgen. Nicht erfasst sind sonstige private Beziehungen jenseits solcher intimen oder vergleichbaren Qualität, einschließlich eines familiären Einschlusses, wie beispielsweise der Einbezug bei der Kinderbetreuung.

Die Vorschrift ist in ihrer Anwendung auf das gezielte Eingehen (oder Fortführen) einer Beziehung, mit dem einzigen Zweck, Informationen zu sammeln begrenzt. Nicht erfasst sind Sachverhalte, bei denen eine Person eine intime Beziehung aus einer Vielzahl von eigenen Motiven unterhält, welche sich nicht auf die Informationsbeschaffung für den Bundesnachrichtendienst reduzieren lassen. Die denkbaren Lebenssachverhalte sind insoweit nicht eingrenzbar; begleitende Motive, welche einer gezielten Eingehung einer Intimbeziehung zum Zwecke der Informationsgewinnung für den Bundesnachrichtendienst entgegenstehen, können pekuniäre Abhängigkeiten von der Zielperson, Machtdynamiken, verwandschaftliche Bindungen, die Tätigkeit für andere Nachrichtendienste oder emotionale Gründe sein.

Zu Absatz 5

Satz 1 trifft eine nach der Verfassungsrechtsprechung (vgl. BVerfG, Urteil vom 26. April 2022, 1 BvR 1618/17, Rn. 283ff.) gebotene Maßgabe zum Kernbereichsschutz bereits auf der Erhebungsebene. Unbedingt verlässliche technische Lösungen sind zwar aktuell noch nicht verfügbar, die Regelung muss aber zukunftsfest sein, also auch Vorsorge für den Fall einer zukünftigen Verfügbarkeit entsprechender technischer Systeme treffen. Satz 2 und Satz 3 gewährleisten demgegenüber den gebotenen Kernbereichsschutz bei Maßnahmen nach §§ 37 und 38 auf der Aus- und Verwertungsebene (vgl. dazu BVerfGE vom 26. April 2022, 1 BvR 1618/17, Rn. 286, 315). Die Regelung berücksichtigt die besondere Kernbereichsnähe bei den genannten Eingriffen in informationstechnische Systeme, welche das Recht auf Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme von Inländern und Deutschen betreffen, und ist inhaltlich dem § 100d Absatz 3 StPO nachempfunden (vgl. zu dieser Vorschrift insbesondere BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 180/23, Rn. 266).

Technische Aufklärungsmaßnahmen beinhalten – schon aufgrund der zumeist automatisierten Datenerhebung – eine besondere Gefahr der Erfassung auch von Daten aus dem Kernbereich privater Lebensgestaltung. Es sind daher so weit wie möglich – ohne den Erfolg der nachrichtendienstlichen Maßnahme zu gefährden – technische Vorkehrungen zu treffen, um eine solche Erfassung zu verhindern. Können kernbereichsrelevante Daten vor oder bei der Datenerhebung nicht ausgesondert werden, ist die nachrichtendienstliche Maßnahme allerdings auch dann zulässig, wenn hierbei die Wahrscheinlichkeit besteht, dass am Rande auch Kernbereichsinformationen miterfasst werden (vgl. BVerfG, a.a.O.). Dabei ist zu beachten – dies entspricht ebenfalls der verfassungsgerichtlichen Wertung, vgl. BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 180/23, Rn. 262ff. – dass häufig aufgrund der technischen (Automatisierung der Datenerhebung) und/oder tatsächlichen (fremdsprachige oder schlecht verständliche Inhalte) Umstände eine Erfassung von kernbereichsrelevanten Inhalten im Rahmen der hier erfassten Eingriffe in informationstechnische Systeme nicht auf Erhebungsebene ausgeschlossen werden kann. In diesen Fällen besteht kein „Abbruchgebot“, sondern dem Kernbereichsschutz ist auf Aus- und Verwertungsebene zu entsprechen (BVerfG, a.a.O.). Insoweit ist dafür Sorge zu tragen, dass kernbereichsrelevante Daten so frühzeitig herauszufiltern sind, „dass sie den Sicherheitsbehörden nach Möglichkeit nicht offenbar werden“ (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 224). Das Gericht greift insoweit seine bereits zuvor entwickelten Grundsätze zu einem „zweistufigen Schutzkonzept“, welches zwischen Erhebungs- und Auswertungs-/Verwertungsebene unterscheidet, auf. Da bei den hier gegenständlichen Maßnahmen im Vorfeld nicht ersichtlich ist, ob und inwieweit durch sie auch kernbereichsrelevante Inhalte erhoben werden (können), kommt der Prüfung auf der Auswertungs-/Verwertungsebene ein besonderes Gewicht zu.

Gleichwohl ist eine unbegrenzte Vorabsichtung aller erhobenen Daten durch eine unabhängige Stelle nicht praktikabel – und verfassungsrechtlich auch nicht geboten. Praktikabel ist ein solches Erfordernis schon mit Blick auf die möglichen Datenmengen, die händisch gesichtet werden müssten, nicht. Es ist schlechterdings unmöglich – zumal solange die entsprechenden technischen Verfahren zur Vorfeldfilterung noch nicht im Bereich des Möglichen liegen –, dass der Unabhängigen Kontrollrat (oder auch eine andere Stelle) die

enormen Datenmengen in einem vernünftigen Zeitraum prüfen könnte. Selbst wenn die Kontrolle nur sehr rudimentär erfolgte und ein beträchtlicher Teil der Mitarbeiterinnen und Mitarbeiter künftig ausschließlich als „Datensichter“ beschäftigt würde, wäre die entstehende Arbeitslast in der Praxis nicht zu bewerkstelligen. Insoweit ist zu berücksichtigen, dass moderne Endgeräte leicht Speicherkapazitäten im Terrabyte-Bereich vorhalten. Dies können mit tausenden, zehntausenden oder hunderttausenden Einzeldateien gefüllt sein.

Eine individuelle Vorprüfung aller Daten ist aufgrund der nunmehr verfolgten Regelung indes auch verfassungsrechtlich nicht geboten: Weitergehend als § 100d Absatz 3 StPO (der einer verfassungsrechtlichen Kontrolle standgehalten hat, vgl. BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 180/23, Rn. 266) sieht § 21 Absatz 5 Satz 2 und 3 nämlich eine ausdifferenzierte Regelung vor, die gerade solche Daten, bei denen bereits aufgrund ihrer „Beschaffenheit“ (also der Umstände ihrer Speicherung, Kennzeichnung oder Datenart) mit an Sicherheit grenzender Wahrscheinlichkeit klar ist, dass keine Kernbereichsrelevanz bestehen kann, von einer Vorsichtung ausnimmt. Bestehen demgegenüber aufgrund der „äußeren Umstände“ tatsächliche Anhaltspunkte dafür, dass ein individuelles Datum kernbereichsrelevante Inhalte enthält, so ist eine inhaltliche Einsichtnahme durch den Bundesnachrichtendienst bereits nicht zulässig; das Datum ist vielmehr unverzüglich zu löschen oder dem Unabhängigen Kontrollrat zur inhaltlichen Prüfung vorzulegen. Durch diese Regelungssystematik ist hinreichend sichergestellt, dass kernbereichsrelevante Inhalte den Sicherheitsbehörden „nach Möglichkeit nicht offenbar werden“ (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 224). Im Übrigen ist für die weiterhin bestehende Möglichkeit der vereinzelten Kenntnisnahme von höchstpersönlichen Inhalten zu berücksichtigten, dass diese unverzüglich zu löschen sind, die Kenntnis also faktisch auf das absolut Unumgängliche beschränkt bleibt und erst recht eine Weiterverarbeitung gänzlich ausgeschlossen ist. Dass dieser Umstand grundsätzlich verfassungskonform ist, hat das Bundesverfassungsgericht bereits klargestellt (vgl. BVerfG, Beschluss vom 12. Oktober 2011, 2 BvR 236/08 u.a., Rn. 221ff.) und zuletzt auch für Maßnahmen nach § 100b StPO – mit leicht missverständlichem Verweis auf „Kommunikationsinhalte“ – dem Grunde nach bestätigt: „Werden bei einer Überwachungsmaßnahme trotz der Sicherungen in § 100d Absatz 1, Absatz 3 Satz 1 StPO kernbereichsrelevante Daten erfasst, bieten – ungeachtet dessen, dass es dazu an einer zulässigen Rüge fehlt (vgl. Rn. 151) – § 100d Absatz 2, Absatz 3 Satz 2 StPO in-sofern einen nachgelagerten Schutz auf der Aus- und Verwertungsebene, als Kommunikationsinhalte des höchstpersönlichen Bereichs nicht verwertet werden dürfen, sondern unverzüglich zu löschen sind“ (BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 180/23, Rn. 267).

Im Einzelnen bedeutet dies für den Grundfall des in Satz 2 geregelten nachträglichen Kernbereichsschutzes auf Auswertungs- und Verwertungsebene: Sollte im Rahmen dieser Auswertung oder Verwertung von mittels einer der in Satz 2 genannten Maßnahmen erhobenen Daten aufgrund von tatsächlichen Anhaltspunkten der Verdacht bestehen, dass es sich bei diesen Daten um kernbereichsrelevante Erkenntnisse handelt, so sind die jeweiligen Daten dem Grundsatz nach zu löschen. Über eine unvermeidbare Kenntnisnahme bei der Datenerhebung oder ersten Weiterverarbeitung hinaus, sind die entsprechenden individuellen personenbezogenen Daten, die nicht vom Bundesnachrichtendienst selbst bereits gelöscht wurden, weil die Kernbereichsrelevanz evident war, vor einer weiteren Nutzung durch den Unabhängigen Kontrollrat zu sichten und daraufhin zu prüfen, ob es sich um kernbereichsrelevante Informationen handelt (vgl. dazu BVerfG, Urteil vom 26. April 2022, 1 BvR 1619 /17, Rn. 283ff, 286).

Zugleich wird in Satz 3 klargestellt, dass ein tatsächlicher Anhaltspunkt für eine Kernbereichsrelevanz insbesondere darin liegen kann, dass Daten in einem „unmittelbaren Zusammenhang“ mit solchen Daten liegen, bei denen eine Kernbereichsrelevanz bereits positiv festgestellt wurde. In diesem Fall sind die Daten ohne inhaltliche Einsichtnahme zu löschen oder dem Unabhängigen Kontrollrat vorzulegen. Entscheidend für die Bewertung des „unmittelbaren Zusammenhangs“ ist dabei, dass der tatsächliche Anhaltspunkt mit Blick auf das individuelle Datum vorliegen muss, nicht also bereits daraus abgeleitet werden kann, von welchem Endgerät die Daten erhoben wurden. Dies liegt darin begründet, dass

auch bei z.B. privat genutzten Mobiltelefon die große Mehrzahl gespeicherter Daten gerade keine kernbereichsrelevanten Inhalte enthält (etwa, weil es sich um Anwendungs- oder Betriebssystemdaten handelt). Es wäre gerade die oben beschriebene überbordende und jede Kontrollinstanz überbeanspruchende Förmlichkeit, insoweit alle Daten eine Vorprüfung zu unterziehen. Vielmehr ist mit dem „unmittelbaren Zusammenhang“ etwa der Fall gemeint, dass in der Durchsicht eines spezifischen Dateiordners (o.ä.) eine der Dateien als kernbereichsrelevant identifiziert wurde. In diesem Fall kann – abhängig von den jeweiligen Einzelumständen, wie etwa der Ordergröße oder Bezeichnung – bereits aus dem unmittelbaren Zusammenhang darauf geschlossen werden, dass auch weitere in diesem Ordner enthaltene Daten eine Kernbereichsrelevanz aufweisen. Ein ähnlicher Fall kann etwa vorliegen, wenn in gespeicherter Kommunikation eine kernbereichsrelevante Unterhaltung ausgemacht wird; auch hier kann – abermals abhängig von den Umständen des Einzelfalls – ein tatsächlicher Anhaltspunkt dafür bestehen, dass auch die (z.B.) Antworten auf die entsprechende Kommunikation ebenfalls wieder kernbereichsrelevante Inhalte aufweisen.

Eine alternative Ausgestaltung der Regelung dieses Absatzes nach dem Modell der Regelung zur Wohnraumüberwachung (vgl. § 29 Absatz 4) ist bei den hier in Rede stehenden Maßnahmen, welche gerade geprägt sind durch den großen Umfang der erhobenen Daten wie oben dargestellt faktisch nicht realisierbar. Dies entspricht im Übrigen auch der Rechtslage anderer europäischer Staaten. So hat eine Prüfung der Rechtslage in nur einigen rechtstaatlichen Demokratien im europäischen Ausland (konkret: Bulgarien, Dänemark, Frankreich, Griechenland, Österreich, Portugal, Slowakei, Schweden, Vereinigtes Königreich) ergeben, dass eine vollumfängliche Vorabsichtung erhobener Daten durch ein unabhängiges Kontrollgremium diesen Rechtsordnungen fremd ist. Tatsächlich gehen die Regelungen aller der genannten Länder (nicht nur in dieser Frage) deutlich über die nunmehr getroffenen Regelungen weit hinaus.

Schließlich ist es auch Gebot praktischer Konkordanz, den Schutz besonders gewichtiger Rechtsgüter, dem die Tätigkeit des Bundesnachrichtendienstes dient, nicht über eine Verfahrensgestaltung auszuhöhlen, welche entweder unerfüllbare oder lähmende Vorgaben trifft. Wäre eine weitergehende Verfahrenssicherung, die im Grundgesetz nicht ausdrücklich vorgesehen ist, nicht lediglich eine Billigkeitsabwägung, sondern eine zwingende Anforderung zur Gewährleistung von menschenrechtlichen Standards, so wäre zu erwarten, dass sich solche Verfahren vergleichbar in anderen menschenrechtsbasierten Rechtsordnungen finden. Für den absoluten Schutz der Menschenwürde ist unerheblich, in welchem institutionellen Rahmen der Staat – sei es im Bundesnachrichtendienst, sei es im Unabhängigen Kontrollrat – von solchen Informationen ungewollte Kenntnis erlangt (um sie sogleich zu löschen). Für die Kontrolle der Verwaltungspraxis und ihre Fortentwicklung im Zusammenspiel mit der unabhängigen Kontrolle sind im Übrigen Strukturkontrollen des Unabhängigen Kontrollrates ungleich wirksamer als isolierte Einzelfallbetrachtungen.

Zu § 22 (Schutz von Vertraulichkeitsbeziehungen)

Mit § 22 werden Regelungen zum Schutz gegen das gezielte heimliche Eindringen in Vertraulichkeitsbeziehungen bei dem Einsatz von nachrichtendienstlichen Mitteln geschaffen. Die Regelung beruht auf dem bisherigen § 21 und erweitert dessen Anwendungsbereich des Schutzes von Vertraulichkeitsbeziehungen auf den Einsatz anderer nachrichtendienstlicher Mittel. Ebenfalls wird der Kreis der geschützten Personen gegenüber der bisherigen Vorschrift erweitert und nunmehr auch Parlamentarierinnen und Parlamentarier aufgenommen. Zugleich wurde insbesondere die in Absatz 2 geregelte Verstrickungsregelung der allgemeinen Systematik angepasst.

Die Regelung betrifft besonders vertrauliche Daten, die von bestimmten Berufs- und Personengruppen (Geistliche, Rechtsanwältinnen und Rechtsanwälte, Journalistinnen und Journalisten sowie Parlamentarierinnen und Parlamentarier) im Rahmen ihrer beruflichen Beziehungen regelmäßig ausgetauscht werden. Ausgenommen sind hiervon Fälle, in denen durch freiwillige Zusammenarbeit der jeweiligen Person mit dem

Bundesnachrichtendienst nicht in die Vertraulichkeitsbeziehung eingegriffen wird. Bisher gab es derartige Regelungen nur für technische Aufklärungsmaßnahmen (bisherige § 21 und § 35). Entsprechend des Anspruchs der Neufassung des BND-Gesetzes, normenklare auf die Aufgabe des Bundesnachrichtendienstes zugeschnittene Regelungen schaffen, wird eine Regelung getroffen, die nicht mehr auf für Erhebungsbefugnisse im Nachrichtendienstrecht wesensfremde Zeugnisverweigerungsrechte der Strafprozessordnung verweist, sondern spezifische Regelungen trifft.

Nicht erfasst vom Awendungsbereich der Regelung sind Fallgestaltungen, in denen eine Person die ihr im Rahmen des geschützten Vertrauensverhältnisses anvertrauten oder bekannt gewordenen Informationen unter Missachtung des Vertrauensverhältnisses mit Dritten oder beispielsweise auch mit dem Bundesnachrichtendienst selbst teilt (Bruch der Vertraulichkeitsbeziehung).

Zu Absatz 1

Die Regelung fußt auf dem bisherigen § 21 Absatz 1. Die dortige Begrenzung des Anwendungsbereichs auf eine „gezielte“ Erhebung, welche an die Verwendung von Suchbegriffen im Rahmen der strategischen Fernmeldeaufklärung anknüpfte, wurde dabei angepasst: Unzulässig ist die Erhebung von personenbezogenen Daten mit Ziel der Erlangung von Daten aus einer Vertraulichkeitsbeziehung. Damit ist es dem Bundesnachrichtendienst verwehrt, absichtsvoll Daten aus einer Vertraulichkeitsbeziehung zu erheben. In Satz 2 ist geregelt, wann Daten einer Vertraulichkeitsbeziehung entstammen: Es handelt sich um diejenigen Daten, die den o.g. geschützten Berufsgruppen im Rahmen der jeweiligen Eigenschaft erhalten oder von ihnen übermitteln werden (vgl. hierzu den vergleichbaren Aufbau des § 53 der Strafprozessordnung).

Ein Mitglied der Berufsgruppe unterliegt nicht in all seinen Kommunikationen einem absolutem Schutz – vielmehr kommt es darauf an, in welchem spezifischen Kontext die Kommunikation erfolgt und nur diejenigen Verkehre, welche gerade eine besondere Vertraulichkeit für sich in Anspruch nehmen können, sind von der Erfassung ausgenommen. Bei vielen Berufsgruppen wird es dabei vor der Erhebung nicht möglich sein, eine Aussage über die Vertraulichkeit der zu erhebenden Kommunikation zu geben. In diesen Fällen ist eine Erhebung zulässig und es wird sodann durch Absatz 3 sichergestellt, dass etwaige erhobene Daten aus einer Vertraulichkeitsbeziehung sachgerecht behandelt, d.h. in der Regel sofort gelöscht werden.

Die Frage, ob eine Person zu einer der geschützten Personengruppen zählt, erfordert eine wertende Betrachtung unter Berücksichtigung der jeweiligen Einzelfallumstände. So kommt es – insbesondere im Ausland – nicht auf die Berufsbezeichnung oder eine staatliche Zertifizierung an, sondern auf die tatsächlichen Begebenheiten.

Beispielsweise sind als Journalisten getarnte Personen, z.B. Mitarbeitende anderer Nachrichtendienste oder Mitglieder oder Sympathisanten terroristischer Vereinigungen wie z.B. dem sogenannten Islamischen Staat, die mediale Propaganda betreiben, wie u.a. die Veröffentlichung von Anleitungen zum Bombenbau oder Videos von Exekutionen, nicht vom Schutzbereich umfasst, da für diese bereits der persönliche Schutzbereich des Artikel 5 Absatz 1 Satz 2 des Grundgesetzes nicht eröffnet ist. Ausgenommen vom personellen Schutzbereich sind darüber hinaus „Journalisten“, die für staatliche oder staatlich gelenkte Presseeinrichtungen in Staaten arbeiten, in denen die Pressefreiheit stark eingeschränkt ist und der Staat erheblichen Einfluss auf die Berichterstattung nimmt. Die Pressefreiheit schützt in inhaltlicher Sicht nur Publikationen, die am Kommunikationsprozess zur Ermöglichung freier individueller und öffentlicher Meinungsbildung teilnehmen – geschützt werden soll also die freie Presse mit dem Ziel der Kontrolle und des kritischen Hinterfragens des Agierens der öffentlichen Gewalt. In bestimmten Staaten kontrollieren Regierungen allerdings weite Teile der Medienlandschaft, sodass eine freie Presse nicht existiert. Personen, die dort für staatliche Medien arbeiten, sind in ihrer journalistischen Arbeit stark

eingeschränkt und können über Inhalte nicht frei bestimmen bzw. sind letztendlich der verlängerte Arm ihrer diktatorischen Regierungen. Für die Einschätzung, bei welchen Staaten dies der Fall ist, kann auf das jeweils aktuelle Ranking der Organisation „Reporter ohne Grenzen“ Bezug genommen werden. Tätigkeiten von Journalisten für staatliche oder staatlich gelenkte Presseeinrichtungen von gemäß dem Ranking als „dunkelrot“ eingestuften Staaten unterfallen nicht dem Schutz der Pressefreiheit. Ausdrücklich nicht betroffen hiervon sind kritische Journalisten aus diesen Staaten; diese sind mithin von § 22 geschützt. In Einzelfällen kann die Eröffnung des Schutzbereichs des § 22 auch für Journalistinnen und Journalisten aus nicht gelisteten Ländern verneint werden, wenn Erkenntnisse vorliegen, dass diesen aufgrund der Tätigkeit für eine spezielle staatlich gelenkte oder terroristische Medienanstalt keine freie Berichterstattung möglich ist und sie vielmehr einen Beitrag als Propagandasprachrohr für staatliche Stellen oder terroristische Gruppierungen leisten. Ebenso können zur Unterstützung der wertenden Betrachtung auch – international entwickelte – journalistische Standards wie die „Journalism Trust Initiative“ (JTI) herangezogen werden.

In Satz 3 wird die Wertung des § 53a StPO und des § 110d Absatz 5 Satz 2 aufgegriffen und systemgerecht übertragen.

Zu Absatz 2

Eine besondere Schutzbedürftigkeit besteht auch dann nicht, wenn die betroffene Person in die jeweilige Bedrohung verstrickt ist oder eine Gefahr für ein besonders gewichtiges Rechtsgut abgewendet werden muss.

Die Verstrickung kann – der allgemeinen Systematik des Gesetzes folgend – durch Verantwortlichkeit bzw. Unterstützen (Nummern 1 und 2), aber auch durch einen spezifischen Zusammenhang mit der Bedrohung (Nummer 3) entstehen. Einerseits ist also eine Verstrickung in eine zumindest erhebliche Bedrohung hinreichend, um den Vertraulichkeitsschutz im Einzelfall durchbrechen zu können. Andererseits sind tatsächliche Anhaltspunkte für eine Verstrickung nicht hinreichend; vielmehr bedarf es Tatsachen, welche die Annahme einer Verstrickung rechtfertigen.

Entscheidend für die Anwendung des Absatzes 2 ist dabei diejenige Person, gegen die die Maßnahme gerichtet ist. Handelt es sich demgegenüber um eine Maßnahme gegen eine Person, die ihrerseits mit einer der in Absatz 1 Satz 2 genannten Berufsgruppen in Kontakt steht, und teilt die letztgenannte Person ihrerseits unter Missachtung der Vertraulichkeit Informationen aus einer Vertraulichkeitsbeziehung mit einer anderen Person mit, so unterfallen diese Informationen nicht dem § 22. Dies bedeutet zugleich, dass bei einer verstrickten Person grundsätzlich alle Daten erhoben werden können; also auch solche, welche aus Vertraulichkeitsbeziehungen stammen. Hierbei ist freilich – den allgemeinen Grundsätzen folgend – eine Löschung derjenigen Daten vorzunehmen, welche keine nachrichtendienstliche Relevanz haben. Somit wäre es beispielsweise ausnahmsweise zulässig, die Kommunikation eines Rechtsanwaltes zu überwachen, wenn dieser sich an terroristischen Anschlagsplänen beteiligt. Werden im Rahmen dieser Überwachung indes Gespräche mit Mandanten abgehört, welche keinerlei Bezug zu den terroristischen Machenschaften haben, so sind diese unverzüglich zu löschen.

Zu Absatz 3

In Absatz 3 ist – den bisherigen § 21 Absatz 3 aufgreifend – der Fall geregelt, dass die Erhebung entweder gegenüber einer Person erfolgt, deren Zugehörigkeit zu einer der in Absatz 1 genannten Gruppen unbekannt ist oder wenn die Aufklärungsmaßnahme auf eine Tätigkeit gerichtet war, die keinen Zusammenhang mit der konkret geschützten Eigenschaft aufwies. In diesen Fällen ist eine Erhebung nach Maßgabe des Absatzes 1 zwar grundsätzlich zulässig, indes muss sichergestellt sein (und wird durch Absatz 3 sichergestellt), dass

keinerlei Daten weiterverarbeitet werden, welche die Vertraulichkeitsbeziehung eines nicht in eine Bedrohung verstrickten Mitgliedes der jeweiligen Berufsgruppe erfassen.

Ein Beispiel wäre die Informationsgewinnung bei einem erkannten Spion, der beruflich als Rechtsanwalt tätig ist. Die Aufklärung zielt auf Erkenntnisse, die beim Betroffenen bei Gelegenheit seiner Spionagetätigkeit anfallen. Wenn er – ohne gezieltes Hinwirken des Bundesnachrichtendienstes auf solche Informationsgewinnung – auch Informationen, die seiner anwaltlichen Tätigkeit unterliegen, offenbart, folgt aus Absatz 3 die Unverwertbarkeit und Löschungspflicht. Nicht erfasst ist die Informationsgewinnung bei Dritten, die nicht Berufsgeheimnisträger sind, über Angelegenheiten, über die der Berufsgeheimnisträger hätte Verschwiegenheit wahren müsste. Insoweit liegt – begründet durch die Auslandstätigkeit des Bundesnachrichtendienstes – eine Abweichung von § 29 Absatz 5 des MAD-Gesetzes vor. Vgl. die Gesetzesbegründung: „Einbezogen ist also auch die Informationsgewinnung durch Maßnahmen, die gegen andere Personen gerichtet sind, wenn an dem überwachten Sachverhalt auch Berufsgeheimnisträgerinnen und Berufsgeheimnisträger beteiligt sind und diese dabei Informationen weitergeben, über die sie das Zeugnis verweigern dürften."

Zu Absatz 4

In Absatz 4 findet sich eine Dokumentationspflicht als begleitende, verfahrenssichernde Vorgabe. Die Kennzeichnungspflicht der erhobenen Daten folgt bereits unmittelbar aus der Verwendungseinschränkung in Verbindung mit § 58 Absatz 1, für im Rahmen von Maßnahmen der technischen Aufklärung erhobene Daten ergibt sich diese direkt aus § 64 Absatz 3.

Zu § 23 (Vorgaben für den Einsatz nachrichtendienstlicher Verbindungen)

In § 23 werden spezielle Vorgaben für den Einsatz nachrichtendienstlicher Verbindungen geregelt und der Begriff der nachrichtendienstlichen Verbindung definiert. Die Befugnis zum Einsatz nachrichtendienstlicher Verbindungen jenseits der Fälle des besonders geregelten eingriffsintensiven Einsatzes (vgl. nachfolgenden § 24) ergibt sich aus § 18.

Zu Absatz 1

Absatz 1 enthält eine Definition des Begriffs der nachrichtendienstlichen Verbindung. Im Rahmen seiner Auftragserfüllung setzt der Bundesnachrichtendienst Personen, die nicht Beschäftigte des Bundesnachrichtendienstes sind und deren Zusammenarbeit mit dem Bundesnachrichtendienst Dritten verborgen bleiben soll (so die Legaldefinition der nachrichtendienstlichen Verbindungen), in unterschiedlichen Funktionen ein. Diese unterstützen bei der Beschaffung nachrichtendienstlich relevanter Informationen oder werden im Rahmen nachrichtendienstlicher Operationen zur Erfüllung sonstiger Aufträge genutzt. Nachrichtendienstliche Verbindungen können zum einen Personen sein, die offene oder geheime Nachrichten – zum Beispiel durch Gespräche oder Beobachtung - erlangen. Zum anderen können dies Personen sein, die bei der sonstigen nachrichtendienstlichen Tätigkeit eingesetzt werden, z.B. durch Transport von Schriftgut und Gegenständen oder durch Übersetzungsleistungen. Der Bundesnachrichtendienst führt nachrichtendienstliche Verbindungen also in einer Vielzahl und Vielfalt von Ausgestaltungen. Nachrichtendienstliche Verbindungen können über einen kurzen oder langen Zeitraum sowie unterschiedlich eng geführt und unterschiedlich eng gesteuert werden. Sie können in eher unregelmäßigen Zeitabständen, anlassbezogen oder sehr regelmäßig getroffen werden. Sie können umfassend zu ihrem jeweiligen Umfeld berichten oder nur Gelegenheiten zu Kurzkontakten zu Aufklärungszielen des Bundesnachrichtendienstes nutzen und Informationen darüber weitergeben. Der Begriff der nachrichtendienstlichen Verbindung ist insofern zu unterscheiden vom verfassungsschutzrechtlichen Begriff der Vertrauensperson.

Zu Absatz 2

Diese Norm regelt allgemeine Vorgaben für die Gewinnung und den Einsatz von nachrichtendienstlichen Verbindungen, wenn es sich bei ihnen um deutsche oder inländische

Personen handelt, die sich im Bundesgebiet aufhalten. Werden Ausländer im Ausland als nachrichtendienstliche Verbindung geführt, finden diese speziell mit Blick auf die Lebenssituation im Bundesgebiet ausgerichteten Vorgaben keine Anwendung. Die kurzzeitige Einreise eines Ausländers in das Bundesgebiet für z.B. einem Urlaubsaufenthalt, Verwandtschaftsbesuch oder ein Treffen mit Mitarbeitenden des Bundesnachrichtendienstes zum Zwecke der Anwerbung führt nicht zu einer Anwendung dieser speziellen Vorgaben.

Handelt es sich bei Person, die geführt werden soll, um eine deutsche oder inländische Person, so ist eine Führung als nachrichtendienstliche Verbindung unzulässig, wenn die Person die in den Nummern 1 bis 5 aufgeführten Varianten – die dem bisherigen § 9b Absatz 2 des Bundesverfassungsschutzgesetzes entsprechen – unterfällt.

In Satz 2 ist geregelt, dass eine Maßnahme im Falle einer Ausnahme nach Satz 1 Nummer 2 oder 3 nach höchstens sechs Monaten zu beenden ist, wenn durch sie keine Informationen zu zumindest erheblichen Bedrohungen erlangt wurden. Dies trägt dem Ausnahmecharakter weiter Rechnung und soll unbotmäßige Beeinträchtigungen ausschließen. Sollten innerhalb von sechs Monaten Informationen zu zumindest erheblichen Bedrohungen erlangt worden sein, so bedarf es keiner erneuten Prüfung.

Zu Absatz 3

Absatz 3 regelt die Ausnahmen der allgemeinen Vorgaben des Absatzes 2. Maßgeblich für den Ausschluss von nachrichtendienstlichen Verbindungen sind nach der aktuellen Rechtslage die Regelungen in § 9b des Bundesverfassungsschutzgesetzes, die über § 5 des BND-Gesetzes auch für den Bundesnachrichtendienst gelten. Die Ausschlusskriterien des § 9b des Bundesverfassungsschutzgesetzes gehen auf eine Innenministerkonferenz zurück (vgl. BT-Drs. 18/4654). Hieraus folgt bereits, dass die Vorgaben für den Bundesnachrichtendienst, der einen andern Aufklärungsschwerpunkt und eine andere Arbeitsweise als das Bundesamt für den Verfassungsschutz hat, nicht passend sind. Zugleich berücksichtigen die hier geregelten Ausnahmen die grundsätzlichen Einschränkungen bei der Anwerbung dergestalt, dass eine Durchbrechung der in Absatz 2 genannten Verbote nur zulässig ist, wenn die Aufgabenerfüllung des Bundesnachrichtendienstes andernfalls wesentlich erschwert werden würde.

Zu Nummer 1

Immer häufiger werden auch minderjährige Personen von terroristischen Vereinigungen angesprochen und angeworben. In besonderen Ausnahmefällen können daher auch diese wichtige Informationen liefern, weshalb eine Ausnahmeregelung von Absatz 2 Nummer 1 erforderlich ist. Um dem Schutz von minderjährigen Personen dennoch gerecht zu werden, ist dennoch ein Mindestalter von 16 Jahren erforderlich.

Zu Nummer 2

In Nummer 2 sind (allgemeine) Ausnahmen zu den Verboten des Absatz 2 Nummer 2 bis 4 vorgesehen.

Maßgeblicher Gedanke der Anbahnungsverbote ist die Verlässlichkeit der zu gewinnenden Information, da die spätere Gerichtsverwertbarkeit von besonderer Bedeutung ist. Insbesondere kann die finanzielle Abhängigkeit (Absatz 2 Nummer 2) sich nachteilig auf die Qualität von beschafften Informationen auswirken. Da die Tätigkeit des Bundesnachrichtendienstes aber nicht in gleichem Maße auf spätere hoheitliche Maßnahmen ausgerichtet ist, ist auch insoweit eine Ausnahme geboten.

Dies gilt auch für die in Absatz 2 Nummer 3 geregelten Fälle, in denen eine Teilnahme der nachrichtendienstlichen Verbindung an einem „Aussteigerprogramm“ erfolgt. Dieser Phänomenbereich betrifft Personen, denen durch Aussteigerprogramme dabei geholfen wird, extremistische Szenen zu verlassen (vgl. *Dietrich* in Dietrich/Gärditz, Handbuch des Rechts

der Nachrichtendienste, 2. Auflage, 2026, VI § 2 Rn. 59); eine Instrumentalisierung durch den Bundesnachrichtendienst steht hier schon deshalb nicht zu befürchten, weil dieser nicht auf die Aufklärung inländischer Strukturen ausgerichtet ist. Entsprechend spricht nichts dagegen, „Aussteiger“ zu ihren Informationen über das Ausland zu befragen, zumal diese Personen für den Bundesnachrichtendienst oftmals die einzige Informationsquelle über Auslandssachverhalte darstellen können. Diese Personen haben auch keine Repressalien durch ihre Tätigkeit für den Bundesnachrichtendienst zu befürchten.

Weiter bedarf es einer Ausnahme für das Verbot, Parlamentarier oder ihre Mitarbeitenden als nachrichtendienstliche Verbindung zu führen. Die Aufgabe des Bundesnachrichtendienst schließt eine Überwachung von Parteien (etwa zur Prüfung, ob diese verfassungsfeindlich sind) aus. Entsprechend läuft das Führen nachrichtendienstlicher Verbindung nicht Gefahr, auf die Willensbildung von Parteien Einfluss zu nehmen. Auch beobachtet der Bundesnachrichtendienst keine Abgeordneten, sodass ein Eingriff in das freie Mandat nicht zu befürchten steht. Demgegenüber kann es aber insbesondere mit Blick auf die Auslandsaufklärung von großem Interesse sein, Informationen (freiwillig) auch von Parlamentariern oder ihren Mitarbeitenden zu erhalten; etwa zu Auslandsbesuchen in Länder, in denen die Erkenntnislage anderenfalls überaus schwierig ist.

Zu Nummer 3

Die in Nummer 3 enthaltene Ausnahme zu Absatz 2 Nummer 5 entspricht dem geltenden Recht (vgl. § 9b Absatz 2 Satz 2 des Bundesverfassungsschutzgesetzes).

Zu Absatz 4

Absatz 4 übernimmt mit Anpassungen die bisherige Regelung aus § 9a Absatz 2 des Bundesverfassungsschutzgesetzes (verdeckte Mitarbeiter und nach bisherigem § 9b Absatz 1 Satz 1 des Bundesverfassungsschutzgesetzes anwendbar auch auf Vertrauensleute) für die nachrichtendienstlichen Verbindungen des Bundesnachrichtendienstes.

Werden Bedienstete des Bundesnachrichtendienstes ausnahmsweise anstelle und in der Funktion einer nachrichtendienstlichen Verbindungen tätig, etwa im Bereich der HUMINT und/oder sozialen Medien, so ergibt sich die Rechtfertigung für hierbei möglicherweise notwendige Straftaten gegen Rechtsgüter – im Rahmen der allgemeinen Schranken, vgl. § 6 – bereits aus der gesetzlichen Befugnis. Beispiele hierfür sind etwa Äußerungen und Posts, die ein extremistisches Weltbild vorspiegeln sollen und damit Tatbestände wie Volksverhetzung (§ 130 Abs. 5), Gewaltdarstellung (§ 131 Abs. 1 Nr. 1 a), Belohnung und Billigung von Straftaten (§ 140 StGB) erfüllen können. Ebenso sind als notwendige Begleithandlungen der Informationsgewinnung solche Tätigkeiten erfasst, die unterstützenden Charakter haben, wie z.B. Übersetzungsdienstleitungen oder notwendige kleinere Sach- und Geldspenden. Die hierin liegenden Erfüllungen von Straftatbeständen wie Terrorismusfinanzierung (§ 89c Abs. 1 Nr. 8), Aufforderung zu Straftaten (§ 111 Abs. 2), Unterstützung einer terroristischen Vereinigung (§ 129a Abs. 5 S.1 StGB) etc. sind infolge des Handelns innerhalb der gesetzlichen Befugnisse und der Notwendigkeit für die Informationserhebung gerechtfertigt.

Die in Satz 3 neu geschaffene Sonderregelung für die Tätigkeiten von nachrichtendienstlichen Verbindungen im Ausland greift den Umstand auf, dass diese Tätigkeiten einerseits nach dem jeweils geltenden ausländischen Rechtsregime strafbar bleiben, eine Strafbarkeit nach deutschem Recht – Voraussetzung ist also, dass dieses hier Anwendung findet – zurückstehen muss. Dies ist dem Umstand geschuldet, dass für den Bundesnachrichtendienst der Einsatz von nachrichtendienstlichen Verbindungen im Ausland von essentieller Bedeutung ist. Dies gilt insbesondere in Ländern, in denen die Mitarbeiterinnen und Mitarbeiter des Bundesnachrichtendienstes aufgrund von mangelnden Sprachkenntnissen, dem auffallenden äußerem Erscheinungsbild oder der Sicherheitslage nicht selbst agieren können, die aber zugleich zum Hauptaufklärungsfeld gehören.

Hier trägt die Einschränkung auf (sämtliche) Individualrechtsgüter dem akuten Bedarf keine Rechnung – beispielhaft seien hier genannt: Die nachrichtendienstliche Verbindung im Söldner-Milieu mit (auch-)deutscher Staatsangehörigkeit entwendet unter gewaltsamer Öffnung eines PKWs im Ausland militärisches Material (Waffen/Technik/Informationen), dass er dann an den Bundesnachrichtendienst zur Analyse weiterleitet. Die nachrichtendienstliche Verbindung mit (auch-)deutscher Staatsangehörigkeit klärt im Auftrag des Bundesnachrichtendienstes subversive Bestrebungen und hybride Maßnahmen eines ausländischen Geheimdienstes in einem Umfeld auch, in welcher sie aufgrund ihrer Herkunft nicht auffällt, auf. Zur Legendenhärtung muss sie sich an Beleidigungs-Kampagnen gegen Menschen und Institutionen aus dem pro-westlichen politischen Spektrum beteiligen. Dazu werden auch Graffitis mit Parolen an Häuserfassaden gesprüht und andere Sachbeschädigungen begangen. Eine nachrichtendienstliche Verbindung im Islamisten-Milieu mit deutscher Staatsangehörigkeit unterschlägt Material eines wichtigen Terroristen in Syrien und leitet es an den Bundesnachrichtendienst zur Auswertung weiter. In diesen Fällen muss der Bundesnachrichtendienst nicht nur gegenüber der nachrichtendienstlichen Verbindung bestätigen können, dass keine Strafbarkeit nach deutschem Recht besteht, um ihre Einsatzbereitschaft zu erhöhen. Zugleich wäre es auch unerträglich, wenn sich der Mitarbeitende des Bundesnachrichtendienstes bei der Aufforderung, eine entsprechende Tätigkeit vorzunehmen, einer Anstiftung strafbar machen würde. Auch dem trägt der neue Satz 3 Rechnung.

Zu Absatz 5

Absatz 5 übernimmt für die nachrichtendienstlichen Verbindungen des Bundesnachrichtendienstes mit Anpassungen die bisherige Regelung aus § 9a Absatz 3 (verdeckte Ermittler und nach bisherigem § 9b Absatz 1 Satz 1 des Bundesverfassungsschutzgesetzes anwendbar auch auf Vertrauensleute). Wenn ein Strafverfahren infolge der Tatrechtfertigung nach Absatz 4 oder aufgrund Absatz 5 eingestellt wird, liegt es in der Natur der Sache, den Zusammenhang mit einem verdeckten Einsatz nicht transparent zu machen. Dazu wird die Bundesregierung eine Klarstellung in Nummer 89 RiStBV bzgl. der Begründung einer Einstellung nach Absatz 5 in einer Einstellungsmitteilung anstreben. In diesen Fällen ist der Hinweis auf fehlendes öffentliches Interesse sachgerecht. Auch beim Recht auf Akteneinsicht kann dem zugrundeliegenden Anliegen im Rahmen des geltenden Rechts durch angemessene Verfahrensgestaltung Rechnung getragen werden.

Zu Absatz 6

Bereits allgemein unzulässig ist die gezielte Erhebung von kernbereichsrelevanten Informationen (§ 21 Absatz 1 Satz 1). § 23 Absatz 6 ergänzt darüber hinaus diese allgemeine Regelung zum Schutz des Kernbereichs privater Lebensgestaltung um spezielle Maßgaben bei Maßnahmen unter Einsatz einer nachrichtendienstlichen Verbindung. Kernbereichsgeneigte Einsatzsituationen sind grundsätzlich zu vermeiden. Der Bundesnachrichtendienst wirkt also im Rahmen der Möglichkeiten der konkreten Einsatzsituation darauf hin, dass keine kernbereichsrelevanten Informationen erhoben werden. Dabei sind insbesondere sicherheitliche Erwägungen wie auch die konkrete Einsatzsituation (z.B. der Umstand, dass die nachrichtendienstliche Verbindung nicht weiß, dass sie mit dem Bundesnachrichtendienst spricht) zu berücksichtigen.

Die Gefahr, dass Informationen erhoben werden, die den Kernbereich der privaten Lebensgestaltung betreffen, ist insbesondere in Fällen, bei denen beim Einsatz einer nachrichtendienstlichen Verbindung gegen eine Person eine besondere persönliche Vertrauensbeziehung zu dieser besteht, erhöht. Eine solche besondere persönliche Vertrauensbeziehung birgt das erhöhte Risiko, dass die andere Person von sich aus auch kernbereichsrelevante Informationen offenbart. Dies begründet jedoch keinen grundsätzlichen Einsatzausschluss, sondern stellt Anforderungen an die Führung einer nachrichtendienstlichen Verbindung (d.h. nicht darauf hinsteuernd, solche Erhebungen möglichst vermeidend) und den Ausschluss der Weiterverarbeitung solcher ungezielt anfallenden Informationen.

Erlangt eine nachrichtendienstliche Verbindung einsatzbezogen kernbereichsrelevante Informationen, darf sie diese nicht an den Bundesnachrichtendienst weitergeben; hierauf hat der Bundesnachrichtendienst hinzuwirken. Allerdings ist hierbei speziell mit Blick auf den Bundesnachrichtendienst im Kontext seiner Aufgabe der Auslandsaufklärung zu beachten, dass die Art der Führung von nachrichtendienstlichen Verbindungen von der Art der Führung und des Einsatzes von Vertrauenspersonen im verfassungsschutzrechtlichen Kontext abweicht. Beispielsweise werden nachrichtendienstliche Verbindungen aus operativ-sicherheitlichen Erwägungen nicht immer klar geführt, d.h. die Zusammenarbeit mit dem Bundesnachrichtendienst wird ihnen nicht offengelegt, was die Einwirkungsmöglichkeiten auf die nachrichtendienstliche Verbindung faktisch begrenzt. Auch ist die Vertrauens- und Führungssituation zwischen der nachrichtendienstlichen Verbindung und dem sie führenden Mitarbeitenden des Bundesnachrichtendienstes zu berücksichtigen. Die Tätigkeit als nachrichtendienstliche Verbindung kann für diese sehr belastend sein, gerade wenn sie gegen eine Person eingesetzt wird, sich dabei in einer besonderen persönlichen Vertrauensbeziehung befindet oder ihr besondere persönliche Informationen anvertraut werden. Es kann dann auch für die Zusammenarbeit wichtig sein, dass sich die nachrichtendienstliche Verbindung auch über solche Belastungen mitteilen kann und ein solches Gespräch nicht etwa seitens der Mitarbeitenden des Bundesnachrichtendienstes einseitig beendet wird. Derartige Informationen sind jedoch von der Weiterverarbeitung durch den Bundesnachrichtendienst ausgeschlossen. Um verfassungsrechtlichen Anforderungen Genüge zu tun, wirkt der Bundesnachrichtendienst dennoch – soweit in Anbetracht insbesondere der operativ-sicherheitlichen Umstände der konkreten Situation möglich – darauf hin, dass sofern Informationen in irgendeiner Art und Weise in Schrift, Bild, Ton oder auf sonstige Weise durch die nachrichtendienstliche Verbindung festgehalten wurden, diese gelöscht oder sonst vernichtet werden (vgl. BVerfG, Beschluss vom 9. Dezember 2022, 1 BvR 1345/21, Rn. 119).

Der Umstand, dass kernbereichsrelevante Informationen im Rahmen einer Maßnahme angefallen sind, ist zugunsten einer späteren Kontrollmöglichkeit zu dokumentieren (vgl. BVerfG Beschluss vom 9. Dezember 2022 - 1 BvR 1345/21, Rn. 119).

Zu Absatz 7

Die Änderung ermöglicht in besonderen Einzelfällen eine größere Flexibilität in der Zusammenarbeit mit nachrichtendienstlichen Verbindungen. Grundlage dieser besonderen Art der Zusammenarbeit ist eine absolute Verschwiegenheitszusage beider Parteien, auf welcher das notwendige Vertrauensverhältnis aufgebaut wird. Wird mit der Verpflichtung von der nachrichtendienstlichen Verbindung ein schriftliches Bekenntnis zur Zusammenarbeit eingefordert, kann dies in einzelnen Fällen die Vertrauensbeziehung zwischen den Mitarbeitenden des Bundesnachrichtendienstes und der nachrichtendienstlichen Verbindung so empfindlich stören, dass die Zusammenarbeit von der nachrichtendienstlichen Verbindung im Zweifel abgebrochen würde. In diesen Einzelfällen konnte bisher seitens der Behörde lediglich komplett auf eine Verpflichtung verzichtet werden, um die Zusammenarbeit weiterzuführen.

Die Regelung ermöglicht hier zukünftig den Rückgriff auf eine ausschließlich mündliche Verpflichtung, sofern dies im Einzelfall im Interesse der inneren oder äußeren Sicherheit der Bundesrepublik Deutschland geboten ist. Dies ist insbesondere der Fall, wenn die nachrichtendienstliche Verbindung einen Zugang zu Informationen über eine aufzuklärende Bedrohung hat, die ohne die Mitwirkung der nachrichtendienstlichen Verbindung nicht oder nur mit unverhältnismäßigem Aufwand erlangt werden könnten und im Falle der Aufforderung zur Unterzeichnung einer Niederschrift zu befürchten wäre, dass die nachrichtendienstliche Verbindung die Zusammenarbeit beendet.

Da die nachrichtendienstlichen Verbindungen in den dargestellten Fällen keinerlei Vorbehalte gegenüber der von ihnen geforderten Verpflichtung zur gewissenhaften Erfüllung ihrer Obliegenheiten, sondern lediglich gegenüber der schriftlichen Verpflichtung hegen, ist die

ausschließlich mündliche Verpflichtung gegenüber einer gänzlichen Unterlassung der Verpflichtung deutlich vorzugswürdig.

Im Falle der mündlichen Verpflichtung wird die Niederschrift über die Verpflichtung durch die Behörde ohne die Unterschrift der zu verpflichtenden Person aufgenommen.

Zu Unterabschnitt 2 (Besondere Befugnisse zum Einsatz nachrichtendienstlicher Mittel)

In Unterabschnitt 2 sind diejenigen nachrichtendienstlichen Mittel gesondert aufgeführt, die über die allgemeinen Vorgaben des Unterabschnitt 1 hinausgehend mit gesonderten Erhebungsvoraussetzungen versehen sind oder aufgrund der Typizität des Mittels und für eine bessere rechtssystematische Orientierung jedenfalls in eigenen Vorschriften „gebündelt“ werden sollen. Diese Erhebungsbefugnisse führen teilweise schon aufgrund ihrer Natur zu einem gesteigerten Eingriff in die Grundrechte Betroffener, der gleichermaßen gesteigerte Erhebungsschwellen und/oder Verfahrensabsicherungen bedarf. Das Eingriffsgewicht variiert dabei zwar im Einzelfall je nach konkretem Sachverhalt, indes lassen sich aufgrund objektiver Parameter – wie etwa der Länge oder des Ziels einer Maßnahme – gewisse Gruppen bilden, für die gesteigerte Erhebungsschwellen erforderlich sind. Der Stufensystematik des Gesetzes entsprechend, ist in diesen Fällen – im Einzelnen in den jeweiligen Befugnisnormen ausdifferenziert – ein Rückgriff auf die Qualifikationsstufen des § 3 Absatz 1 und § 4 Absatz 1 geboten.

Dabei wird – aufgrund des unterschiedlichen Schutzgehaltes der Grundrechte im Ausland (vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 104, *Arts* in NVwZ 2025, 455, 459) – ein gestuftes, pauschalisierendes System gewählt, bei dem die Eingriffsschwelle von nachrichtendienstlichen Mittel bei Ausländern im Ausland im Grundsatz eine „Stufe“ hinter der eines vergleichbaren Mitteleinsatzes gegenüber Inländern/Deutschen zurückbleibt. Diese Pauschalisierung ist geboten, da die „Absenkung“ des Schutzgehaltes bei einem Einsatz nachrichtendienstlicher Mittel gegenüber Ausländern im Ausland (einheitlich) dadurch begründet ist, dass dem deutschen Staat im Ausland keine Hoheitsgewalt zukommt. Dies schränkt ihn maßgeblich bei der Verwendung von erhobenen Daten ein, was bereits auf Erhebungsebene (pauschal) eingriffsmindernd zu berücksichtigen ist.

Soweit nach Maßgabe der Vorschriften in diesem Unterabschnitt einzelne nachrichtendienstliche Mittel (gegenüber Ausländern im Ausland) auch auf Grundlage der „Grundstufe“ der nachrichtendienstlichen Auslandsaufklärung zulässig sind, ist ihre Verortung hier rechtssystematischen Gründen geschuldet. Diese Mittel könnten ebenso dem § 18 Absatz 1 unterfallen, da die jeweilige Eingriffsschwelle identisch ist. Um zu vermeiden, dass einzelne Mittel trotz gleicher Zeiträume teilweise dem § 18 Absatz 1 und teilweise den Sonderregelungen dieses Unterabschnitts unterfallen, wurden in letzterem insoweit vorrangige Befugnisse geschaffen.

Zu § 24 (Einsatz nachrichtendienstlicher Verbindungen gegen eine Person)

In § 24 ist der Einsatz nachrichtendienstlicher Verbindungen gegen eine Person geregelt. Dabei enthält § 20 Absatz 1 die gesetzliche Vorgabe, wann ein nachrichtendienstliches Mittel gegen eine Person gerichtet ist.

Zur Erfüllung seines gesetzlichen Auftrags der Auslandsaufklärung kann der Bundesnachrichtendienst nachrichtendienstliche Verbindungen gegen Ausländerinnen oder Ausländern im Ausland, aber auch gegenüber Personen, die ihren Aufenthalt im Bundesgebiet haben oder sich durch ihre deutsche Staatsangehörigkeit in einem besonderen Näheverhältnis zur deutschen Staatsgewalt befinden, einsetzen. Für die rechtliche Einordnung der Maßnahme ist damit maßgeblich, gegenüber wem die nachrichtendienstliche Tätigkeit (der Grundrechtseingriff) stattfindet, der Belegenheitsort einzelner nachrichtendienstlicher Handlungen ist dagegen nicht maßgeblich. Die Staatsangehörigkeit oder der gewöhnliche Aufenthaltsort der nachrichtendienstlichen Verbindung selbst ist insoweit nicht entscheidend.

Maßgeblich ist vielmehr, gegen welche Person die nachrichtendienstliche Verbindung mit dem Ziel der Aufklärung gerade dieser Person eingesetzt ist, denn es ist die Informationsbeschaffung, die mit einem Eingriff in die Rechte anderer Personen verbunden ist.

Der Einsatz von nachrichtendienstlichen Verbindungen wirkt dementsprechend nicht per se eingriffsintensiv für die betroffenen Personen. Das Eingriffsgewicht des Einsatzes von nachrichtendienstlichen Verbindungen kann stark variieren. Regelmäßig werden nachrichtendienstliche Verbindungen eingesetzt, um relevante, z.B. militärische Sachverhalte oder Entitäten aufzuklären. Dabei geht es dem Bundesnachrichtendienst jedoch in der Regel nicht darum, Personen als solche aufzuklären. Vielmehr sind einschlägige inhaltliche lage- bzw. entitätsrelevante Informationen gerade ohne vertieften Bezug zu den Personen selbst, Ziel der Maßnahmen. Es gibt Fallkonstellationen, bei denen über einen langen Zeitraum eine Person mit nachrichtendienstlich relevantem Wissen regelmäßig, z.B. etwa zweimal im Jahr zu Entwicklungen in einem bestimmten militärischen Bereich eines ausländischen Staates befragt wird. Private Informationen von natürlichen Personen spielen dabei typischerweise keine wesentliche Rolle. Ein erhöhtes Eingriffsgewicht ist daher in diesen Regelfällen zu verneinen.

In § 24 wird demgegenüber nun speziell der Einsatz einer nachrichtendienstlichen Verbindung gegen eine Person geregelt, also wenn die Maßnahme gerade darauf abzielt, dass eine systematische Sammlung von Informationen zu dieser Person um ihrer selbst willen erfolgen soll.

Entsprechend der Rechtsprechung des Bundesverfassungsgerichts nimmt die Eingriffsintensität des Einsatzes von nachrichtendienstlichen Verbindungen mit der Wahrscheinlichkeit des Zugangs zu höchstprivaten Informationen einer Person zu. Verfassungsrechtlich bedeutsam ist, welche Intensität die Beziehungen erlangen (vgl. BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 341). Dementsprechend bestimmt diese Regelung Fallkonstellationen des Einsatzes von nachrichtendienstlichen Verbindungen, die über den oben beschriebenen Standardeinsatz dieses nachrichtendienstlichen Mittels hinausgehen, da sie besonders eingriffsintensiv wirken und damit höheren materiellen Schwellen unterliegen müssen, als diejenigen, die in § 18 vorgesehen sind. Dies ist der Fall bei einem Einsatz einer nachrichtendienstlichen Verbindung gegen eine Person oder nochmals gesteigert durch eine hinzutretende besondere persönliche Vertrauensbeziehung zwischen der nachrichtendienstlichen Verbindung und der betroffenen Person. Diese Fallkonstellationen werden nach einer sechsmonatigen Anfangsphase, in der die Intensität der Datenerhebung typischerweise in qualitativer und quantitativer Hinsicht noch kein erhöhtes Eingriffsgewicht erreicht (siehe weitere Ausführungen zu Absatz 2 nachfolgend), überhaupt erst zum Tragen kommen können.

In § 24 wird ein Sonderfall des Einsatzes eines nachrichtendienstlichen Mittels geregelt, nämlich der Einsatz einer nachrichtendienstlichen Verbindung gegen eine Person (vgl. § 20). Dementsprechend sind zusätzlich zu den Vorgaben in dieser Regelung auch die grundsätzlichen Vorgaben betreffend einen gegen Personen gerichteten Einsatz nachrichtendienstlicher Mittel zu beachten. Im Fall des hiesigen Absatz 1 ist dies die Präferenzregel des § 20 Absatz 2 sowie im Fall des hiesigen Absatz 2 das Verantwortlichkeitsprinzip des § 20 Absatz 3. Für die nicht eingriffsintensiven Fälle des Einsatzes einer nachrichtendienstlichen Verbindung gegen eine Person, die auf Grundlage des § 18 erfolgen (Einsatzzeitraum unter sechs Monaten bzw. kein Aufbau einer besonderen persönlichen Vertrauensbeziehung) gilt 20 Absatz 2 ohnehin.

Das abgestufte System der Absätze 1 (gegenüber Ausländern im Ausland) und 2 (gegenüber Inländern und Deutschen) trägt dem Umstand Rechnung, dass die nachrichtendienstliche Maßnahme gegenüber einer Ausländerin oder einem Ausländer im Ausland grundsätzlich ein geringeres Eingriffsgewicht aufweist. Diese Personengruppe unterliegt typischerweise nicht dem Zugriff deutscher Behörden und ist damit in deutlich verringertem Ausmaß Folgemaßnahmen ausgesetzt, vgl. BVerfG Urteil vom 19. Mai 2020, 1 BvR

2835/17 (154, 152), Rn. 186. Für die rechtliche Einordnung der Maßnahme ist damit maßgeblich, gegenüber wem die nachrichtendienstliche Verbindung zum Zweck der Informationsgewinnung eingesetzt wird, der Belegenheitsort einzelner nachrichtendienstlicher Handlungen ist dagegen nicht maßgeblich. Entsprechend ist – gegenüber den in Absatz 2 geregelten „Inlandssachverhalten“ – eine mit dem verminderten Eingriffsgewicht korrespondierende Abstufung der Eingriffsschwellen vorgesehen.

Zu Absatz 1

Das Eingriffsgewicht des Einsatzes einer nachrichtendienstlichen Verbindung steigt, wenn sich der Einsatz gegen eine Person richtet, d.h. wenn die nachrichtendienstliche Verbindung eine Person „um ihrer selbst willen“ aufklärt. Bei einer solchen Ausgestaltung der nachrichtendienstlichen Maßnahme wird davon ausgegangen, dass zwischen der nachrichtendienstlichen Verbindung und der betroffenen Person als Aufklärungsziel eine intensivere Beziehung entstehen kann, als in den Fällen, in denen die nachrichtendienstliche Verbindung nur zu ihrer Kenntnis zu bestimmten Sachverhalten Auskunft gibt.

Absatz 1 enthält die Befugnis für den Einsatz einer nachrichtendienstlichen Verbindung gegen Ausländerinnen und Ausländern im Ausland für einen Zeitraum von über sechs Monaten (Nummer 1) oder, wenn die betroffene Person zu der nachrichtendienstliche Verbindung eine besondere persönliche Vertrauensbeziehung unterhält (Nummer 2).

Zu Nummer 1

Bezüglich des Zeitraums von sechs Monaten ist erst nach dieser Zeit ist davon auszugehen, dass zum einen der Kontakt der nachrichtendienstlichen Verbindung zur betroffenen Person als auch der Kontakt der nachrichtendienstlichen Verbindung zum Bundesnachrichtendienst in quantitativer und qualitativer Hinsicht eine Intensität erlangen kann, die ein erhöhtes Eingriffsgewicht mit sich bringen kann. Der Sechsmonatszeitraum berücksichtigt also im Sinne der Rechtsprechung des Bundesverfassungsgerichts insbesondere das Ausmaß der Ausnutzung persönlicher Vertrauensverhältnisse durch die nachrichtendienstliche Verbindung. Der Sechsmonatszeitraum beginnt in dem Moment, in dem die nachrichtendienstliche Verbindung gegenüber dem Bundesnachrichtendienst zustimmt mit diesem zusammen zu arbeiten und alle Vorprüfungen durch den Bundesnachrichtendienst abgeschlossen sind. Wird der Einsatz einer nachrichtendienstlichen Verbindung erst nachträglich eingriffsintensiv, ist diesbezüglich eine Anpassung der Anordnung des Einsatzes der nachrichtendienstlichen Verbindung erforderlich. Der Sechsmonatszeitraum beginnt in diesem Fall mit der entsprechenden Steuerung der nachrichtendienstlichen Verbindung. Die unabhängige Vorabkontrolle kommt nach Ablauf der Sechsmonatsphase zur Anwendung, vgl. BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 351, 353.

Zu Nummer 2

Die besondere persönliche Vertrauensbeziehung (welche von der vertieften Vertrauensbasis in § 25 zu unterscheiden ist), wirkt nochmals eingriffsintensivierend, da zur Bestimmung der Schwere eines Eingriffs entscheidend ist, ob und in welcher Intensität der Staat persönliches Vertrauen ausnutzt, um Geheimhaltungsinteressen zu überwinden und so eine Person zur Preisgabe von Informationen zu verleiten. Dabei wiegt die Begründung einer tieferen vermeintlichen Vertrauensbeziehung zur Informationsgewinnung besonders schwer. Das Bundesverfassungsgericht geht davon aus, dass je intensiver die vermeintliche Vertrauensbeziehung ist und je mehr private Informationen die betroffene Person preisgibt, desto tiefer der Grundrechtseingriff wirkt (siehe hierzu BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17 (162, 1), Rn. 340f.). Eine besonders persönliche Vertrauensbeziehung im Sinne dieser Regelung kann etwa bei vertrauensvollen Beziehungen in engen Verwandtschaftsverhältnissen oder langen, intensiven Freundschaftsbeziehungen vorliegen. Sie ist von sonstigen engen Vertrauenskontakten zu unterscheiden Die konkrete Würdigung kann nur nach Maßgabe der speziellen Umstände des jeweiligen Einzelfalls erfolgen.

Beispielsweise kann in bestimmten Einsatzlagen, die auf abgeschottete Strukturen aufbauen (z.B. Organisierte Kriminalität oder terroristische Gruppierungen), auch eine enge Beziehung womöglich auf allgemeinen subkulturellen sozialen Normen und nicht einer besonderen persönlichen Bindung aufbauen. Die Enttäuschung eines solchen subkulturellen Kodex ist kein im Sinne dieser Norm qualifizierender Vertrauensbruch. Eine besonders persönliche Vertrauensbeziehung ist ferner zu unterscheiden von einer wirtschaftlichen Abhängigkeit oder Unterstützung im Alltag oder sonstigen alltäglichen Beziehungen, etwa der Nachbarschaft (auch in Gemeinschaftsunterkünften), bei Freizeitaktivitäten oder in einem Freundeskreis. Nicht maßgeblich sind auch frühere besonders persönliche Vertrauensbeziehungen, beispielsweise eine vormalige, aber zwischenzeitlich zerrüttete intensive Freundschaft.

Zu Absatz 2

Dieser Absatz regelt den Einsatz einer nachrichtendienstlichen Verbindung gegen deutsche Staatsangehörige oder sich im Bundesgebiet dauerhaft aufhaltenden Personen unter erhöhten Voraussetzungen korrespondierend zur erhöhten Eingriffstiefe dieser Maßnahme. Dabei beschränkt Nummer 2 den Einsatz einer nachrichtendienstlichen Verbindung zur Erlangung von Informationen gegen deutsche Staatsangehörige oder sich im Bundesgebiet dauerhaft aufhaltende Personen, zu der diese zudem noch eine besondere persönliche Vertrauensbeziehung unterhält, auf die Aufklärung von Bedrohungen von herausgehobener Bedeutung. Abzugrenzen ist dies von den noch intensiveren Intimbeziehungen oder vergleichbar engsten persönlichen Bindungen, die einen Ausschlussgrund nach § 21 Absatz 4 bilden.

Zu § 25 (Nutzung einer Legende auf vertiefter Vertrauensbasis)

Um der Rechtsprechung des Bundesverfassungsgerichts gerecht zu werden, regelt § 25 erhöhte Voraussetzungen für die Fälle, in denen Mitarbeiterinnen oder Mitarbeiter des Bundesnachrichtendienstes eine Legende mit dem Ziel auswählen und verwenden, um eine besonders vertiefte Vertrauensbasis zu Dritten zu schaffen und diese zur Informationsgewinnung auszunutzen und so im Rahmen dieses Verhältnisses auch mit der Erlangung höchstprivater oder eines großen Umfangs persönlicher Informationen zu rechnen ist (vgl. BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 341).

Eine Legendennutzung ist dabei die Tarnung einer nachrichtendienstlichen Handlung.

Die Vorschrift ist von § 24, bei dem die „Verwendung“ einer nachrichtendienstlichen Verbindung, welche gegebenenfalls zu der Zielperson eine besondere (persönliche) Vertrauensbeziehung unterhält, geregelt ist, zu unterscheiden. Bei § 25 ist demgegenüber der Einsatz von Bediensteten des Bundesnachrichtendienstes selbst geregelt, die zu Dritten per se keine vergleichbare persönliche Beziehung aufbauen (insoweit im Unterschied zu Innenbehörden). Vielmehr bleibt bei den in § 25 erfassten Fällen stets eine „Geschäftsbeziehung“ bestehen, bei der ein Dritter dem Bundesnachrichtendienst (auch ohne zu wissen, dass er mit diesem zusammenarbeitet) Informationen für eine Gegenleistung zur Verfügung stellt.

Ein Anwendungsfall des § 25 kann die Legendennutzung gegenüber einer nachrichtendienstlichen Verbindung sein. Nicht alle nachrichtendienstlichen Verbindungen des Bundesnachrichtendienstes werden klar geführt. Der Regelfall dieser Legendennutzung fällt allerdings unter § 18, denn die Legendennutzung der hauptamtlichen Mitarbeitenden des Bundesnachrichtendienstes gegenüber einer nachrichtendienstlichen Verbindung erfolgt in der Regel nicht zur Herstellung und Ausnutzung eines besonderen Vertrauensverhältnisses. Regelmäßig stehen die Mitarbeitenden des Bundesnachrichtendienstes zur nachrichtendienstlichen Verbindung nicht in einem besonderen Näheverhältnis. Es handelt sich eher um eine geschäftliche Beziehung (in der Regel Austausch Information gegen Geldleistung). Die Legendennutzung durch die Mitarbeitenden des Bundesnachrichtendienstes kann auch dem Schutz der nachrichtendienstlichen Verbindung (sog. „plausible deniability“) dienen.

Typischerweise besteht also zwischen den Mitarbeitenden des Bundesnachrichtendienstes und einer nachrichtendienstlichen Verbindung keine besondere persönliche Vertrauensbeziehung wie diese zwischen einer nachrichtendienstlichen Verbindung und der aufzuklärenden Person bestehen kann.

Im Ausnahmefall kann aber eine Legende derart angelegt und genutzt werden, um zum Zweck der Informationsgewinnung eine – gegenüber dem Standardfall – besonders vertiefte Vertrauensbasis (nicht aber eine besondere persönliche Vertrauensbeziehung) der Mitarbeitenden des Bundesnachrichtendienstes zu der nachrichtendienstlichen Verbindung aufzubauen oder zu pflegen. Für diese Fälle regelt § 25 erhöhte Zulässigkeitsvoraussetzungen. Kein Anwendungsfall des § 25 liegt vor, wenn nachrichtendienstliche Verbindungen von sich aus z.B. im Rahmen eines Treffens persönliche und private Informationen über sich selbst teilen – wie es in manchen Kulturkreisen als Gesprächseinstieg üblich ist und regelrecht erwartet wird, dies aber nicht Ziel der Legendennutzung ist.

Ein weiterer Anwendungsfall des § 25 kann dann vorliegen, wenn die oder der Mitarbeitende des Bundesnachrichtendienstes unter Nutzung einer auf Dauer angelegten Legende eine besonders vertiefte Vertrauensbeziehung zu Beteiligten einer aufzuklärenden Bedrohung mit dem Ziel aufbaut, dieses persönliche Vertrauen zur Überwindung von Geheimhaltungsinteressen auszunutzen und den Beteiligten so zur Preisgabe von Informationen zu verleiten (vgl. BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 340). Dabei erlangt die oder der Mitarbeitende des Bundesnachrichtendienstes die Informationen in diesem Fall direkt von den Beteiligten der aufzuklärenden Bedrohung und nicht über eine nachrichtendienstliche Verbindung.

Nicht umfasst von § 25 sind hingegen solche Legendennutzungen durch Mitarbeitende des Bundesnachrichtendienstes, die nur flankierend zu anderen operativen Maßnahmen in unregelmäßigen Zeitabständen und anlassbezogen erfolgen, oder aber die Nutzung einer auf Dauer angelegten Legende gegenüber Dritten, die nicht an der aufzuklärenden Bedrohung beteiligt sind und von denen keine Informationen erlangt werden sollen; Rechtsgrundlage für diese Art der Legendennutzung wäre § 18.

Ein Anwendungsfall des § 25 kann sich auch aus dem Aufbau eines Kontakts einer oder eines Mitarbeitenden des Bundesnachrichtendiensts im Internet unter Legende ergeben. Dadurch kann in aller Regel kein schutzwürdiges Vertrauen entstehen, denn grundsätzlich entsteht im Internet kein geschütztes Vertrauen. In der digitalen Umgebung des Internet ist es möglich, in weitem Umfang Kommunikationsbeziehungen aufzubauen, in deren Rahmen das Vertrauen eines Kommunikationsteilnehmers in die Identität und Wahrhaftigkeit seiner Kommunikationspartner nicht schutzwürdig ist, da hierfür keinerlei Überprüfungsmechanismen zur Verfügung stehen. Dies gilt selbst dann, wenn bestimmte Personen über einen längeren Zeitraum an der Kommunikation teilnehmen und sich auf diese Weise eine Art „elektronische Gemeinschaft“ gebildet hat. Auch dabei ist jedem Teilnehmer bewusst, dass er die Identität seiner Partner oder Partnerin nicht kennt oder deren Angaben über sich jedenfalls nicht prüfen kann, siehe dazu BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07 (120, 274ff.) Rn. 310, 311. Ein schutzwürdiges Vertrauen der betroffenen Person in die Identität und die Motivation seines Kommunikationspartners kann jedoch entstehen, wenn die Kommunikation im Internet realweltlich flankiert wird (durch zwischengeschaltete persönliche Treffen in physischer Präsenz). So kann ein geschütztes Vertrauen und möglicherweise aufgrund des Hinzutretens weiterer Umstände wie z.B. eines langen Zeitraums sogar ein Verhältnis auf einer besonders vertieften Vertrauensbasis entstehen. Diesem Umstand tragen die erhöhten materiellen Voraussetzungen des § 25 Rechnung.

Das abgestufte System der Absätze 1 (gegenüber Ausländern im Ausland) und 2 (gegenüber Inländern und Deutschen) trägt dem Umstand Rechnung, dass die nachrichtendienstliche Maßnahme gegenüber einer Ausländerin oder einem Ausländer im Ausland grundsätzlich ein geringeres Eingriffsgewicht aufweist. Diese Personengruppe unterliegt

typischerweise nicht dem Zugriff deutscher Behörden und ist damit in deutlich verringertem Ausmaß Folgemaßnahmen ausgesetzt, vgl. BVerfG Urteil vom 19. Mai 2020, 1 BvR 2835/17 (154, 152), Rn. 186. Für die rechtliche Einordnung der Maßnahme ist damit maßgeblich, gegenüber wem die Legende zum Zweck der Informationsgewinnung eingesetzt wird, der Belegenheitsort einzelner nachrichtendienstlicher Handlungen ist dagegen nicht maßgeblich. Entsprechend ist – gegenüber den in Absatz 2 geregelten „Inlandssachverhalten“ – eine mit dem verminderten Eingriffsgewicht korrespondierende Abstufung der Eingriffsschwellen vorgesehen.

Zu Absatz 1

Der Absatz regelt die materiellen Voraussetzungen bei einem Tätigwerden des Bundesnachrichtendienstes gegenüber Ausländerinnen und Ausländern im Ausland.

Zu Absatz 2

Absatz 2 regelt die materiellen Voraussetzungen bei einem Tätigwerden gegenüber Personen, die sich im Bundesgebiet aufhalten oder sich durch ihre deutsche Staatsangehörigkeit – unabhängig von ihrem Aufenthalt – in einem besonderen Näheverhältnis zur deutschen Staatsgewalt befinden. Hier begründet diese besondere Nähe zur deutschen Staatsgewalt, die gesteigerte Eingriffsintensität der Maßnahme, welche dazu führt, dass der Einsatz des nachrichtendienstlichen Mittels nur bei Vorliegen einer erheblichen Bedrohung zulässig ist. Zudem ist für eine solche nachrichtendienstliche Maßnahme eine Vorabkontrolle durch den Unabhängigen Kontrollrat vorgesehen.

Zu § 26 (Einsatz technischer Mittel zur längerfristigen Standortfeststellung)

§ 26 regelt den Einsatz technischer Mittel zur gezielten Erhebung von personenbezogenen Daten zur längerfristigen Standortfeststellung einer Person.

Im Grundsatz handelt es sich bei Maßnahmen der technischen Standortfeststellung um die Erhebung punktueller personenbezogenen Daten, eben um einen Standort einer Person zu einem bestimmten Zeitpunkt zu bestimmen. Anders als eine Observation durch visuelle oder akustische Überwachung sind mit Maßnahmen der technischen Standortfeststellung nur begrenztere Informationen, gerade nicht zum sonstigen Verhalten oder konkreter sozialer Interaktion, erhebbar, weshalb solche Maßnahmen grundsätzlich weniger eingreifend bleiben.

Mit der Dauer solcher Maßnahmen können diese jedoch auch an Eingriffsgewicht gewinnen. Abzugrenzen ist dies jedoch von einer bloß fragmentarischen Überwachung, zu der ein nicht laufend mitgeführter Gegenstand (z.B. Laptop) oder ein bestimmtes Verkehrsmittel (z.B. Kfz) genutzt wird (BVerfG, Beschluss vom 17. Juli 2024, 1 BvR 2133/22, Rn. 166, 168). Im Bereich der Spurfolgetechnik kann bspw. der Standort eines Kfz festgestellt werden. Wenn es sich hingegen um einen Gegenstand handelt, der – wie beispielsweise in breiten Lebenswelten heute ein Smartphone – typischerweise laufend an der Person geführt wird, und die Standortüberwachung über einen relevanten Zeitraum durchgehend erfolgt, so dass aus den gesammelten Daten objektiv ein persönlichkeitsrelevantes Bewegungsprofil erstellbar ist, ist es für die Eingriffsgewichtung unerheblich, ob die Maßnahme auch zu diesem Zweck durchgeführt wird (vgl. BVerfG, Beschluss vom 17. Juli 2024, 1 BvR 2133/22, Rn. 145).

Nicht vom Anwendungsbereich umfasst ist die Auswertung von auf der Grundlage anderer Befugnisnormen erhobener Daten, die Informationen enthalten, die zur Aufenthaltsbestimmung oder zur Erstellung von Bewegungsmustern geeignet sind wie etwa die Datenerhebung aus Telekommunikationsnetzen mittels eines IMSI-Catchers oder die Auswertung von aus allgemein zugänglichen Quellen erhobener Daten. Entscheidendes Kriterium für die Abgrenzung der Befugnis des § 26 von anderen Befugnissen – beispielsweise der technischen Aufklärung – ist, dass der Einsatz technischer Mittel gerade zur Standortfeststellung

erfolgt, also die Standortdaten nicht nur miterfasst werden, sondern gerade das (alleinige) Ziel der Überwachungsmaßnahme bilden.

Für die rechtliche Einordnung dieser nachrichtendienstlichen Maßnahme ist maßgeblich, gegenüber wem und wo die Standortfeststellung getätigt wird. Im Bundesgebiet kann der Bundesnachrichtendienst die nachrichtendienstliche Handlung unter erleichterten Rahmenbedingungen durchführen. Im Ausland sind derartige nachrichtendienstliche Handlungen für einen fremden Staat in der Regel strafbewehrt. Insofern ist die Tätigkeit gegenüber einer sich im Bundesgebiet aufhaltenden Person in Absatz 2 geregelt. Findet die Maßnahme gegenüber einem deutschen Staatsangehörigen im Ausland statt, ändert sich zwar an den Umständen der Durchführung nichts, jedoch fällt ins Gewicht, dass sich eine Person mit deutscher Staatsangehörigkeit – unabhängig von ihrem Aufenthalt – in einem besonderen Näheverhältnis zur deutschen Staatsgewalt befindet – insofern also auch ein Fall des Absatz 2.

Das abgestufte System der Absätze 1 (gegenüber Ausländern im Ausland) und 2 (gegenüber Inländern und Deutschen) trägt dem Umstand Rechnung, dass die nachrichtendienstliche Maßnahme gegenüber einer Ausländerin oder einem Ausländer im Ausland grundsätzlich ein geringeres Eingriffsgewicht aufweist. Diese Personengruppe unterliegt typischerweise nicht dem Zugriff deutscher Behörden und ist damit in deutlich verringertem Ausmaß Folgemaßnahmen ausgesetzt, vgl. BVerfG Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 186. Für die rechtliche Einordnung der Maßnahme ist damit maßgeblich, gegenüber wem die nachrichtendienstliche Maßnahme eingesetzt wird, der Belegenheitsort einzelner nachrichtendienstlicher Handlungen ist dagegen nicht maßgeblich. Entsprechend ist – gegenüber den in Absatz 2 geregelten „Inlandssachverhalten“ – eine mit dem verminderten Eingriffsgewicht korrespondierende Abstufung der Eingriffsschwellen vorgesehen.

Zu Absatz 1

Der Absatz regelt die materiellen Voraussetzungen bei einem Tätigwerden des Bundesnachrichtendienstes gegenüber Ausländerinnen oder Ausländern im Ausland. Dabei ist abhängig vom jeweiligen Zeitraum der Überwachung eine Abstufung geboten.

Zu Nummer 1

In Nummer 1 sind solche Einsatzvarianten gebündelt, welche aufgrund ihres Eingriffsgewichts – jedenfalls bei personeller und örtlicher Auslandszielrichtung – einen Mitteleinsatz (noch) auf Ebene der nachrichtendienstlichen Auslandsaufklärung als Grundstufe rechtfertigen. Zu dem Umstand, dass dieser Mitteleinsatz – trotz der zu § 18 Absatz 1 vergleichbaren Schwellen – in Unterabschnitt 2 geregelt ist, vgl. oben.

Zu Buchstabe a

Hierunter fallen einerseits durchgehende Überwachungen über eine volle Woche, auf Grundlage derer aussagekräftige Bewegungsprofile entstehen können, die in erheblich eingreifender Weise Persönlichkeitsrelevanz besitzen (Doppelbuchstabe aa). Außerdem erfasst werden punktuelle Einsätze, die in der Zusammenschau eines größeren Zeitraums – hier 14 oder mehr Tage in einem Zeitraum von 30 Tagen – ein gleichwertiges Eingriffsgewicht wie durchgehende Einsätze über einen kürzeren Zeitraum erreichen (Doppelbuchstabe bb). Maßgebend bleibt aber auch insoweit, dass der Einsatz täglich durchgehend erfolgt, also geeignet ist die Bewegungen an diesem Tag zusammenhängend zu überwachen.

Zu Buchstabe b

Zudem ist klargestellt, dass bei nicht durchgehenden oder punktuellen Standortbestimmungen, die in ihrer Eingriffstiefe gleichwohl einer durchgehenden Überwachung in den in

Nummer 1 genannten Zeiträumen entsprechen, ebenfalls eine längerfristige Standortfeststellung vorliegt.

Zu Nummer 2

In Nummer 2 sind Mitteleinsätze geregelt, deren Eingriffsintensität das Erreichen der ersten Qualifikationsstufe erfordert. Aus durchgehend dreißigtägiger Überwachung (Absatz 1 Nummer 2 Buchstabe a Doppelbuchstabe aa) oder einer wöchentlich durchgehenden Überwachung an fünf oder mehr Wochen innerhalb eines Zeitraums von 60 Tagen (Absatz 1 Nummer 2 Buchstabe a Doppelbuchstabe bb) können womöglich validierte weitergehende Bewegungsmuster erkannt werden, die einerseits Schlüsse auf dauerhafte Beziehungen zu bestimmten Orten und mittelbar womöglich auch auf verfestigte Beziehungen zu bestimmten Personen eröffnen können und andererseits selbst atypische, seltenere örtliche Beziehungen mit erfassen. Daraus folgt ein gesteigertes Eingriffsgewicht, dass die Voraussetzungen der ersten Qualifikationsstufe erforderlich macht. Abermals werden zudem auch atypische Fälle erfasst, bei denen das jeweilige Eingriffsgewicht einer Überwachung den in Nummer 2 Buchstabe a genannten Zeiträumen entspricht (Absatz 1 Nummer 2 Buchstabe b).

Zu Absatz 2

Absatz 2 regelt die materiellen Voraussetzungen bei einem Tätigwerden gegenüber Personen, die sich im Bundesgebiet aufhalten oder sich durch ihre deutsche Staatsangehörigkeit – unabhängig von ihrem Aufenthalt – in einem besonderen Näheverhältnis zur deutschen Staatsgewalt befinden, wenn die Maßnahme über einen Zeitraum durchgeführt wird, der zu einer Erstellung eines – zumindest partiellen – Bewegungsprofils führen kann.

Dabei gilt für Maßnahmen, die längerfristig im Sinne des Absatzes 1 Nummer 1 Buchstabe a) sind, dass diese nur zulässig sind, wenn sie im Einzelfall erforderlich sind, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen (Absatz 2 Nummer 1).

Absatz 2 Nummer 2 regelt die Voraussetzungen für Maßnahmen, die aufgrund ihrer besonders langen Dauer ein nochmals qualifiziertes, besonderes Eingriffsgewicht aufweisen, was bei einem Einsatz gegenüber Deutschen und Inländern das Erreichen der zweiten Qualifikationsstufe erfordert.

Zu Absatz 3

In Absatz 3 wird der durchgehende Einsatz näher definiert. Maßgeblich ist insoweit, dass eine zusammenhängende Überwachung der Bewegungen einer Person erfolgt. Die Qualifikationsschwellen, die sich nach der Einsatzdauer richten, können somit nicht durch Kurzzeitunterbrechungen umgangen werden. Maßgeblich ist, ob eine Maßnahme auch bei temporärer Unterbrechung noch als Gesamtansatz sachlich verbundener Teilakte zu verstehen ist. Andererseits bedingt die Beendigung einer Maßnahme nicht notwendig den technischen Rückbau von Einsatzmitteln. Maßgeblich ist deren Nutzung zur Standortfeststellung. Sie können also auch für spätere Einsätze an ihren Platzierungen verbleiben, ohne dass dies die Dauer eines abgeschlossenen Einsatzes verlängert.

Zu Absatz 4

Absatz 4 stellt klar, dass die Erhebung von Standortdaten im Rahmen von Maßnahmen nach dem Unterabschnitt 3 nicht dem § 26 unterfallen. Hierdurch werden Wertungswidersprüche vermieden, die dadurch entstehen könnten, dass die Befugnisse zur technischen Aufklärung oftmals Standortdaten „mitumfassen“, diese allerdings weder das Ziel der technischen Aufklärungsmaßnahme sind noch eine verlässliche Prognose dazu getroffen werden kann, ob und in welchem Ausmaß Standortdaten wirklich erfasst werden.

Zu § 27 (Längerfristige optische und akustische Überwachung)

Die Regelung trägt dem Umstand Rechnung, dass das Eingriffsgewicht von Überwachungen sehr unterschiedlich sein kann (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 357). Die Grundbefugnis zur optischen und akustischen Überwachung ergibt sich bereits unmittelbar aus § 18. § 27 ergänzt diese Grundnorm, indem typischerweise eingriffsqualifizierende Umstände an korrespondierende Voraussetzungen geknüpft werden. Hierbei findet die Dauer der Maßnahmen besondere Berücksichtigung.

Erfasst ist dabei sowohl eine (nur) optische, eine (nur) akustische wie auch eine kumulativ optische und akustische Überwachung.

Für die Qualifikationskriterien der Maßnahmendauer in Absatz 2 ist dabei jeweils entscheidend, dass die Maßnahme gegenüber einer Person mit deutscher Staatsangehörigkeit oder einer sich im Bundesgebiet aufhaltenden Person für einen längeren Zeitraum personengerichtet durchgeführt wird. Wird beispielsweise ein Objekt stationär auch längerfristig überwacht, um festzustellen welche Personen sich dort einfinden, ist die Dauer kein Indikator dafür, dass hierbei jeweils gewichtige Eingriffe in die informationelle Selbstbestimmung dieser Personen erfolgen. Gleiches gilt, wenn die stationäre Beobachtung gegen eine bestimmte Person gerichtet ist, da hier eben nur ein sehr enger, lokaler Ausschnitt – auch längerfristiger stationärer Beobachtung – im Blick ist. Die Dauer indiziert das qualifizierte Gewicht des Eingriffs nur bei ortsunabhängiger, d.h. der Person folgender Überwachung. Dies wird mit dem Begriff „durchgehend“ tatbestandlich erfasst. Durchgehend meint unterbrechungsfrei. Eine Unterbrechung, die nicht aus der fachlichen Einschätzung ihrer Geeignetheit und Erforderlichkeit für die Auslandsaufklärung, d.h. der angestrebten Erkenntnisgewinnung unter wirtschaftlichem Mitteleinsatz, plausibel ist und danach als Umgehung der Schwellen erscheint, steht der Qualifikation als durchgehende Maßnahme jedoch nicht entgegen. Umgekehrt sind fachlich nachvollziehbare Unterbrechungen, etwa zu bestimmten Zeitfenstern, beachtlich, unabhängig davon, ob hierbei andere Überwachungsmaßnahmen (wie technische Spurfolge oder Ortsüberwachung) fortlaufen.

Für die rechtliche Einordnung dieser nachrichtendienstlichen Maßnahme ist maßgeblich, gegenüber wem und wo die Überwachung stattfindet. Innerhalb des Bundesgebiets kann der Bundesnachrichtendienst – verglichen mit einer solchen Tätigkeit im Ausland – Überwachungen unter etwas erleichterten Rahmenbedingungen durchführen, da den durchführenden Mitarbeiterinnen und Mitarbeitern zumindest von staatlicher Seite im Regelfall insbesondere keine Strafverfolgung droht. Insofern ist die Überwachungstätigkeit gegenüber einer sich im Bundesgebiet aufhaltenden Person in Absatz 2 geregelt. Findet die Maßnahme gegenüber einem deutschen Staatsangehörigen im Ausland statt, ändert sich zwar an den Umständen der Durchführung nichts, jedoch fällt ins Gewicht, dass sich eine Person mit deutscher Staatsangehörigkeit – unabhängig von ihrem Aufenthalt – in einem besonderen Näheverhältnis zur deutschen Staatsgewalt befindet – insofern also auch ein Fall des Absatz 2.

Zu Absatz 1

Der Absatz regelt die materiellen Voraussetzungen bei einer längerfristigen optischen und/oder akustischen Überwachung gegenüber Ausländerinnen und Ausländern im Ausland. Die abgestufte Ausgestaltung der gesetzlichen Befugnis in Absatz 1 – insbesondere, dass die Befugnis bereits zur nachrichtendienstlichen Auslandsaufklärung zulässig ist, solange der Zeitraum der Nummer 2 nicht erreicht wurde, und darüber hinaus „nur“ die zweite Qualifikationsstufe erfordert – trägt dem Umstand Rechnung, dass die nachrichtendienstliche Maßnahme gegenüber einer Ausländerin oder einem Ausländer im Ausland ein geringeres Eingriffsgewicht aufweist. Diese Personengruppe unterliegt typischerweise nicht dem Zugriff deutscher Behörden und ist damit in deutlich verringertem Ausmaß Folgemaßnahmen ausgesetzt, vgl. BVerfG Urteil vom 19. Mai 2020 1 BvR 2835/17 (154, 152), Rn. 186.

Zu Nummer 1

Die in Nummer 1 Buchstabe a zugrunde gelegte Dauer von 48 oder mehr Stunden greift die Frist des früheren Art. 19a BayVSG auf. Die Regelung ist vom Bundesverfassungsgericht (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17 (161, 1)) geprüft worden, ohne dass die Dauer auf Kritik gestoßen ist. Die Frist betrifft eine durchgängige Überwachung über diese Dauer, also nicht die zeitliche Summe von zu verschiedenen Zeiten ansetzender Observation. Mit der zweiten Alternativen werden jedoch eine Mehrzahl von lediglich punktuellen Observationen erfasst, wenn etwa die aufzuklärende Person regelmäßig bestimmte Orte aufsucht, etwa Szeneeinrichtungen an bestimmten Tagen zu bestimmten Zeiten, und angenommen wird, dass dort relevantes Geschehen zu beobachten ist. Die in Nummer 1 Buchstabe b enthaltene Schwelle von sieben oder mehr Tagen innerhalb eines Zeitraums von 30 Tagen soll solche punktuellen Überwachungen erfassen. In atypischen Konstellationen, wenn beispielsweise im Monat weniger, dabei aber nicht nur punktuell, sondern tagsüber komplett oberviert würde, würde dies ebenfalls erhebliches Eingriffsgewicht entfalten.

Zu Nummer 2

Mit einer Wochendauer erfolgt eine Überwachung, die unterschiedliche Lebensabläufe an allen Werktagen und dem Wochenende einschließt. In diesen Fällen bedarf der Mitteleinsatz (gegenüber Ausländern im Ausland) aufgrund der Eingriffsintensität der ersten Qualifikationsstufe.

Zu Absatz 2

In Absatz 2 ist der Einsatz der längerfristigen optischen und akustischen Überwachung gegenüber Deutschen und sich im Bundesgebiet aufhaltenden Personen geregelt. Nach Absatz 2 Nummer 1 erfordert eine Maßnahme, die längerfristig im Sinne des Absatzes 1 Satz 2 ist, aufgrund des besonderen Eingriffsgewichts, welches für diese Personen von der Nähe zur staatlichen Gewalt ausgeht, dass diese im Einzelfall erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen. Bei dem in Nummer 2 nochmals erhöhten Eingriffsgewicht ist das Vorliegen der Voraussetzungen der zweiten Qualifikationsstufe erforderlich.

Zu Absatz 3

Der Einsatz technischer Mittel zur optischen oder akustischen Aufzeichnung schafft eine erweiterte Möglichkeit, dass heimlich beobachtete Verhalten umfassend zu erfassen und auch noch nachgängig vertiefend auszuwerten. Der Anwendungsbereich der Norm ist auf den nichtöffentlichen Raum begrenzt. Auch im öffentlichen Raum besteht zwar ein schutzwürdiges Interesse, dass eigenes Verhalten nicht Gegenstand gezielter staatlicher Beobachtung ist. Dies ist aber bereits mit der allgemeinen Befugnis zum Einsatz heimlicher Informationsgewinnung durch Einsatz nachrichtendienstlicher Mittel beschränkt und auch insoweit also nicht voraussetzungslos zulässig, sondern an § 18 Absatz 1 gebunden.

Im Inland ist die Aufzeichnung (der allgemeinen Stufensystematik beim Einsatz von ND-Mitteln gegen Inländer/Deutsche und gegen Ausländer im Ausland folgend) jeweils eingriffsqualifizierend. Das bedeutet, dass, falls die Maßnahme auf die Überwachung von deutschen Staatsangehörigen oder sich im Bundesgebiet aufhaltenden Personen zielt (also z.B. nicht nur eine zufällige Erfassung eines Deutschen im Ausland erfolgt), die erste Qualifikationsstufe erforderlich ist. Eine noch weitergehende Eingriffsintensivierung, welche das Erfordernis der zweiten Qualifikationsstufe begründet, liegt vor, wenn damit zu rechnen ist, dass aufgrund der Maßnahme mit der Erfassung höchstprivater Informationen zu rechnen ist. Dies kann etwa der Fall sein, wenn das Verhalten in einem nicht öffentlichen Raum aufgezeichnet werden soll, der eine besondere Schutzzone darstellt, ohne zugleich ein Wohnraum zu sein. Ein Beispiel hierfür wäre etwa eine familiäre Feierlichkeit in einem angemieteten Lokal.

Zu Absatz 4

Die qualifizierten „Inlands-Voraussetzungen“ gelten nicht für die Fälle der Absicherung von durch den Bundesnachrichtendienst eingesetzten Personen in Situationen wie z.B. den Treffen mit einer nachrichtendienstlichen Verbindung. D.h. das Maßnahmen nach den Absätzen 1 bis 3, bei denen der Schutz dieser Personen im Mittelpunkt steht, den erhöhten materiellen und formellen Voraussetzungen dieser Norm nicht genügen müssen. Ausgenommen bleibt der Fall des Absatzes 3 Satz 2, bei dem mit der Erhebung von höchstprivaten Informationen zu rechnen ist.

Umfasst sind Treffen des Bundesnachrichtendienstes mit seinen nachrichtendienstlichen Verbindungen oder Personen, die als nachrichtendienstliche Verbindungen gewonnen werden sollen, und die unter Umständen auch Maßnahmen nach Satz 1 einbeziehen können. Die Absicherung im Sinne des Absatzes 4 erfolgt in der Regel durch eine Schutz-Observation, also eine Observation zum Ausschluss einer Gefahr für Leib und Leben des Mitarbeitenden des Bundesnachrichtendienstes oder auch der nachrichtendienstlichen Verbindung. Die Observation soll dazu dienen, festzustellen, dass kein dem Treffen vorhergehender oder nachfolgender Kontakt der nachrichtendienstlichen Verbindung zu einem anderen Nachrichtendienst erfolgt oder z.B. eine Gegenobservation der nachrichtendienstlichen Verbindung bzw. der Mitarbeitenden des Bundesnachrichtendienstes durch einen anderen Nachrichtendienst stattfindet. Hierbei handelt es sich um für die effektive nachrichtendienstliche Tätigkeit des Bundesnachrichtendienstes notwendige Schutzmaßnahmen. Diese besondere Sicherung der operativ eingesetzten Personen hat eine derart hohe Bedeutung für die Funktionsfähigkeit des Bundesnachrichtendienstes, dass derartige Maßnahmen nicht an die in der Norm vorgegebenen zeitlichen Grenzen gebunden sind und die hier als ein besonderer Fall der Eigensicherung spezifisch geregelt wird. Insbesondere die geheimdienstliche Aufklärungstätigkeit anderer Staaten birgt für Leib, Leben und Freiheit insbesondere der operativ Mitarbeitenden des Bundesnachrichtendienstes – sogar zunehmend – Gefahren, die bis in deren Privatleben (insbesondere Reisen ins Ausland) hineinwirken. Dies begegnet insofern auch keinen rechtlichen Bedenken, da die Zielrichtung dieser Maßnahmen sich von derjenigen der eigentlichen Maßnahme zur Informationsbeschaffung im Sinne des Aufklärungsauftrags des Bundesnachrichtendienstes unterscheidet. Ziel der Maßnahme ist nicht die Gewinnung von außen- oder sicherheitspolitisch bedeutsamen Informationen, sondern die Sicherung der operativ eingesetzten Personen. Die Eingriffsintensität gegenüber den von dieser Sicherungsmaßnahme betroffenen Personen ist hierbei geringer, da das nachrichtendienstliche Mittel nicht eingesetzt wird, um Informationen zu erlangen, die in Produkte des Bundesnachrichtendienstes einfließen sollen, mithin in der Regel keine nachteiligen Folgemaßnahmen für die betroffene Person drohen.

Gleiches gilt für Maßnahmen bei der Prüfung von Personen in Bezug auf ihren Einsatz als nachrichtendienstliche Verbindungen. Insoweit wird auf die Begründung zu § 20 Absatz 4 verwiesen.

Zu Absatz 5

In Absatz 5 ist klargestellt, dass die Voraussetzungen einer Wohnraumüberwachung bzw. eines Eingriffs in Informationstechnische-Systeme nicht unterlaufen werden dürfen.

Zu § 28 (Maßnahmen bei Post- und Warensendungen)

Die Regelung ermöglicht es dem Bundesnachrichtendienst, die dem Brief- oder Postgeheimnis nach Artikel 10 Absatz 1 des Grundgesetzes unterliegenden Sendungen zu öffnen, einzusehen und in der Sendung enthaltende Gegenstände zu manipulieren.

Eine Beschränkung dieses Grundrecht darf nach Artikel 10 Absatz 2 Satz 1 des Grundgesetzes nur auf Grund eines Gesetzes erfolgen. Dieser Vorgabe entsprechend war in dem nunmehr aufgelösten Artikel 10-Gesetz (§§ 3 Absatz 1, 1 Absatz 1 des Artikel 10-Gesetzes) unter anderem der Bundesnachrichtendienst zu Beschränkungen des Grundrechts aus

Artikel 10 Absatz 1 des Grundgesetzes befugt. Diese Beschränkungsbefugnis war aufgrund der Auflösung des Artikel 10-Gesetzes in das Bundesnachrichtendienstgesetz zu übertragen. Dabei wurden die Voraussetzungen der Befugnis systematisch von dem im Artikel 10-Gesetz enthaltenen Straftatenkatalog gelöst und stattdessen, der allgemeinen Systematik dieses Gesetzes entsprechend, auf die in § 3 Absatz 1 typisierten erheblichen Bedrohungen für besonders hochrangige Rechtsgüter gegründet. Durch diese Vereinheitlichung der Systematik wird das Gesetz sowohl für den Normanwender als auch für etwaige Betroffene verständlicher. Zudem bildet die Bezugnahme auf Bedrohungen den spezifischen Auftrag des Bundesnachrichtendienstes ab, zum Zwecke der Früherkennung von Bedrohungen seine Aufklärung bereits im Vorfeld von (konkreten) Gefährdungslagen zu betreiben (vergleichbar für die Verfassungsschutzbehörden: BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 154).

Zu Absatz 1

Die Befugnis in Absatz 1 gilt für ein Tätigwerden des Bundesnachrichtendienstes gegenüber Ausländerinnen und Ausländern im Ausland, deren Sendungen aufgrund internationaler Transportwege auch Deutschland passieren können (vgl. Absatz 2, der demgegenüber eine spezielle Regelung bei der Betroffenheit deutscher Staatsangehöriger oder von Inländerinnen und Inländern trifft). Das Öffnen und Einsehen von Sendungen, die dem Brief- oder Postgeheimnis unterliegen, durch den Bundesnachrichtendienst begründet einen Eingriff in Artikel 10 Absatz 1 des Grundgesetzes von beträchtlichem Gewicht. Ein solcher Eingriff bedarf einer hinreichenden verfassungsrechtlichen Rechtfertigung. Dabei ist insbesondere zu berücksichtigen, dass die Einbußen an grundrechtlich geschützter Freiheit nicht in unangemessenem Verhältnis zu den Gemeinwohlzwecken stehen, denen die Grundrechtsbeschränkung dient (BVerfG, Urteil vom 14. Juli 1999, 1 BvR 2226/94, Rn. 219). § 28 Absatz 1 trägt diesem Verhältnis zwischen Grundrechtsschutz und Gemeinwohl dadurch Rechnung, dass die Befugnis des Bundesnachrichtendienstes nur eröffnet ist, wenn sie Einzelfall erforderlich ist, um Informationen zu erheblichen Bedrohungen zu erlangen. Demgegenüber kann eine Überwachung auch dergestalt erfolgen, dass nur die „Verkehrsdaten“ von Sendungen erfasst – bzw. (praktisch relevanter) im Rahmen eines Auskunftsverlangens vom jeweiligen Postdienstleister abgefragt werden. In diesem Fall ist – sofern es sich um die Daten von Ausländern im Ausland handelt – eine Überwachung schon auf der Grundstufe nachrichtendienstlicher Auslandsaufklärung gerechtfertigt.

Zu Absatz 2

In Absatz 2 ist die Befugnis zum Öffnen und Einsehen von Postsendungen gegenüber deutschen Staatsangehörigen, inländischen juristischen Personen sowie sich im Bundesgebiet aufhaltenden Personen näher geregelt. Die Vorschrift findet dabei aufgrund der Auflösung des Artikel 10-Gesetzes nunmehr Eingang ins BND-Gesetz.

Dabei wird – bei Vereinheitlichung der Systematik – dem hiervon ausgehenden, besonders gewichtigen Eingriff in das Grundrecht aus Artikel 10 Absatz 1 des Grundgesetzes durch das tatbestandliche Erfordernis einer Bedrohung von herausgehobener Bedeutung Rechnung getragen, wenn sich die Erhebung auf Inhalte der Sendungen (mithin: im technischen Sinne „Inhaltsdaten“) erstreckt. Wird demgegenüber die Maßnahme auf die Umstände der Verkehre (also „Verkehrsdaten“) beschränkt, so ist sie bereits zulässig, wenn tatsächliche Anhaltspunkte für eine erhebliche Bedrohung vorliegen.

Der in § 3 Absatz 1 des Artikel 10-Gesetzes enthaltene Bezug auf einen Katalog von Straftaten wird aufgelöst und ersetzt. Dies ist aus einer Reihe von Gründen geboten: Zunächst entspricht der Bezug auf konkrete Straftatbestände auf Ebene der nachrichtendienstlichen Informationserhebung nicht der Arbeit des Bundesnachrichtendienstes, dessen Tätigkeit gerade im Rahmen und zum Zwecke der Früherkennung von Bedrohungen erfolgt. Die Anknüpfung an den „Verdacht“ einer Straftatbegehung ist insoweit systemfremd. Des Weiteren folgt aus der Auflösung des Straftatbestandes und der nunmehr vorgesehenen

Bezugnahme auf Bedrohungen von herausgehobener Bedeutung eine systematische Harmonisierung, welches sowohl die Verständlichkeit des Gesetzes erhöht als auch dessen Anwendung erleichtert. Zuletzt gebietet auch die Auflösung des Artikel 10-Gesetzes, welches auf alle drei Nachrichtendienste des Bundes Anwendung fand, einen klareren Bezug zum Aufgabenprofil des Bundesnachrichtendienstes, der nunmehr alleiniger Adressat der Regelung ist – so ist etwa § 3 Absatz 1 Nummer 2 des Artikel 10-Gesetzes erkennbar primär auf die Aufgabenerfüllung des Bundesamtes für den Verfassungsschutz und des Bundesamtes für den Militärischen Abschirmdienst zugeschnitten.

In Absatz 2 Satz 2 wird der Subsidiaritätsgrundsatz des § 3 Absatz 2 Satz 1 des Artikel 10-Gesetzes übernommen, demzufolge eine Maßnahme nach § 28 Absatz 2 nur zulässig ist, wenn die Erforschung des Sachverhaltes auf andere – d.h. weniger eingriffsintensive, intensitätsvergleichbare Maßnahmen bleiben ausgenommen – Weise aussichtslos oder wesentlich erschwert wäre. Absatz 2 Satz 3 entspricht der bisherigen Regelung in § 3 Absatz 2 Satz 4 des Artikel 10-Gesetzes.

Zu Absatz 3

Die in Absatz 3 neu geschaffene Befugnis ermöglicht es dem Bundesnachrichtendienst, Post- und Warensendungen zu bearbeiten. Dabei unterscheidet die Regelung zwischen solchen Bearbeitungen, welche der Informationsgewinnung dienen (Satz 1) und solchen, welche über die Informationsgewinnung hinausgehen und der Gefahrenabwehr dienen (Satz 2).

Unter den in Satz 1 geregelten Anwendungsbereich fallen etwa Konstellationen, in denen eine Person von nachrichtendienstlichem Interesse bei einem Elektronikhändler IT-Ausstattung bestellt. Durch das Einwirken auf die Sendung kann die Hard- oder Software der IT-Ausstattung so manipuliert werden, dass eine spätere Maßnahme nach Unterabschnitt 3 möglich wird. Darüber hinaus ermöglicht diese Fallvariante auch, unmittelbar nachrichtendienstliche Er-kenntnisse zu generieren. Ein solcher Anwendungsfall wäre etwa gegeben, wenn eine Person von nachrichtendienstlichem Interesse über einen Logistikdienstleister ein Dual-Use-Gut geliefert bekommt, dessen Endverbleib geklärt werden soll. Durch Manipulation der Sendung (bspw. durch Verbringen eines Spurfolgegeräts) kann der Zielort der Ware ermittelt werden. Eine Manipulation des Dual-Use-Gutes könnte darüber hinaus indes in Ausnahmefällen auch durch Unbrauchbarmachung erfolgen.

In Satz 2 ist darüberhinausgehend eine zusätzliche Befugnis vorgesehen, die es dem Bundesnachrichtendienst – als „Annex“ zur Aufgabe der Informationsbeschaffung – ermöglicht, in einem begrenztem Umfang auch gefahrenabwehrrechtlich tätig zu werden, wobei insoweit alle denkbaren Veränderungen des Inhalts einer Sendung (einschließlich einer Manipulation der Adressdaten etc.) tatbestandlich umfasst ist. Neben der Veränderung von Kommunikationsinhalten ist insbesondere auch die technische Manipulation von Gegenständen, die Unbrauchbarmachung von Gerätschaften oder der Austausch von Stoffen umfasst.

Der Befugnis liegen die folgenden Erwägungen zu Grunde: Aufgrund des Tätigkeitsschwerpunktes des Bundesnachrichtendienstes im Ausland kann er im Rahmen seiner aufklärenden Aufgabenerfüllung auf Gefahren aufmerksam werden, die auf das Inland gerichtet sind und für deren Abwehr keine andere Sicherheitsbehörde zuständig ist. Es handelt sich hierbei – dies folgt schon aus dem Aufklärungsbereich des Bundesnachrichtendienstes und ist infolge der Kautelen der maßgebenden Gesetzgebungskompetenz des Artikel 73 Absatz 1 Nummer 1 des Grundgesetzes auch notwendig – um solche Gefahren, welche unmittelbar auf das Verhältnis der Bundesrepublik zu anderen Völkerrechtssubjekten ausstrahlen können, sei es, weil die Gefahr durch eine fremde Macht (mit-)verursacht wurde oder sei es, weil ihre Verwirklichung (oder Abwehr) das diplomatische Verhältnis der Bundesrepublik zum Ausgangsstaat beeinträchtigen würde. In diesen Fällen, dies gebieten bereits die grundrechtlichen Schutzpflichten, kann der Staat nicht tatenlos zusehen, wie sich die Gefahr zu einer Störung verwirklicht.

Es bleibt sichergestellt, dass die Zuständigkeit des Bundesnachrichtendienstes nicht mit der allgemeinen Kompetenzordnung des Grundgesetzes, nach der die Gefahrenabwehr in der Zuständigkeit der Länder liegt, kollidiert. Da eine Zuständigkeit der Gefahrenabwehrbehörden (sowohl des Bundes als auch der Länder) bereits aufgrund der fehlenden hoheitlichen Gewalt im Ausland nicht in Betracht kommt, muss der Bundesnachrichtendienst in diesen selektiven Fällen ausnahmsweise die Gefahrenabwehr übernehmen. Falls und soweit eine entsprechende Befugnis im Inland ausgeübt werden soll (bzw. insgesamt zur Wahrung der grundgesetzlichen Kompetenzordnung und Zuständigkeit der Länder für die Gefahrenabwehr) ist normativ sichergestellt, dass ein Handeln des Bundesnachrichtendienstes insoweit nur subsidiär zu etwaigen Befugnissen anderer Behörden in Frage kommt. Hierbei sind sowohl die tatsächlichen als auch die rechtlichen Umstände umfangreich zu berücksichtigen; insbesondere die Tatsache, dass der Bundesnachrichtendienst über Fähigkeiten verfügt, welche andere Behörden nicht aufweisen, und dass er Informationen hat, die er mit anderen Behörden nicht teilen darf (Third Party Rule) sind zu berücksichtigen.

Auch steht das informationelle Trennungsprinzip der Einräumung der hier geregelten, besonderen Einwirkungsbefugnis nicht entgegen. Die besonderen Erhebungsbefugnisse des Bundesnachrichtendienstes – welche bereits zur Bedrohungsfrüherkennung zulässig sind; somit anders als die Erhebungsbefugnisse von Polizeibehörden, die in der Regel eine zumindest konkretisierte Gefahrenlagen voraussetzen – sind verfassungsrechtlich deshalb gerechtfertigt, weil der Bundesnachrichtendienst selbst nicht über „operative Anschlussbefugnisse“ verfügt (vgl. BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 302 sowie BVerfG, Beschluss vom 10. November 2020, 1 BvR 3214/15, Rn. 120). Begrenzt bleiben muss folglich die Verwendung von personenbezogenen Daten, welche mit besonderen, nachrichtendienstlichen Befugnissen erhoben wurden. Demgegenüber entfalten die besonderen Einschränkungen bei der Datenverwendung („informationelles Trennungsprinzip“) keine Wirkung, wenn gar keine Verwendung von Daten in Rede steht. In diesen Fällen, in denen die Maßnahme ihren Anlass nicht im „Anschluss“ an Datenerhebungen, sondern in sich selbst („causa-sui“) findet, steht die verfassungsgerichtliche Rechtsprechung zum informationellen Trennungsprinzip einer eigenen „Einwirkungsbefugnis“ des Bundesnachrichtendienstes nicht entgegen.

Die hier genannten besonders gewichtigen Rechtsgüter rekurrieren einerseits auf die in § 2 genannten Rechtsgüter. Die dortige, nicht abschließende Auflistung, wird insoweit durch die in § 4 Absatz 1 und 2 des Außenwirtschaftsgesetz genannten Rechtsgüter ergänzt.

In der in Absatz 2 enthaltenen Befugnis handelt es sich um eine solche „causa-sui“ Befugnis: Nicht die vorherige Erhebung von personenbezogenen Daten bietet ihren Anlass. Vielmehr handelt es sich um Konstellationen, in denen während der aufklärenden Tätigkeit des Bundesnachrichtendienstes in Folge eines Cyberangriffs gleichsam „zufällig“ Opferdaten oder Angriffswerkzeuge gefunden werden. In diesen Fällen ist es geboten, dass der Bundesnachrichtendienst die gefundenen Daten löschen kann – auch, um die staatlichen Schutzpflichten zu erfüllen.

Zu Nummer 1

Voraussetzung ist zunächst eine unmittelbar bevorstehende Gefahr für ein besonders gewichtiges Rechtsgut. Durch die tatbestandliche Verengung auf eine „unmittelbar bevorstehende“ Gefahr (im Vergleich zur „konkreten Gefahr“) wird bereits der Ausnahmecharakter der Vorschrift deutlich. Der Begriff entstammt dem allgemeinen Polizeirecht und schließt alle Sachverhalte ein, bei denen ein akuter Schadenseintritt mit sehr hoher Wahrscheinlichkeit zu erwarten. Dabei bleibt zugleich das – allgemeine nachrichtendienstliche – prognostische Element der „tatsächlichen Anhaltspunkte“ maßgebend. Entscheidend ist also, ob der Bundesnachrichtendienst aufgrund tatsächlicher Anhaltspunkte der Einschätzung ist, dass ein akuter Schaden für ein besonders gewichtiges Rechtsgut mit sehr hoher Wahrscheinlichkeit zu erwarten ist.

Zu Nummer 2

In Nummer 2 findet sich die – schon aus kompetenziellen Gründen – erforderliche Subsidiarität gegenüber sonstigen Behörden. Dies schließt einerseits diejenigen Fälle ein, bei denen der Bundesnachrichtendienst im Ausland tätig wird bzw. seine Maßnahmen im Ausland ihre Wirkung entfalten und eine Zuständigkeit einer anderen Behörde schon aus diesem Umstand nicht in Betracht kommt. Darüber hinaus sind aber auch Fälle denkbar, in denen der Bundesnachrichtendienst im Inland handelt und wirkt, bei denen eine Maßnahme einer inländischen Gefahrenabwehrbehörde aber gleichwohl nicht in Betracht kommt. Dies kann aufgrund tatsächlicher Umstände (z.B., weil die zugrundeliegenden Informationen von ausländischen Partnerdiensten geliefert wurden und nicht weitergabefähig sind oder weil der entstehende Zeitverzug der Wirksamkeit der Gefahrenabwehr entgegenstehen würde) oder aufgrund rechtlicher Umstände (z.B., weil inländische Behörden über keine entsprechenden Befugnisse verfügen) der Fall sein. Entscheidend ist zudem, ob die Maßnahme der inländischen Behörde in gleichem Maße geeignet wäre, ob sie also ebenso wirksam die Gefahr abwehren würde. Von der Subsidiarität ausgenommen bleiben andere Nachrichtedienste, also die Verfassungsschutzämter und das Bundesamt für den Militärischen Abschirmdienst.

Zu Nummer 3

In Nummer 3 ist – klarstellend und da die Vorgaben des § 6 hier nicht greifen, da es sich nicht um eine Datenerhebungsbefugnis handelt – ein besonderes Verhältnismäßigkeitsgebot der hier in Rede stehenden Maßnahmen statuiert.

Zu Absatz 4

Durch die in Absatz 4 enthaltenen Verweise auf die Kennzeichnungs-, Prüf- und Löschsowie Protokollierungspflichten der (besonderen) technischen Aufklärungsmaßnahmen von Kommunikationsdaten mit qualifiziertem Inlandsbezug wird sichergestellt, dass diese Vorgaben – wie bislang auch im Artikel 10-Gesetz vorgesehen – auch künftig für die Daten von Deutschen/Inländern gelten.

Zu § 29 (Wohnraumüberwachung)

Die technische Datenerhebung aus Wohnungen (nunmehr in der Überschrift bereits mit dem in der Praxis gängigen Begriff der „Wohnraumüberwachung“ beschrieben) weist ein besonderes Eingriffsgewicht auf. Der hiermit einhergehende Eingriff in die Unverletzlichkeit der Wohnung stellt eine so belastende Maßnahme für Betroffene dar, dass bereits unmittelbar in Artikel 13 des Grundgesetzes verfassungsrechtlich gebotene Einschränkungen und Voraussetzungen für entsprechende Maßnahmen getroffen werden.

Mit der Neuregelung folgen zwei maßgebliche Anpassungen der Befugnis. Zum einen unterfällt auch die Überwachung von im Bundesgebiet liegenden Wohnungen sowie von Wohnungen von deutschen Staatsangehörigen im Ausland künftig der Kontrolle des Unabhängigen Kontrollrates. Zum anderen ist eine Wohnraumüberwachung gegenüber Ausländern im Ausland künftig explizit – in Absatz 1 – geregelt und sieht eigene Eingriffsschwellen vor, welche im Vergleich zu Maßnahmen gegenüber Deutschen und Inländern abgesenkt sind.

Mit der in Absatz 1 geregelten Wohnraumüberwachung von Ausländern im Ausland ist über die obigen Ausführungen hinaus noch eine weitere Lösung von der strengen Geltung von Artikel 13 Absatz 4 des Grundgesetzes verbunden. Entsprechend der verfassungsgerichtlichen Rechtsprechung, wonach „sich die aus den Grundrechten konkret folgenden Schutzwirkungen danach unterscheiden können, unter welchen Umständen sie zur Anwendung kommen“ und sich folglich der Schutz einzelner Grundreche im In- und Ausland unterscheiden kann (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Leitsatz 1 und Rn. 104), ist insoweit eine Unterscheidung zwischen Maßnahmen der Wohnraumüberwachung gegenüber Deutschen und Inländern auf der einen und Ausländern im Ausland auf der anderen

Seite geboten. Leitend ist insoweit die Erwägung, dass Ausländerinnen und Ausländer im Ausland nicht in der gleichen Weise der (deutschen) staatlichen Hoheitsgewalt ausgesetzt ist. Insoweit sind, da bereits der Schutzgehalt des Artikel 13 Absatz 4 des Grundgesetzes für diese Betroffenen nicht im gleichen Umfang Geltung entfaltet wie für Deutsche und sich im Bundesgebiet aufhaltende Personen, zugleich auch die verfahrenssichernden Vorgaben einzuschränken. Anderenfalls würde der – vom Verfassungsgericht explizit zugestandene – Unterschied des Schutzgehaltes schon dadurch durchbrochen, dass die verfassungsrechtlichen Vorgaben faktisch auf einen Gleichlauf der Regelungen für wertungsmäßig unterschiedliche Sachverhalte hinauslaufen würde.

Zur Reichweite der Wohnraumüberwachung ist klarstellend und in Abgrenzung zur technischen Aufklärung zu beachten: Werden Signale aus der Wohnung ausgesteuert, liegt keine Wohnungsüberwachung darin, diese auf dem Übertragungsweg aufzufangen, etwa ein aus einer Wohnung geführtes Telefonat. Wird die Ausleitung aus der Wohnung dagegen vom Bundesnachrichtendienst gesteuert, kann dies im Einzelfall eine technische Wohnungsüberwachung sein, etwa wenn ein manipuliertes Mobiltelefon vom Bundesnachrichtendienst in vorheriger (oder nachträglich eintretender) Kenntnis der räumlichen Verortung zur akustischen Überwachung von in der Wohnung geführten Gesprächen aktiviert wird.

Die Regelung passt zudem auch im Einzelnen den bisherigen § 5 i.V.m. § 9 Absatz 2 des Bundesverfassungsschutzgesetzes an die Vorgaben der Verfassungsrechtsprechung an (hierzu nachfolgend im Einzelnen).

Zu Absatz 1

Der Absatz regelt die materiellen Voraussetzungen bei einem Tätigwerden des Bundesnachrichtendienstes gegenüber Ausländerinnen und Ausländern im Ausland. Die Ausgestaltung der gesetzlichen Befugnis in Absatz 1 trägt dem Umstand Rechnung, dass die nachrichtendienstliche Maßnahme gegenüber einer Ausländerin oder einem Ausländer im Ausland ein geringeres Eingriffsgewicht aufweist. Diese Personengruppe unterliegt typischerweise nicht dem Zugriff deutscher Behörden und ist damit in deutlich verringertem Ausmaß Folgemaßnahmen ausgesetzt, vgl. BVerfG vom 19. Mai 2020, 1 BvR 2835/17 (154, 152), Rn. 186. Entsprechend ist die Eingriffsschwelle hier gegenüber der Schwelle der „dringenden Gefahr“ (Absatz 2) geringfügig, auf die zweite Qualifikationsstufe herabgesetzt.

Zu Absatz 2

In Absatz 2 übernimmt Nummer 1 die in Artikel 13 Absatz 4 des Grundgesetzes vorgegebene Einsatzschwelle der dringenden Gefahr. Künftig ist folglich nicht mehr vorausgesetzt, dass die Gefahr bereits gegenwärtig ist. Die Nummern 2 und 3 rekurrieren auf die sehr hohe Einsatzschwelle des bisherigen § 5 i.V.m. § 9 Absatz 2 Sätze 1 und 2 Bundesverfassungsschutzgesetz. Da sowohl akustische wie auch optische Überwachung zulässig sind, dies unter denselben Voraussetzungen, ist eine getrennte Regelung überflüssig. Da es sich um die Maßnahme des höchsten Eingriffsgewichts handelt, ist sie im Inland gegenüber anderen Maßnahmen subsidiär, was Nummer 2 klarstellt. Nummer 4 schützt den Kernbereich privater Lebensgestaltung (BVerfG vom 26. April 2022, 1 BvR 1619/17, Rn. 280), wobei in Entsprechung der verfassungsgerichtlichen Rechtsprechung zugleich klar gemacht wird, dass einer Maßnahme nicht entgegensteht, wenn nur eine „Erfassung am Rande“ zu erwarten ist (vgl. zu § 21 Absatz 3).

Zu Absatz 3

Die Begrenzung der Maßnahmenrichtung in Absatz 3 folgt ebenso der Verfassungsrechtsprechung (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 211).

Zu Absatz 4

Absatz 4 dient insbesondere der besonderen Gewährleistung des Schutzes des Kernbereichs privater Lebensgestaltung auf der Auswertungsebene, da eine solche Maßnahme besonders tief in den Rückzugsraum des Betroffenen eindringt (vgl. BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 279, 282). Zuständig für die Vorabsichtung ist der Unabhängige Kontrollrat. Der Unabhängige Kontrollrat nimmt auch die weitere Kontrolle der besonderen Datenweiterverarbeitungsregelungen, etwa im Hinblick auf die besondere Zweckbindung nach Absatz 6, wahr.

Zu Absatz 5

Absatz 5 trifft eine besondere Ausnahmeregelung von der Vorabkontrolle nach Absatz 4 bei Gefahr im Verzug.

Zu Absatz 6 und Absatz 7

Absätze 6 bis 7 treffen unabhängig von den Regelungen in § 56 Ergänzungsregelungen zur organisatorischen Sicherung der materiellen Weiterverarbeitungsmaßgaben. Insbesondere ist die Kennzeichnung der erhobenen Daten erforderlich, um sicherzustellen, dass die – für die Wohnraumüberwachung aus verfassungsrechtlichen Gründen stark eingeschränkten – Weiterverarbeitungsmöglichkeiten gewahrt bleiben.

Zu Unterabschnitt 3 (Besondere Befugnisse der technischen Aufklärung)

Auch bei den Mitteln der technischen Aufklärung nach diesem Unterabschnitt – also der strategischen Aufklärung, der Telekommunikationsüberwachung und dem Zugriff auf informationstechnische Systeme – handelt es sich, der generellen Systematik des Gesetzes folgend, um nachrichtendienstliche Mittel, auf die die in Unterabschnitt 1 getroffenen allgemeinen Vorgaben grundsätzlich Anwendung finden. Dabei werden letztere indes durch eine Reihe von Spezialregelungen in den jeweiligen Erhebungsvorschriften verdrängt, welche den Besonderheiten der technischen Aufklärung Rechnung tragen.

Die technische Aufklärung durch den Bundesnachrichtendienst wird dabei auch deshalb in einem gesonderten Unterabschnitt geregelt, um den Besonderheiten dieser Erhebungsart und zugleich dem hohen Stellenwert der hierdurch erhobenen Daten für die Auslandsaufklärung Rechnung zu tragen. Mit der Neufassung der Vorschriften und der Gesetzessystematik erfolgt eine moderate, grundrechtskonforme Erweiterung der technischen Aufklärungsbefugnisse des Bundesnachrichtendienstes.

Dabei ermächtigen die in diesem Unterabschnitt enthaltenen Befugnisse den Bundesnachrichtendienst zur Erhebung von personenbezogenen Daten. Diese unterscheiden sich in der hier vorgenommenen, abgestuften Systematik grundsätzlich in vier verschiedene Datenarten: 1. Kommunikationsbezogene Inhaltsdaten, 2. kommunikationsbezogene Metadaten (die oftmals auch als „Verkehrsdaten“ bezeichneten Begleitumstände der Kommunikation), 3. personenbezogene Daten, welche einem Kommunikationsvorgang und damit dem Schutzbereich des Artikel 10 des Grundgesetzes unterfallen, aber nicht Teil einer interpersonellen Kommunikation zwischen zwei oder mehr Personen sind, und 4. „sonstige“ personenbezogene Daten, deren Schutz sich (ausschließlich) nach dem Recht auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrecht richtet.

Bei den zuerst genannten drei Datenkategorien handelt es sich um solche, die dem besonderen Schutz(bereich) des Artikel 10 Absatz 1 des Grundgesetzes unterfallen (vgl. BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Rn. 88). Insoweit besteht ein inneres Stufenverhältnis zwischen diesen drei Datenkategorien, in dem eine Erhebung und Auswertung von Inhaltsdaten den schwersten Grundrechtseingriff in das Fernmeldegeheimnis darstellt. Bei den Verkehrsdaten, also den Umständen der Kommunikation im weiteren Sinne, die im BND-Gesetz als „Metadaten“ auch solche Kommunikationsumstände betreffen, die

für die Kommunikation nicht „erforderlich“ sind, handelt es sich um die „mittlere“ Datenkategorie. Auch diese Daten sind in einem hohen Maßen schützenswert, da sie – abhängig von ihrer Erhebungsdichte und den jeweiligen Einzelumständen – weitreichende Einblicke in die Lebensführung einer Person zulassen können. Zuletzt sind solche personenbezogenen Daten, welche nicht Gegenstand einer unmittelbaren interpersonellen Kommunikation sind – in der Terminologie des Bundesverfassungsgerichts: „andere mithilfe von Telekommunikationstechniken über Distanz transportierte Daten“, vgl. BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Rn. 91 – ebenfalls durch Artikel 10 Absatz 1 des Grundgesetzes geschützt, da sich die „grundrechtstypische Gefährdungslage“ auch bei diesen Daten manifestiert. Hierunter fallen etwa diejenigen personenbezogenen Daten, die beim „Surfen im Internet“, beim Abrufen von Mails, beim Hoch- und Herunterladen von Daten über das Internet (Up- und Downloads) und insbesondere bei einem Datenaustausch mit Dienst-leistungen, die über das Internet zur Verfügung gestellt werden, automatisch abgesetzte Lokalisationsdaten eingeschalteter Mobiltelefone oder im Rahmen des Datenstroms im Zuge automatischer Daten-Synchronisierungen oder Daten-Backups, anfallen (BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, a.a.O.).

Bei den „sonstigen“ Daten der vierten Datenkategorie handelt es sich demgegenüber um solche Daten, die zwar dem Schutz des allgemeinen Persönlichkeitsrechts (in seiner Ausprägung als Recht auf informationelle Selbstbestimmung ggf. in Verbindung mit dem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme) unterfallen, nicht aber dem Fernmeldegeheimnis (vgl. hierzu näher: BVerfG, Beschluss vom 21. Juni 2016, 2 BvR 637/09, Rn. 30ff., BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 180/23, Rn. 228ff.). Solche Daten werden im Rahmen der Befugnisse der technischen Aufklärung primär durch Zugriff auf informationstechnische Systeme erhoben. Insoweit ist mit Blick auf die Betroffenheit der o.g. Grundrechte dahingehend zu unterscheiden, ob eine Datenerhebung vom Gewährleistungsgehalt des IT-System-Grundrechts erfasst wird. Dies richtet sich primär danach, um was für ein IT-System es sich handelt, etwa ob es „als eigenes genutzt wird“ (BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 180/23, Rn. 230). Liegt ein Eingriff in das IT-System-Grundrecht vor, so tritt der gleichermaßen erfolgte Eingriff in das Grundrecht auf informationelle Selbstbestimmung dahinter zurück.

Aufgrund den von der strategischen Aufklärung ausgehenden Eingriffen in das Fernmeldegeheimnis – zu der Intensität der Eingriffe nachfolgend näher – bedürfen dabei Eingriffe in Inhaltsdaten, in Metadaten aber auch in andere mithilfe von Telekommunikationstechniken über Distanz transportierte personenbezogene Daten einer spezialgesetzlichen Ermächtigungsgrundlage. Lediglich soweit es sich bei den aufzuklärenden Daten um bloße „Sachdaten“ handelt, also solche ohne einen Personenbezug (zum Beispiel militärische Funkverkehre ausländischer öffentlicher Stellen), liegt in ihrer Erhebung selbst regelmäßig bereits kein Grundrechtseingriff, sodass diese Erhebungen keiner Ermächtigungsgrundlage bedürfen (vgl. Graulich in GSZ 2021, 121).

Die technische Aufklärung (insbesondere durch die Möglichkeit der strategischen Aufklärung) ist für den Bundesnachrichtendienst zentrales Alleinstellungsmerkmal im Vergleich zu den anderen beiden Nachrichtendiensten des Bundes. Der Bundesnachrichtendienst kann und muss durch technische Aufklärungsmaßnahmen ohne Zeitverzug auf neue Krisen und Bedrohungslagen reagieren. Auch kann er durch Telekommunikationsüberwachungen und Zugriffe auf informationstechnische Systeme gezielt hochwertige Informationen erlangen, die für die Sicherheit der Bundesrepublik Deutschland von unverzichtbarem Wert sind. Diese Aufklärungsfähigkeiten sind insbesondere vor dem Hintergrund der sich verschärfenden Sicherheitslage essentiell. Einerseits, um Veränderungen dieser Sicherheitslage erkennen zu können, aber auch, um die eigenen Fähigkeiten zu stärken und damit die nationale Souveränität in Sicherheitsfragen zu gewährleisten. Weiter dient die Stärkung der Aufklärungsfähigkeiten dazu, dass der Bundesnachrichtendienst weiterhin und verstärkt als attraktiver internationaler Kooperationspartner wahrgenommen wird. Da die aktuellen Bedrohungen der Sicherheit der Bundesrepublik Deutschland nur im Europäischen Raum und mit anderen Partnerstaaten gemeinsam bewältigt werden können, ist auch dieser Aspekt

unter Berücksichtigung der Anschlussfähigkeit an diese Partner von überragend wichtiger Bedeutung. Zuletzt gebietet auch die Rolle des Bundesnachrichtendienstes als militärischer Auslandsnachrichtendienst eine Stärkung der Aufklärungsfähigkeiten insbesondere im Bereich der technischen Aufklärung. Die Bundeswehr erfüllt eine bedeutende Rolle bei der Erstellung der Sicherheitslage des Nordatlantikbündnisses; der Bundesnachrichtendienst wiederum trägt durch Übermittlung nachrichtendienstlicher Einschätzungen maßgeblich zur Lagebilderstellung innerhalb des Nordatlantikbündnisses bei.

Durch das Ablösegesetz wird im Rahmen der Befugnisse zur technischen Aufklärung durch den Bundesnachrichtendienst die Auflösung des Artikel 10-Gesetzes für den Bundesnachrichtendienst durch Übertragung der dort enthaltenen Erhebungsbefugnisse in das BND-Gesetz umgesetzt. Auch durch die vielfältigen unmittelbar daraus entstehenden Änderungen, die darüber hinaus auch rechtsförmliche Korrekturen, systematische Vereinfachungen und Wortlautanpassungen zur Steigerung der Verständlichkeit umfassen, ist eine vollständige Neusystematisierung der Vorschriften für die technische Aufklärung durch den Bundesnachrichtendienst erforderlich und erfolgt.

Dies betrifft insbesondere den Bereich der „strategischen Aufklärung“ (vormals strategische Fernmeldeaufklärung). Die Neufassung der Gesetzessystematik der strategischen Aufklärung wird nachfolgend überblicksartig dargestellt. Dabei wird insbesondere auf die Ziele der neuen Systematik, auf ihre Erforderlichkeit und Folgen sowie auf wesentliche verfassungsrechtliche Aspekte eingegangen.

Die neue Systematik verfolgt eine Reihe von Zielen: Zunächst sollen die technischen Aufklärungsfähigkeiten gestärkt und ein ganzheitlicher Ansatz für die Erhebung von personenbezogenen Daten im Rahmen der technischen Aufklärung geschaffen werden. Das bedeutet, dass die mit technischen Mitteln erhobenen Daten grundsätzlich (und soweit wie möglich) in vergleichbarer Art und Weise behandelt werden, insbesondere, dass die Erhebung von personenbezogenen Daten nicht länger zwischen einem spezifischen „Inlands-Regime“ (dem Artikel 10-Gesetz) und einem „Auslands-Regime“ unterscheidet, sondern die Datenerhebung zunächst einheitlich geregelt wird und die erforderlichen erhöhten Schutzvorgaben von „Inlands-Daten“ (also den Daten von deutschen Staatsangehörigen, sich im Bundesgebiet aufhaltenden Personen und inländischen juristischen Personen) im Rahmen der anschließenden inhaltlichen Verarbeitung dieser Daten umgesetzt werden. Außerdem wird im Rahmen der strategischen Aufklärung klargestellt, dass die Erhebungsbefugnis auch solche personenbezogenen Daten umfasst, die zwar im Rahmen der Telekommunikation übermittelt werden und dem Schutz des Fernmeldegeheimnisses aus Artikel 10 Absatz 1 des Grundgesetzes unterfallen, bei denen es sich indes nicht um Inhalts- oder Metadaten aus interpersoneller Kommunikation (vgl. die Begriffsbestimmung) handelt. Damit setzt das Gesetz auch die jüngste Rechtsprechung des Bundesverfassungsgerichts um (BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19 und BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 180/23).

Die nunmehr angelegte (Aus-)Differenzierung des Vorgangs der Datenerhebung im Wege der strategischen Aufklärung in zwei getrennte Stufen (unter Berücksichtigung der jeweiligen Eingriffsqualität dieser Eingriffe) ist ein weiteres Ziel der systematischen Neufassung. Im Rahmen der ersten Stufe, der „Datenerhebung im engeren Sinne“ greift der Bundesnachrichtendienst im Rahmen der strategischen Aufklärung auf Datenströme in Telekommunikationsnetzen zu (hiermit ist in technischer Hinsicht auch eine notwendige erste Speicherung der Daten verbunden; soweit das Verfassungsgericht in der Erfassung und Speicherung zwei Grundrechtseingriffe sieht, werden diese beiden Eingriffe also gemeinsam geregelt, da eine technische Trennung nicht möglich und eine rechtliche Trennung damit sinnlos wäre, vgl. BVerfG, Urteil vom 14. Juli 1999, 1 BvR 2226/94 u.a., Rn. 187f.).

Eine nachrichtendienstliche Auswertung der erhobenen Daten durch Mitarbeiterinnen und Mitarbeiter des Bundesnachrichtendienstes ist zu diesem Zeitpunkt noch nicht eröffnet. Erst die zweite Stufe, die „Einsichtnahme“, ermöglicht es, die erhobenen Daten einer finalen,

inhaltlichen Auswertung zugänglich zu machen. Diese Unterscheidung in zwei separate Eingriffstatbestände ist notwendig, um den besonderen Aufgaben und Befugnissen des Bundesnachrichtendienstes zu entsprechen: Die Einzigartigkeit in der Arbeit des Bundesnachrichtendienstes – insbesondere was die ihm vorbehaltene „strategische Aufklärung“ anbelangt – soll nunmehr, dies ist ein weiteres Ziel der neuen Systematik, normenklar auf rechtlicher Ebene umgesetzt werden.

Dem Bundesnachrichtendienst ist es im Rahmen seiner strategischen Aufklärung möglich, eine Vielzahl von (auch personenbezogenen) Daten zu erheben, ohne dabei auf eine individualisierende Überwachung einzelner Anschlüsse – wie sie etwa mit einer Telekommunikationsüberwachung intendiert wird – Rückgriff zu nehmen. Der Bundesnachrichtendienst kann vielmehr Datenströme, deren Ergiebigkeit im Einzelnen nicht vorhersehbar ist, erfassen und so „ungezielt“ personenbezogene Daten erheben, ohne die hohen Voraussetzungen, die für eine individualisierende Telekommunikationsüberwachung maßgeblich sind, anlegen zu müssen. Dies ist dem Umstand geschuldet, dass eine „strategische“ Aufklärung notwendigerweise (primär) final angeleitet ist (vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 157) und eine etwaige Wertigkeit der erhobenen Daten zum Zeitpunkt der Erhebung der Daten im engeren Sinne noch nicht bewertet werden kann. Vielmehr ist für die „strategische“ Zielrichtung der Maßnahme gerade immanent, dass der Bundesnachrichtendienst zunächst keinerlei Kenntnis davon haben kann, ob die Daten für seine Auftragserfüllung ergiebig, d.h. von nachrichtendienstlichem Wert sind. Diese Prüfung der erhobenen Daten auf ihre nachrichtendienstliche Wertigkeit folgt denknotwendigerweise nachgelagert, da eine inhaltliche Prüfung zwingend eine vorherige Erhebung voraussetzt.

Gegenüber der bisherigen Gesetzessystematik, welche die Erhebung und Einsichtnahme von personenbezogenen Daten durch die strategische Aufklärung einheitlich regelt, ist mit der nunmehr getroffenen Unterscheidung auf Erhebungsseite zwischen der Erhebung im engeren Sinne und der vorübergehenden „Erstspeicherung“ (erste Stufe) und der „Einsichtnahme“ im Sinne einer initialen Auswertung und Prüfung auf Relevanz der erhobenen Daten (zweite Stufe) mit dem Ziel, sie für die abschließende Analyse durch Mitarbeiterinnen und Mitarbeiter des Bundesnachrichtendienstes, die mit der inhaltliche Auswertung im engeren Sinne betraut sind, verfügbar zu machen, eine klare rechtliche Abgrenzung dieser beiden Schritte verbunden. Dabei war diese Unterscheidung in faktischer Hinsicht auch bislang geboten: Der bisherige § 19 erlaubt dem Bundesnachrichtendienst die „Verarbeitung“ von personenbezogenen Daten, was bislang neben der Erhebung auch alle weiteren Verwendungen der Daten beinhaltet. Dabei werden im Rahmen dieser Erhebung die personenbezogenen Daten zwar mittels Suchbegriffen auf Grundlage einer strategischen Aufklärungsmaßnahme gefiltert, indes – auch wenn keine Suchbegriffe einschlägig sind – im Rahmen des bisherigen § 24 dem Bundesnachrichtendienst für die in der (bisherigen) „Eignungsprüfung“ enthaltenen Zwecke zur Verfügung gestellt. Tatsächlich setzen bislang jedoch sowohl die Möglichkeit einer Filterung durch eine strategische Aufklärungsmaßnahme als auch (und insbesondere) die Eignungsprüfung voraus, dass der Bundesnachrichtendienst zuvor einen technischen Zugang auf die personenbezogenen Daten erlangt. Dieser Schritt wird nunmehr klar geregelt und mit der Befugnis verbunden, die so erhobenen Inhaltsdaten für einen Zeitraum von höchstens sechs Monaten zu speichern und sorgt damit für Rechtssicherheit und Rechtsklarheit. Durch diese Speicherung und die sich anschließende Befugnis die in dem vorgegebenen Zeitraum gespeicherten Kommunikationsdaten z.B. daraufhin zu filtern, ob in ihnen ein Suchbegriff enthalten ist, wird es dem Bundesnachrichtendienst ermöglicht, schneller auf Krisen reagieren zu können. Findet der Bundesnachrichtendienst im Rahmen der Eignungsprüfung relevante Suchbegriffe, kann er diese unverzüglich mit dem Datenbestand abgleichen und relevante Verkehre nutzen. Bislang konnte der Suchbegriff (nur) für zukünftige Datenerhebungen genutzt werden, wobei es bei der Übertragung immer vom Zufall abhängt, auf welchen Leitungen die Verkehre übertragen werden, d.h. ob auch zukünftig relevante Verkehre mit dem erkannten Suchbegriff auf den überwachten Strecken übertragen werden, kann nicht vorausgesagt werden.

Es handelt sich bei der Erhebung und vorübergehenden Speicherung im Sinne der Regelungen nach § 31 ff. von (auch) Inhaltsdaten dabei auch dann, wenn hierdurch noch nicht die inhaltliche Auswertung der Daten ermöglicht wird, um einen Grundrechtseingriff (regelmäßig in das Fernmeldegeheimnis), vgl. BVerfG, Urteil vom 2. März 2010, 1 BvR 256/08 u.a., Rn. 190. Die Erhebung im engeren Sinne verkörpert dabei den (zunächst notwendigen) ersten Schritt der strategischen Aufklärung, welcher die Daten dem Bundesnachrichtendienst zwar in technischer Hinsicht zugänglich macht, aber noch keine „Nutzung“ (im obigen, weiten Sinne einer Verarbeitung) ermöglicht (vgl. hierzu auch BVerfG, Urteil vom 14. Juli 1999, 1 BvR 2226/94 u.a., Rn. 231). Der von der Erhebung im engeren Sinne und der hierauf folgenden Zwischenspeicherung ausgehende Grundrechtseingriff ist dabei von beträchtlicher, aber gleichwohl geringerer Intensität als der Eingriff, welcher von einer anschließenden Weiterverarbeitung ausgeht. Dies ist den folgenden Gründen geschuldet:

Durch die strategische Aufklärung wird – auch unter Berücksichtigung der gesetzlichen Grenzen und kapazitätsbedingten Einschränkungen – eine große Menge von Daten erhoben. Der Umstand, dass insoweit auch Daten erhoben werden, die für die Auftragserledigung durch den Bundesnachrichtendienst keinen relevanten Informationsgehalt haben, „ändert nichts daran, dass die gesamthafte Erfassung und Auswertung von Datenströmen im Ergebnis zu bedeutsamen Erkenntnissen führen kann“ (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 144). Da der konkrete Datenstrom im Vorfeld nicht inhaltlich begrenzt werden kann, werden dabei auch eine große Vielzahl solcher Daten miterhoben, die bereits aufgrund ihrer Natur keinerlei Relevanz für die Auftragserfüllung des Bundesnachrichtendienstes haben. Hierzu zählen beispielhaft die großen Datenmengen, die durch das Streamen von Medien über das Internet fließen. Auch hierin sind personenbezogene Daten enthalten, sodass (auch wenn es sich bei diesen regelmäßig nicht um Kommunikationsinhalte oder Metadaten handelt) eine Grundrechtsbetroffenheit gegeben ist und ein Eingriff in Artikel 10 Absatz 1 des Grundgesetzes vorliegt (vgl. BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Rn. 88ff.). Da ein Großteil der Daten nur aufgrund technischer Notwendigkeiten miterhoben wurde und die Daten unmittelbar nach ihrer Erhebung wieder verworfen werden, da sie unter keinem Gesichtspunkt für die nachrichtendienstliche Auslandsaufklärung von Interesse sein können (dergestalt bereits an der gesetzlichen Zielrichtung der strategischen Aufklärung vorbei gehen) und deswegen keiner manuellen oder automatisierten Auswertung ihrer Inhalte (geschweige denn eine Übermittlung mit anschließenden operativen Folgen) erfolgen wird, liegt regelmäßig bereits kein Grundrechtseingriff vor, da in diesem Fall die Daten zwar miterfasst, aber „unmittelbar nach der Signalaufbereitung technische wieder spurenlos ausgesondert werden“ (Vgl. BVerfG, Urteil vom 14. Juli 1999, 1 BvR 2226/94 u.a., Rn. 187.)

Auch soweit personenbezogene Daten, welche dem Schutzbereich des Grundrechts aus Artikel 10 Absatz 1 des Grundgesetzes unterfallen, tatsächlich erhoben (und nicht unmittelbar wieder gelöscht) werden, ist die Intensität, die mit dem Eingriff auf Ebene der Erhebung erfolgt, deutlich niedriger als durch den rechtlich wie tatsächlich nachfolgenden Prozess der Einsichtnahme in die erhobenen Daten. Die personenbezogenen Daten können nämlich vom Bundesnachrichtendienst nur dann eingesehen werden, wenn die insoweit maßgeblichen Schwellen erreicht sind. Sie können zuvor weder einem Bearbeiter zur inhaltlichen Auswertung vorgelegt werden, noch können sie im Rahmen von Analysen und Lagebildern des Bundesnachrichtendienstes verwendet werden, noch können sie regelmäßig an andere Stellen übermittelt werden (eine Ausnahme hiervon bilden lediglich die Bundeswehr, der der Bundesnachrichtendienst in Folge seiner Funktion als militärischer Auslandsnachrichtendienst in begrenztem Umfang Daten schon vor Einsichtnahme übertragen darf, sowie Übermittlungen im Rahmen von Kooperationen oder von gemeinsamen Dateien mit Innenbehörden oder ausländischen Partnern, die jedoch ihrerseits spezialgesetzlich an besondere Voraussetzungen geknüpft sind). Dabei sorgen die rechtlichen Voraussetzungen der Einsichtnahme dafür, dass nachrichtendienstlich unergiebige Daten (zuvorderst die bloß aus technischen Gründen miterfassten Daten von Nichtbetroffenen) nicht in die Weiterverarbeitung gelangen, wenn sie nicht die materiellen Schwellen der jeweiligen Einsichtnahmebefugnis erreichen, und nach Ablauf der Speicherfrist gelöscht werden. Erst recht bedarf

es sodann für eine etwaige Übermittlung der Daten an andere Stellen der Einhaltung zusätzlicher materiellrechtlicher und verfahrenssichernder Voraussetzungen.

Das Bundesverfassungsgericht hat in der „strategischen Kommunikationsüberwachung“ zwar einen Eingriff von „besonders schweren Gewicht“ gesehen (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 146). Diese Wertung folgte indes daraus, dass in der vom Bundesverfassungsgericht geprüften Form der strategischen Fernmeldeaufklärung keine rechtliche Unterscheidung vom Vorgang der Erhebung und dem der anschließenden Einsichtnahme angelegt war. Entsprechend sind vier der fünf vom Bundesverfassungsgericht genannten Faktoren, welche das Eingriffsgewicht der strategischen Fernmeldeaufklärung zu einem „besonders schweren“ erhöhten, für die hier (allein) maßgebliche Ebene der Datenerhebung nicht einschlägig, da sie unmittelbar auf die Verarbeitung Bezug nehmen (vgl.: Verweis auf Folgemaßnahmen, Rn. 149; Verweis auf Auswertung und Analyse, Rn. 150f., Verweis auf gezielte Erfassung durch Suchbegriffe, Rn. 152, Verweis auf anlasslose Auswertung gespeicherter Verkehrsdaten, Rn. 153). Diese eingriffsintensivierenden Faktoren finden für das Eingriffsgewicht der nunmehr gesondert geregelten „ersten Stufe“ (Datenerhebung) insoweit nicht länger Berücksichtigung.

Allerdings liegt in der heimlichen Überwachung der Telekommunikation bereits grundsätzlich ein „schwerer Eingriff“, „unabhängig davon, ob die Überwachung im Inland oder im Ausland stattfindet oder sich auf Inländer und Deutsche oder Ausländer bezieht“ (vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 147). Dieser grundsätzlichen Gleichbehandlung der Daten von deutschen Staatsangehörigen, Inländern und ausländischen Staatsangehörigen im Ausland – auf Eingriffsebene – wird mit der neuen Systematik nunmehr entsprochen. Dies führt indes nicht dazu, dass die besondere Schutzbedürftigkeit der personenbezogenen Daten der genannten Personen unberücksichtigt bliebe. Vielmehr wird sie auf Ebene der Einsichtnahme durch gesonderte, höhere Voraussetzungen für die Verarbeitung sowie verfahrenssichernde Vorgaben umfassend umgesetzt.

Eingriffserschwerend kommt auf der ersten Stufe der strategischen Aufklärung hinzu, dass das Gesetz nunmehr die Einsichtnahme nicht als einen mit der Erhebung verknüpften Vorgang ansieht, sondern sie – in einem begrenzten zeitlichen Rahmen – auch zu einem späteren Zeitpunkt gestattet: Die vorgesehene Systematik erlaubt es dem Bundesnachrichtendienst nämlich künftig, die zweite Stufe der strategischen Aufklärung – das heißt die Einsichtnahme in die erhobenen personenbezogenen Daten – erst zu einem späteren Zeitpunkt durchzuführen. Dem Bundesnachrichtendienst wird hierfür die Möglichkeit eröffnet, die im Rahmen der strategischen Aufklärung erhobenen Inhaltsdaten für einen eng begrenzten Zeitraum von sechs Monaten zu speichern (vgl. § 66 Absatz 1). Dabei ist zwar eine Zwischenspeicherung von Verkehrsdaten auch im bisherigen § 26 Absatz 5 bereits angelegt; was im Rahmen der Weiterverarbeitungsvorschriften übernommen wird. Demgegenüber ist dem Bundesnachrichtendienst nunmehr aber eröffnet, auch Inhaltsdaten aus der strategischen Aufklärung nicht unmittelbar nach Erhebung auszuwerten, sondern die Einsichtnahme anhand von Suchbegriffen zu einem späteren Zeitpunkt (innerhalb der Speicherfrist) zu vollziehen.

Die hierdurch geschaffene Möglichkeit zur zeitlich eng begrenzten Speicherung (auch) von Inhaltsdaten, die gegenwärtig nur im Bereich der Eignungsprüfung vorgesehen ist, ist aus einer Reihe von Gründen für die Aufgabenerfüllung durch den Bundesnachrichtendienst dringend erforderlich:

Wesensmerkmal der strategischen Aufklärung ist, dass der Bundesnachrichtendienst bei Erhebung der Daten zunächst keine genaue Kenntnis von der Ergiebigkeit der erhobenen Daten hat. Lediglich anhand der Strecken kann eine Einordnung der möglichen Herkunftsländer der Verkehre getroffen werden. Zugleich ist ihm durch die Eignungsprüfung u.a. die Möglichkeit eröffnet, nachrichtendienstlich relevante – das heißt faktisch für den Schutz besonders gewichtiger Rechtsgüter vor Bedrohungen erforderliche – Suchbegriffe im Wege der Eignungsprüfung zu generieren. Diese Suchbegriffe können (de lege lata) indes

lediglich für die zukünftige Erhebung von personenbezogenen Daten genutzt werden, wobei eine zukünftige Erfassung oder Ergiebigkeit keineswegs sicher ist. Die Kommunikationsinhalte, welche die nachrichtendienstliche Relevanz einzelner Suchbegriffe stützen, müssen demgegenüber verworfen werden und stehen dem Bundesnachrichtendienst nicht länger zur Verfügung. Dies ist insbesondere bei kurzfristig eingetretenen Krisen und bei bereits erfolgten Beeinträchtigungen von Rechtsgütern nicht hinzunehmen. Dem Bundesnachrichtendienst liegen in diesem Fall relevante Verkehre vor, die wichtige Erkenntnisse bringen. Er muss diese jedoch verwerfen, da kein Suchbegriff enthalten ist, der zum Zeitpunkt der Erhebung in den Steuerungssystemen des Bundesnachrichtendienstes enthalten war. Die bereits feststehende Relevanz für den Schutz besonders gewichtiger Rechtsgüter vor Bedrohungen bleibt insoweit folgenlos und der Bundesnachrichtendienst ist darauf verwiesen, darauf zu hoffen, dass die Suchbegriffe auch künftig einschlägig sind, nachrichtendienstlich relevante Inhalte transportieren und in der – meist infolge des nicht vorhersehbaren Routings bei paketvermittelten Verkehren zufälligen – Erfassung auch erhoben werden können. Bei Ereignissen, die in der Vergangenheit liegen (wie z.B. erfolgte Anschläge) ist damit einer Erhebung faktisch ausgeschlossen.

Die begrenzten Möglichkeiten des Bundesnachrichtendienstes, seinen gesetzlichen Aufgaben zum Schutz besonders gewichtiger Rechtsgüter vor Bedrohungen mittels der strategischen Aufklärung nachzukommen, erfordert daher dringend eine Ausweitung der zugänglichen Datenbasis. Diese Begrenzungen sind unmittelbare Folge u.a. der faktisch limitierten Erfassungsmöglichkeiten (abermals und zuvorderst bedingt durch die leitungsunabhängige Paketvermittlung von Daten, bei der die Route einer Übertragung nicht vorhersehbar ist) und der begrenzten Zugangsmöglichkeiten auf Telekommunikationsnetze. Der Bundesnachrichtendienst vermag aufgrund dieser Umstände faktisch nur einen sehr geringen Teil der Kommunikation zu erfassen bzw. aus diesem Teil personenbezogene Daten zu erheben. Diesen Begrenzungen lässt sich zumindest insoweit begegnen, als der Bundesnachrichtendienst die erhobenen Daten in (schon aufgrund technischer Limitationen) sehr begrenztem Umfang zumindest kurzfristig speichern darf und nicht gezwungen ist, potentiell relevante Daten sofort zu verwerfen. Um das Eingriffsgewicht zu kompensieren, wird demgegenüber dem bisherigen Recht nunmehr die „Streckenauswahl“ mit eigenen tatbestandlichen Voraussetzungen unterleg (vgl. hierzu nachfolgend und § 31 Absatz 3).

Weiter vermag der Bundesnachrichtendienst derzeit solche Daten, die keine personenbezogenen Daten enthalten (Sachdaten), nur sehr eingeschränkt zu erfassen, da er dies bereits bei Erhebung erkennen und entsprechend filtern muss, was technisch mit großen Schwierigkeiten verbunden ist. Zudem wird dem Bundesnachrichtendienst so die Möglichkeit gegeben, die nötige Informationsbasis von Sachdaten zu schaffen.

Die nunmehr vorgesehene Möglichkeit einer kurzfristigen Speicherung von erhobenen Daten (abermals: ohne dass damit schon eine Einsichtnahme in die personenbezogenen Daten und ein damit verbundener schwerwiegender Grundrechtseingriff einhergeht) entspricht den gesetzlichen Befugnissen ausländischer europäischer Partnerdienste. So sieht etwa der *Investigatory Powers Act 2016* des Vereinigten Königreichs eine Speicherung von Inhaltsdaten ohne zwingende zeitliche Begrenzung vor, solange die Daten erforderlich sind (vgl. Section 150 des *Investigatory Powers Act 2016*: *„there are no longer any relevant grounds for retaining a copy of any material if, and only if its retention is not necessary, or not likely to become necessary…“*). Dabei folgt das britische Recht einer vergleichbaren Teilung zwischen Erhebung von Daten (zu der auch der Prozess einer Filterung und Indexierung gezählt wird) und der Einsichtnahme (die sog. „examination“, vgl. Section 152 des *Investigatory Powers Act 2016).* Eine Speicherung von erhobenen Daten ist dabei nicht an gesetzliche Höchsfristen geknüpft, sondern folgt einem Prinzip der „Notwendigkeit“ für bestimmte gesetzlich festgelegte Zwecke. Hierbei ist neben der rechtlichen Zulässigkeit (im Sinne einer Notwendigkeit für die gesetzlich bestimmten Zwecke, z.B. der nationalen Sicherheit) primär auch die physisch-technische (Un-)Möglichkeit der langfristigen Speicherung von gigantischen Datenmengen leitend.

Weiter noch reichen die Möglichkeiten des französischen Rechts, welches ebenfalls einer zweistufigen Systematik folgt. Nach dem *Code de la sécurité intérieure* ist grundsätzlich zulässig, dass Daten, die im Rahmen der „ersten Stufe“ erhoben wurden – Inhalts- wie Metadaten – für bis zu vier Jahre ohne inhaltliche Auswertung gespeichert werden können. Artikel L. 854-2 Absatz 1 des *Code de la sécurité intérieure* regelt zunächst die Erhebung aus „Netzwerken“ (*réseaux*), die dergestalt Ziel der Erhebungen sind. Ein tatsächlicher Zugriff auf die relevanten Daten ist sodann erst möglich, wenn auf einer zweiten Stufe eine Autorisierung der Auswertung (*exploitation*) erfolgt ist. Die Zweistufigkeit zeigt sich im französischen Recht bei der Behandlung von Inlandsdaten (welche der nunmehr angelegten Systematik ähnelt): Eine Erfassung im Rahmen der strategischen Aufklärung ist hier grundsätzlich möglich; eine Filterung erfolgt primär auf der „zweiten Stufe“ der *exploitation,* Artikel L. 854-1 des *Code de la sécurité intérieure*.

Der im vorliegenden Gesetz gewählte, mehrstufige Aufbau entspricht ferner der Rechtslage des niederländischen Rechts („Wet op de inlichtingen- en veiligheidsdiensten 2017“ - WiV). In diesem wird der „Allgemeine Nachrichten- und Sicherheitsdienst“ – der in der Struktur der niederländischen Sicherheitsbehörden auch die Funktion des Auslandsnachrichtendienstes einnimmt – nach Artikel 48 Absatz 5 WiV befugt, die im Wege von Maßnahmen der strategischen Aufklärung erhobenen Daten für einen Zeitraum von bis zu drei Jahren zu speichern, bevor sie technisch (Artikel 49 WiV) oder inhaltlich (Artikel 50 WiV) ausgewertet werden (müssen). Für Daten, welche verschlüsselt oder aus anderen Gründen in nicht lesbarer Form (z.B. aufgrund neuer oder unbekannter technischer Übertragungsprotokolle) erhoben wurden, besteht die Möglichkeit, die Daten zunächst für einen (verlängerbaren) Zeitraum von drei Jahren zu speichern – nach Entschlüsselung bzw. Lesbarmachung beginnt sodann die „reguläre“ Dreijahresfrist der Auswertung zu laufen. Eine Löschung der Daten hat nach Ende der dreijährigen Frist zu erfolgen oder wenn im Rahmen der Auswertung erkennbar wird, dass die Daten keine nachrichtendienstliche Relevanz haben.

Um – dem Koalitionsvertrag entsprechend – dafür Sorge zu tragen, dass die Leistungsfähigkeit des Bundesnachrichtendienstes mit europäischen Partnerdiensten wieder Schritt hält, ist der Bundesnachrichtendienst gleichermaßen entsprechend zu befähigen. Dabei ist der für die Zwischenspeicherung vorgesehene Zeitraum indes nach wie vor erheblich kürzer als in den o.g. Rechtsordnungen.

Die Speicherung perpetuiert dabei den durch die Erhebung der Daten ausgehenden Eingriff und intensiviert ihn. Zugleich bleibt sie aber in ihrer Reichweite aus mehreren Gesichtspunkten begrenzt, was sich gleichermaßen auf die Intensität des von ihr ausgehenden Eingriff auswirkt:

Zunächst und zuvorderst handelt es sich bei der vorübergehenden Speicherung der im Wege der strategischen Aufklärung erhobenen Daten nicht um eine „Vorratsdatenspeicherung“ im Sinne der Richtlinie 2006/24/EG oder der §§ 175ff. des Telekommunikationsgesetzes. Die Vorratsdatenspeicherung verpflichtet die Anbieter von öffentlich zugänglichen Telekommunikationsnetzen für Endnutzer, praktisch alle Telekommunikationsverkehrsdaten zu speichern und diese unter bestimmten Voraussetzungen den Gefahrenabwehr- oder Strafverfolgungsbehörden zur Verfügung zu stellen. Hieraus folgt, dass „über den gesamten Zeitraum von sechs Monaten praktisch sämtliche Telekommunikationsverkehrsdaten aller Bürger ohne Anknüpfung an ein zurechenbar vorwerfbares Verhalten, eine - auch nur abstrakte - Gefährlichkeit oder sonst eine qualifizierte Situation“ erfasst werden, wobei „grundsätzlich alle Telekommunikationsverbindungen so [erfasst werden sollen], dass die Nutzer möglichst flächendeckend ermittelt werden können (BVerfG, Urteil vom 2. März 2010, 1 BvR 256/08 u.a., Rn. 210).

Diese außerordentliche, nahezu grenzenlose Streubreite ist im Rahmen der strategischen Aufklärung weder rechtlich zulässig noch faktisch möglich: In rechtlicher Hinsicht folgt dies bereits daraus, dass eine strategische Aufklärung von rein-inländischen Verkehren – die

Daten „aller Bürger“ – nur im Rahmen von eng begrenzten Ausnahmen zulässig ist. Reine Inlands-Kommunikation ist bereits bei der Erhebung auszufiltern und kann nicht gespeichert werden, wenn nicht eine der Ausnahmetatbestände vorliegt. Die strategische Aufklärung hat insoweit schon durch die Streckenauswahl einen eindeutigen Fokus auf die Erfassung von (mindestens auch) ausländischer Telekommunikation. Zudem ist die Unterscheidung von einer Vorratsdatenspeicherung auch darin angelegt, dass die strategische Aufklärung – insoweit über die Anforderungen des Bundesverfassungsgerichtes, das auch eine „anlasslose“ strategische Aufklärung ohne objektivierte Eingriffsschwellen für zulässig erklärt hat (vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 178) hinausgehend – eine materielle Eingriffsschwelle voraussetzt und grundsätzlich nur möglich ist, wenn sie zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist, also der Früherkennung von Bedrohungen gegen besonders gewichtige Rechtsgüter dient. Dies führt unmittelbar zu einer rechtlichen Begrenzung der Speicherung, da es bei der strategischen Aufklärung gerade nicht um die unterschiedslose Erfassung der Telekommunikationsverbindungen aller Bürger geht, sondern um die Speicherung von Erhebungen aus Telekommunikationsnetzen, welche der Früherkennung von Bedrohungen gegen besonders gewichtige Rechtsgüter dient. Um dies rechtlich zu verankern, ist nunmehr gesetzlich explizit vorgesehen, dass eine Erhebung nur aus solchen Strecken zulässig ist, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass die Verkehre enthalten, die für die nachrichtendienstliche Auslandsaufklärung von Bedeutung sind. Dies führt dazu, dass der Bundesnachrichtendienst gerade nicht „nur final angeleitet“ nachgerade „wahllos“ Daten erheben kann, sondern durch sorgfältige Streckenauswahl sicherstellen muss, dass es sich um eine anlassbezogene Erhebung handelt. Auch in faktischer Hinsicht ist die im Gesetz vorgesehene Möglichkeit einer begrenzten Speicherung nicht mit dem Instrument der Vorratsdatenspeicherung vergleichbar, da der Umfang der strategischen Aufklärung durch den Bundesnachrichtendienst nicht einmal in Ansätzen an die Speicherung aller Verkehrsdaten auf Providerebene heranreicht und auch nicht heranreichen soll, da der Bundesnachrichtendienst weder Interesse an den personenbezogenen Daten von Unbeteiligten hat noch diese auswerten könnte.

Darüber hinaus ist zu berücksichtigen, dass – anders als im Rahmen der Vorratsdatenspeicherung – auch kein unmittelbarer Zugriff operativer Behörden auf die gespeicherten Daten erfolgen kann und so „das Risiko von Bürgern erheblich [steigen würde], weiteren Ermittlungen ausgesetzt zu werden, ohne selbst Anlass dazu gegeben zu haben“ (vgl. BVerfG, Urteil vom 2. März 2010, 1 BvR 256/08 u.a., Rn. 212). Vielmehr ist selbst ein Zugriff von Mitarbeitenden des Bundesnachrichtendienstes auf die gespeicherten Daten zunächst auf die Einsichtnahme begrenzt, diese unterliegt, wie die gesamte technische Aufklärung des Bundesnachrichtendienstes der Kontrolle durch den Unabhängigen Kontrollrat. Demgegenüber ist eine Kontrolle der Datenverarbeitungsprozesse im Rahmen einer Vorratsdatenspeicherung bei Providern (jedenfalls behördlich und unabhängig) nicht vorhanden. Wenn im Rahmen einer strategischen Aufklärungsmaßnahme in die personenbezogenen Daten Einsicht genommen wird, sind sie auf ihre nachrichtendienstliche Relevanz zu prüfen.

Weiter agiert der Bundesnachrichtendienst unter besonders strengen Geheimhaltungsvorschriften und -bedingungen. Entsprechend sind auch die gespeicherten Daten in besonderem Maße vor „interessierten Dritten“ (vgl. BVerfG, Urteil vom 2. März 2010, 1 BvR 256/08 u.a., Rn. 212) geschützt, sodass ein Missbrauch der Daten durch maliziöse Akteure faktisch ausgeschlossen werden kann.

Zusammenfassend handelt es sich auch bei der Erhebung und Speicherung von personenbezogenen Daten im Wege der strategischen Aufklärung bereits um einen Grundrechtseingriff in Artikel 10 Absatz 1 des Grundgesetzes, der einer verfassungsrechtlichen Rechtfertigung bedarf. Diese ist in dem überragenden öffentlichen Interesse an einer wirksamen Inland-Ausland-Aufklärung (BVerfG, Urteil vom 8. Oktober 2024, 1 BvR 1743/16 u.a., Rn. 161) und Auslandsaufklärung (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17) zu sehen. Um eine wirksame Früherkennung von Bedrohungen gegen die in § 2 Absatz 1 genannten besonders gewichtigen Rechtsgüter zu ermöglichen, ist das Instrument der strategischen

Aufklärung für den Bundesnachrichtendienst von unverzichtbarer Bedeutung. Denn die „Erweiterung und Internationalisierung der Kommunikationsmöglichkeiten und die damit gesteigerte Politisierung und Organisationsfähigkeit international agierender staatlicher und nichtstaatlicher Gruppierungen führen dazu, dass innerstaatliche Gefahrenlagen oftmals durch Netzwerke international zusammenarbeitender Akteure begründet sind“ (vgl. BVerfG, Urteil vom 8. Oktober 2024, 1 BvR 1743/16 u.a., Rn. 161). Für die strategische Ausland-Ausland-Aufklärung tritt hinzu, dass die „Versorgung der Bundesregierung mit Informationen für ihre außen- und sicherheitspolitischen Entscheidungen [ihr hilft], sich im machtpolitischen Kräftefeld der internationalen Beziehungen zu behaupten, und (…) folgenreiche Fehlentscheidungen verhindern [kann]. Insoweit geht es mittelbar zugleich um die Bewahrung demokratischer Selbstbestimmung und den Schutz der verfassungsrechtlichen Ordnung – und damit um Verfassungsgüter von hohem Rang. In Frage steht mithin ein gesamtstaatliches Interesse, das über das Interesse an der Gewährleistung der inneren Sicherheit als solcher deutlich hinausgeht“ (vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 162). Da sich die Bedrohungslage innerhalb der letzten Jahre aufgrund der geopolitischen Entwicklungen drastisch verändert hat, ist auch das öffentliche Interesse an einer wirksamen Aufklärung dieser Bedrohungen sprunghaft angestiegen. Entsprechend ist der Bundesnachrichtendienst weiter zu befähigen, diese Bedrohungen wirksam aufzuklären. Dabei ist es zugleich von großer Bedeutung, dass der Bundesnachrichtendienst mit den Fähigkeiten seiner europäischen Partner Schritt halten kann (vgl. hierzu auch den Koalitionsvertrag, „Verantwortung für Deutschland“, Rn. 2653) da die nachrichtendienstliche Zusammenarbeit von einem Erkenntnisaustausch beider Seiten in gegenseitigem Interesse geprägt ist. Dabei ist zwar – insbesondere was die Speicherfrist erhobener Daten anbelangt – aufgrund der verfassungsgerichtlichen Rahmensetzung keine umfassende „Parität“ zu den nachrichtendienstlichen Befugnissen von Partnerdiensten umsetzbar. Zumindest aber schafft das Gesetz für den Bundesnachrichtendienst durch den hier beschriebenen Systemwechsel wenigstens dem Grunde nach vergleichbare Fähigkeiten im Bereich der strategischen Aufklärung.

Anschließend an die erste Stufe der Datenerhebung folgt die Möglichkeit der Einsichtnahme in die personenbezogenen Daten, ohne die eine nachrichtendienstliche Verwertung der Kommunikationsinhalte und Metadaten nicht erfolgen darf oder kann. Auf die bereits erhobenen Daten kann dabei nach ihrer Erhebung eine Einsichtnahme anhand von Suchbegriffen, eine Einsichtnahme in Metadaten oder ein eng zweckbegrenzter Zugriff zur Bestimmung neuer Suchbegriffe oder Netze (im Rahmen der Eignungsprüfung) erfolgen. Insoweit bildet die neue Systematik den Prozess der strategischen Aufklärung in rechtlicher Hinsicht vollständig und transparent ab: Auch wenn die Filterung (wie im geltenden Recht) unmittelbar im Anschluss an die Erhebung der Daten erfolgt, so folgt sie dieser doch in rechtlicher wie tatsächlicher Hinsicht nach, sodass eine Abgrenzung dieser beiden Schritte erforderlich ist.

Der von dieser (sich an die Erhebung und Speicherung anschließenden) Einsichtnahme in die erhobenen personenbezogenen Daten ausgehende Grundrechtseingriff wiegt schwerer als der von der Erhebung selbst ausgehende Eingriff. Nunmehr werden die erhobenen Daten dem Bundesnachrichtendienst dergestalt zugänglich gemacht, dass sie einer gezielten Kenntnisnahme durch Mitarbeiterinnen und Mitarbeiter ausgesetzt werden. Hieran schließen sich die etwaigen Folgen einer Weiterverarbeitung der personenbezogenen Daten an, die bis zu einer etwaigen Übermittlung der Daten an Behörden mit operativen Anschlussbefugnissen reichen. Dieser – schwerwiegendere – Eingriff – setzt eine ganze Reihe zusätzlicher materieller (d.h. gesteigerte materielle Voraussetzungen) oder formeller (etwa Prüf- und Löschfristen, etc.) voraus, um die Verhältnismäßigkeit zu wahren. Entsprechend ist ein solcher Eingriff nur dann zulässig, wenn er im Rahmen einer – mit hohen materiellen und formellen Schwellen versehenen – strategischen Aufklärungsmaßnahme oder im Rahmen der – nur für enge Zwecke zulässigen – Eignungsprüfung erfolgt.

Die gesetzlichen Regelungen greifen zudem die oben dargestellte Unterscheidung des jeweiligen Schutzgehaltes von personenbezogenen Daten, welche Artikel 10 Absatz 1 des

Grundgesetzes unterfallen, auf: Inhaltsdaten einer interpersonellen Kommunikation unterliegen dabei besonders engen Grenzen. Für Metadaten einer interpersonellen Kommunikation sind aufgrund der (etwas) abgestuften Schutzbedürftigkeit gesetzliche Erleichterungen (insbesondere die Möglichkeit der bevorratenden Speicherung) vorgesehen. Zuletzt unterfallen solche personenbezogenen Daten, welche dem Schutz des Fernmeldegeheimnisses unterfallen, indes nicht Inhalt (oder Umstand) einer interpersonellen Kommunikation waren, den allgemeinen Weiterverarbeitungsvorschriften. Sie sind insoweit anderen personenbezogenen Daten, welch der Bundesnachrichtendienst mit nachrichtendienstlichen Mitteln erhoben hat, gleichgestellt.

Für die Verarbeitung der interpersonellen Kommunikation von deutschen Staatsangehörigen, Inländern und inländischen juristischen Personen, die im Gesetz als Kommunikationsdaten mit qualifiziertem Inlandsbezug bezeichnet werden, gelten dabei besondere Vorgaben. Dies ist dem Umstand geschuldet, dass diese Daten – vornehmlich aufgrund der Nähe der Betroffenen zur staatlichen Hoheitsgewalt – in besonderem Maße schützenswert sind (vgl. zu dem unterschiedlichen Schutzgehalt der Grundrechte: BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 104). Dieser Schutzbedürftigkeit entspricht das Gesetz mit dem Gebot einer Filterung der entsprechenden Daten auf technischem Wege unmittelbar nach Erhebung, besonderen materiellen Voraussetzungen für die Einsichtnahme in diese Daten sowie den besonderen Verfahrensvorgaben bezüglich der Prüfung, Löschung, Protokollierung, Mitteilung und Kontrolle.

Mit erfasst von den in diesem Unterabschnitt enthaltenen Befugnisse sind, wenn diesbezüglich keine spezialgesetzlichen Regelungen vorgesehen sind, der technischen Aufklärung vorgelagerte Maßnahmen zum Beispiel zur Erschließung von Zugängen zu Telekommunikationsnetzen.

Darüber hinaus werden in diesem Unterabschnitt auch die Befugnisse zum Zugriff auf informationstechnische Systeme angepasst. Insbesondere differenziert das bisherige Recht (§ 34) nicht zwischen den unterschiedlichen Eingriffsqualitäten, die mit einem solchen Zugriff verbunden sein können. In der Neufassung der Befugnisnormen für die sogenannte „Computer Network Exploitation“ (CNE) wird nun vielmehr ein differenziertes und gestuftes System vorgesehen, welches einerseits anhand der erhobenen Daten (Art und Umfang) sowie andererseits anhand des Eingriffsziels (in personeller wie sachlicher Hinsicht) unterscheidet und so die einschlägige Verfassungsrechtsprechung zur differenzierten Bewertung der Eingriffstiefen im diesem Bereich umsetzt (vgl. Beschluss vom 24. Juni 2025, 1 BvR 2466/19 „Trojaner I“ sowie Beschluss vom 24. Juni 2025, 1 BvR 180/23 „Trojaner II“. §§ 36ff. sehen für die unterschiedlichen Fallkonstellationen jeweils eingriffsadäquate Schwellen und Verfahrensvorgaben vor.

Ferner werden die bisherig auf die strategische Fernmeldeaufklärung begrenzten besonderen Vorgaben für Kooperationen im Sinne dieses Gesetzes modernisiert, rechtssystematisch vereinfacht, normenklarer gefasst und – durch Erstreckung auf die Telekommunikationsüberwachung und den Zugriff auf informationstechnische Systeme – erweitert.

Zu § 30 (Begriffsbestimmungen der technischen Aufklärung)

Zu Nummer 1

Die Eignungsprüfung ist – dem geltenden Recht entsprechend, vgl. § 24 Absatz 1 des bisherigen Gesetzes – die Bestimmung geeigneter Suchbegriffe oder Telekommunikationsnetze im Rahmen von strategischen Aufklärungsmaßnahmen. Dass die Eignungsprüfung bezogen auf Telekommunikationsnetze nicht mit der einmaligen Feststellung der Relevanz endet, sondern eine periodische Prüfung angezeigt ist, ist durch eine begriffliche Änderung abgebildet.

Zu Nummer 2

Der Begriff der „Einsichtnahme“ wird neu im Gesetz aufgenommen. Dieser Begriff kennzeichnet die nunmehr (erstmals) differenziert geregelte „zweite Stufe“ der strategischen Aufklärung und trägt dem (oben im Einzelnen erläuterten) Umstand Rechnung, dass das Eingriffsgewicht, welches von der technischen Erhebung (im engeren Sinne) ungefilterter Daten, deren Ergiebigkeit noch nicht absehbar ist, sich fundamental von dem inhaltlichen Zugriff durch Mitarbeiterinnen und Mitarbeiter oder entsprechende technische Systeme des Bundesnachrichtendienstes unterscheidet, welcher durch die Einsichtnahme – die gleichermaßen Bestandteil der Datenerhebung im weiteren Sinne darstellt – ermöglicht wird. Abzustellen ist auf den Zeitpunkt der Erzeugung einer „Meldung“, da diese den oben genannten Zugriff zum Zwecke der inhaltlichen Auswertung ermöglicht.

Zu Nummer 3

Der bereits im bisherigen Gesetz enthaltene Begriff der „Inhaltsdaten“ (nunmehr: kommunikationsbezogene Inhaltsdaten) beschreibt diejenigen Kommunikationsdaten, welche – in Abgrenzung zu den „kommunikationsbezogenen Metadaten“ (vgl. Nummer 5) – den konkreten Kommunikationsinhalt zwischen zwei Personen ausmachen. Hierin eingeschlossen sind alle gängigen Formen der Kommunikation (also in Wort, Schrift und Bild). Nicht erfasst sind hingegen personenbezogene Daten, die zwar im Rahmen der technischen Aufklärung erfasst werden, aber keinen interpersonellen Kommunikationsinhalt zum Gegenstand haben. Neben den bereits genannten „Metadaten“ sind dies insbesondere auch Daten, die nicht aus der (interpersonellen) Kommunikation entstammen, also „andere mithilfe von Telekommunikationstechniken über Distanz transportierte Daten“ (BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Rn. 91). Diese Daten unterfallen zwar gleichermaßen dem Fernmeldegeheimnis, welches die Übermittlung von potentiell persönlichkeitsrelevanten Daten auf Distanz erfasst und eine berechtigte Vertraulichkeitserwartung hinsichtlich der kommunizierten Inhalte und Umstände des Datentransports begründet, indes ist der Schutzgehalt im Vergleich zu den Inhalten und Umständen der interpersonellen Kommunikation zwischen zwei Personen herabgesetzt.

Zu Nummer 4

Der Begriff der „kommunikationsbezogenen Metadaten“ bezeichnet die auch „Verbindungsdaten“ genannten Umstände einer Kommunikation. Der Begriff ist insoweit weiter als der bislang übliche Begriff der „Verkehrsdaten“, da nicht nur solche Daten erfasst sind, die für die Kommunikation „erforderlich“ sind, sondern alle (nicht Inhalts-)Informationen, welche die Umstände von interpersonellen Kommunikationen ausmachen.

Nicht umfasst sind sonstige technische Metadaten, die nicht im Rahmen einer interpersonellen Kommunikation anfallen. Vgl. zu diesen „mithilfe von Telekommunikationstechniken über Distanz transportierte Daten“ (BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Rn. 91) bereits oben.

Zu Nummer 5

In Nummer 5 wird der Oberbegriff der personenbezogenen Kommunikationsdaten – für kommunikationsbezogene Inhalts- und Metadaten – bestimmt.

Zu Nummer 6

Der in Nummer 6 definierte „qualifizierte Inlandsbezug“ ist gegeben, wenn die erhobenen kommunikationsbezogenen Inhalts- und Metadaten aus einer in der Übertragung befindlichen interpersonellen Kommunikation, die zwischen (besonders geschützten) Personen mit einem besonderen persönlichen oder räumlichen Bezug zum deutschen Staat stehen, entstammen. Der besondere Schutz dieses qualifizierten Inlandsbezuges folgt letztlich aus eben dieser Nähe – zum einen, da ihre Kommunikation für den Bundesnachrichtendienst

aufgrund des Zugriffs auf inländische Provider faktisch leichter erfasst werden kann; zum anderen, da die belastenden Wirkungen, die sich infolge der Überwachung möglicherweise zeitigen, aufgrund des Zugriffs deutscher Staatsgewalt eher manifest werden können.

Die besonders geschützten Personen beinhalten dabei Deutsche (Buchstabe a), wobei solche Personen ausgenommen bleiben, die nach Maßgabe des § 6 Absatz 3 aufgrund ihrer hoheitlichen Tätigkeit für eine fremde Macht nicht gesondert schützenswert sind. Gleiches gilt im Falle von Inländern (Buchstabe c), wobei insoweit auch die in § 6 Absatz 4 geregelten „Nacheilefälle“ zu berücksichtigen sind. Weiter sind auch inländische juristische Personen vom besonderen Schutzgehalt erfasst, da auch sie sich auf das Grundrecht auf Artikel 10 des Grundgesetzes berufen können (Buchstabe b). Gleichwohl ist insoweit eine Ausnahme für solche juristischen Personen geboten, bei denen tatsächliche Anhaltspunkte dafür bestehen, dass sie von mit nachrichtendienstlichen Aufgaben betrauten ausländischen öffentlichen Stellen gesteuert werden und in deren Interesse tätig sind. Diese juristischen Personen unterfallen keiner besonderen Schutzbedürftigkeit. Die Regelung zielt dergestalt darauf ab, zu verhindern, dass ausländische Nachrichtendienste im Rahmen ihrer – teilweise auch gegen die Bundesrepublik Deutschland selbst gerichteten – Tätigkeit den Schutz der deutschen Grundrechtsverbürgungen ausnutzen, indem sie durch die Gründung einer (formell) inländischen juristischen Person ihre Tätigkeiten vor den Aufklärungsmöglichkeiten des Bundesnachrichtendienstes abschirmen.

Zu Nummer 7

In Nummer 7 ist der Begriff der „reinen Inlandskommunikation“ (erstmals) definiert. Dieser Begriff wird vom Bundesverfassungsgericht verwendet (z.B. BVerfG, Beschluss vom 8. Oktober 2024, 1 BvR 1743/16 u.a., Rn. 28ff.) und meint Fälle der interpersonellen Kommunikation, bei denen es sich sowohl bei Absender als auch bei Empfänger um einen Inländer/Deutschen handelt.

Zu Nummer 8

In Nummer 8 wird der Begriff der selektierten Kommunikationsdaten – welcher im Rahmen der Übermittlung von Daten im Rahmen von Kooperationen mit ausländischen Partnerdiensten von Relevanz ist – definiert. Der hierin enthaltene Begriff des „Selektors“ als Synonym von „Suchbegriffen“ entspricht insoweit auch den internationalen Gepflogenheiten.

Zu Nummer 9

Der Begriff der „strategischen Aufklärung“ wird erstmals definiert. In Abgrenzung zur (individualisierenden) Telekommunikationsüberwachung zielt die strategische Aufklärung nicht auf die Erfassung der gesamten Kommunikation einer bestimmten Person oder eines bestimmten Anschlusses ab. Insoweit geht die strategische Aufklärung regelmäßig damit einher, dass die „Ergiebigkeit“ der Datenerhebung für den Bundesnachrichtendienst im Vorfeld nicht ersichtlich und abschätzbar ist, da gerade eine unbestimmte Vielzahl von Kommunikationsvorgängen erfasst wird.

Die Terminologie wurde im Vergleich zum bisherigen Gesetz modernisiert. Dabei wurde der Begriff der „strategischen Fernmeldeaufklärung“ durch den der „strategischen Aufklärung“ ersetzt. Dies ist schon deshalb geboten, weil durch die strategische Aufklärung nicht nur personenbezogene Daten aus Kommunikationsbeziehungen im engeren Sinne (also Inhaltsdaten und Metadaten) erhoben werden können, sondern auch weitere personenbezogenen Daten, die dem Schutzbereich des Fernmeldegeheimnisses nach Artikel 10 Absatz 1 des Grundgesetzes unterfallen, also „andere mithilfe von Telekommunikationstechniken über Distanz transportierte Daten“.

Zu Nummer 10

Der bereits im geltenden Recht verwendete Begriff bezeichnet die individuellen (und beschränkten) Maßnahmen, welche einer Anordnung und Vorabkontrolle bedürfen, und die Durchführung der strategischen Aufklärung so anleiten und einrahmen.

Zu Nummer 11

Der Begriff des Telekommunikationsnetzes ist – insoweit dem § 3 Nummer 65 des Telekommunikationsgesetzes entsprechend – sehr weit. Insbesondere sind so auch Fälle lokaler Datenerhebung und Fälle mit vorgelagerten Maßnahmen wie Erzeugung des TK-Netzes (z.B. Datenerhebung mittels IMSI-Catcher) erfasst. Dabei meint die „Gesamtheit von Übertragungssystemen“ jeweils diejenigen Systeme, die in einem „Netz“ die Übertragung ermöglichen. Nicht gemeint ist, dass es gleichsam nur „ein Telekommunikationsnetz“ weltweit gäbe.

Zu Nummer 12

Die nunmehr enthaltene Definition des Begriffs der Telekommunikationsüberwachung regelt den Begriff in Abweichung zur Regelung des § 5 Absatz 1 der Telekommunikations-Überwachungsverordnung Die abweichende Definition ist in der Tatsache begründet, dass der Bundesnachrichtendienst als einzige deutsche Behörde eine normenklare Abgrenzung der klassischen Telekommunikationsüberwachung zur strategischen Aufklärung benötigt. Diese wird durch das Abstellen auf die gängige technische Umsetzung der Telekommunikationsüberwachung erreicht, welche regelmäßig auch mit einer gegenüber der strategischen Aufklärung deutlich erhöhten Erfassungswahrscheinlichkeit gegenüber der betroffenen Person verbunden ist.

Zu § 31 (Vorgaben für die strategische Aufklärung)

Bereits in der Erhebung und anschließenden Speicherung von personenbezogenen Daten im Wege der strategischen Aufklärung liegt ein Eingriff in die Grundrechte (konkret in das Recht auf informationelle Selbstbestimmung und/oder das Fernmeldegeheimnis). So werden hierdurch grundsätzlich drei mögliche Datenarten erhoben: Personenbezogene Daten, die im Rahmen eines interpersonellen Kommunikationsvorgangs erhoben werden (Kommunikationsdaten) und die sich wiederum in die Datenarten „Inhaltsdaten“ einerseits und „Metadaten“ (als Daten, welche die Umstände der Kommunikation betreffen) andererseits aufteilen lassen. Darüber hinaus können durch die strategische Aufklärung auch „sonstige“ personenbezogene Daten – unabhängig davon, ob diese in technischer Hinsicht als Inhalts- oder Metadaten zu betrachten wären, in der Diktion des Bundesverfassungsgerichts: „andere mithilfe von Telekommunikationstechniken über Distanz transportierte Daten“ (BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Rn. 91) – erhoben werden; also solche, die nicht im Rahmen eines interpersonellen Kommunikationsvorganges anfallen, aber gleichwohl schützenswert sind und dem Fernmeldegeheimnis unterfallen.

Für all diese Daten wird eine anschließende Verarbeitung durch die Erhebung und Speicherung faktisch überhaupt erst ermöglicht. Damit erfolgt die Erhebung relevanter personenbezogenen Daten letztlich mit dem Ziel, dass der Bundesnachrichtendienst die Daten – für Kommunikationsdaten nur bei Wahrung der gesondert geregelten Voraussetzungen – „nach inhaltlichen Kriterien auswerten kann – sei es auf der Grundlage von Suchbegriffen für Inhaltsdaten, sei es zur Auswertung von akkumulierten Verkehrsdaten oder sei es zur Übermittlung an ausländische öffentliche Stellen im Rahmen einer Kooperation“ (vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 115). Dieser bereits durch die Erhebung erfolgende Eingriff verlangt eine eigene Ermächtigungsgrundlage, die in § 32 Absatz 1 normiert ist.

Lediglich die Erhebung von reinen Sachdaten, das heißt Daten die keinen Personenbezug aufweisen, zum Beispiel die Erhebung militärischer Funkverkehre ausländischer Staaten,

ist insoweit grundrechtsneutral und bedarf keiner besonderen gesetzlichen Regelung (vgl. BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Rn. 91: in Abgrenzung zu den „potentiell persönlichkeitsrelevanten Daten auf Distanz“).

Der durch die Erhebung erfolgende Grundrechtseingriff ist dabei jedoch (noch) von begrenztem Gewicht (hierzu oben). Dem Bundesnachrichtendienst ist ein Zugriff auf die personenbezogenen Kommunikationsdaten (allein) durch die Erhebung nicht gestattet. Diese Daten werden vielmehr lediglich in die Systeme des Bundesnachrichtendienstes überführt und dort vorübergehend gespeichert.

Darüber hinaus bleibt die formalisierte Festlegung „jeweils begrenzter Überwachungsmaßnahmen“ (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 179ff.), die bereits im geltenden Recht angelegt ist, erhalten. Die strategische Aufklärung von Kommunikationsdaten darf nur im Rahmen der eng zweckbegrenzten Eignungsprüfung sowie einer zuvor angeordneten und vom Unabhängig Kontrollrat überprüften strategischen Aufklärungsmaßnahme erfolgen, welche die Aufklärung durch Angaben zum Aufklärungsthema, zur geografischen Region (wo immer möglich, vgl. in der Anordnungsvorschrift) und zur Dauer der Maßnahme begrenzt.

Zu Absatz 1

Absatz 1 enthält die grundsätzliche Vorgabe, dass die strategische Aufklärung nur im Rahmen von spezifischen Aufklärungsmaßnahmen (hierzu § 32) zulässig ist. Die Regelung stellt die für die verfassungsrechtlich gebotene Zielbegrenzung der strategischen Telekommunikationsaufklärung erforderliche formalisierte Festlegung jeweils begrenzter Überwachungsmaßnahmen sicher (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 179ff.). Entsprechend dem geltenden Recht ist eine Erhebung von personenbezogenen Daten im Rahmen der strategischen Aufklärung nicht grenzenlos möglich, sondern erfolgt im Rahmen von konkretisierten strategischen Aufklärungsmaßnahmen, welche die Ziele der Aufklärung nach objektiven Kriterien formalisieren und sie einer objektivrechtlichen Kontrolle zuführen. Diese Maßnahmen begrenzen (in Entsprechung des geltenden Rechts) einerseits die Erhebung von personenbezogenen Daten und die Einsichtnahme in diese sowie andererseits die für die Vorbereitung der Maßnahmen und Generierung von geeigneten Suchbegriffen essentielle Eignungsprüfung.

Für „andere mithilfe von Telekommunikationstechniken über Distanz transportierte Daten“ (BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Rn. 91), also solche, bei denen es sich weder um Inhalts- noch Metadaten handelt, ist eine Begrenzung der strategischen Aufklärung ebenfalls und schon deshalb vorgesehen, um ihrer Schutzbedürftigkeit (mit Blick auf das Fernmeldegeheimnis) Rechnung zu tragen.

Zu Absatz 2

In § 31 Absatz 2 Satz 1 ist – die oben beschriebene Systematik normativ und klarstellend verankernd – geregelt, dass aus den durch die strategische Aufklärung erhobenen personenbezogenen Kommunikationsdaten (d.h. Inhalts- und Metadaten) vom Bundesnachrichtendienst auf der „ersten Stufe“ personenbezogene Kommunikationsdaten zwar erhoben und vorübergehend zwischengespeichert werden dürfen, eine Weiterverarbeitung der Daten indes nur erfolgen darf, nachdem in diese Daten unter den ergänzenden Voraussetzungen der § 33 Absatz 2 und § 34 Absatz 2 Einsicht genommen wurden.

Die Weiterverarbeitung „sonstiger“, im Wege der strategischen Aufklärung erhobener Daten, also solche Daten bei denen es sich weder um kommunikationsbezogene Inhalts- noch Metadaten handelt und die aus diesem Grund zwar dem Schutzbereich des Artikel 10 Absatz 1 des Grundgesetzes unterfallen, indes in ihrer Schutzbedürftigkeit herabgesetzt sind, richtet sich nach den allgemeinen Weiterverarbeitungsvorschriften in Abschnitt 5.

Ausgenommen bleibt von diesem Grundsatz – begründet durch die besondere Funktion des Bundesnachrichtendienstes als militärischer Auslandsnachrichtendienst – lediglich die Möglichkeit einer Übermittlung der Daten an die Bundeswehr nach § 80 Absatz 2, in gemeinsame Dateien mit Innenbehörden, sowie an ausländische Nachrichtendienste und in gemeinsamen Dateien mit ausländischen Nachrichtendiensten im Rahmen von Kooperationen § 93 Absatz 4 sowie § 131 Absatz 5.

In Absatz 2 Satz 2 findet sich eine Ausnahme vom Verbot einer Weiterverarbeitung vor Einsichtnahme: Soll die Weiterverarbeitung lediglich eine spätere Einsichtnahme vorbereiten, etwa indem die Daten maschinell vorgefiltert oder systematisiert werden, so ist dies zulässig, solange diese Weiterverarbeitung ausschließlich zu dem genannten Zweck geschieht. Hierdurch soll sichergestellt werden, dass der Bundesnachrichtendienst nicht auf eine „rein händische“ Prüfung begrenzt bleibt, die faktisch nicht darstellbar und rechtlich – durch die enge Zweckbegrenzung – nicht geboten ist.

Zu Absatz 3

Die Regelung greift den bisherigen § 19 Absatz 8 auf und übernimmt die verfassungsgerichtliche Vorgabe, dass eine unbeschränkte strategische Aufklärung („globale und pauschale Überwachung“, BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 168) unzulässig ist. Im bisherigen Recht wurde diese Vorgabe (ergänzend) durch eine Beschränkung auf „30 Prozent der bestehenden Telekommunikationsnetze“ umgesetzt. Aufgrund der praktischen Schwierigkeiten, die mit einer solchen pauschalen Volumenbegrenzung einhergingen, verfolgt das Gesetz nunmehr zusätzlich auch einen anderen Ansatz und begrenzt die strategische Aufklärung dadurch, dass eine Erhebung nur aus solchen Telekommunikationsnetzen zulässig ist, bei denen tatsächliche Anhaltspunkte dafür bestehen, dass sie personenbezogene Daten enthalten, die für die nachrichtendienstliche Auslandsaufklärung in besonderem Maße erforderlich ist.

Hiermit verbunden ist eine Prüfpflicht für den Bundesnachrichtendienst, im Wege von Netzstrukturanalysen konkrete Telekommunikationsnetze – bzw. Bestandteile dieser Netze, wann immer dies möglich ist, z.B. einzelne Leitungen – daraufhin zu prüfen, ob sie aufgrund tatsächlicher Anhaltspunkte für die nachrichtendienstliche Aufklärung besonders wertig sind. Dabei kann sich die „Erforderlichkeit in besonderem Maße“ sowohl daraus ergeben, dass besonders relevante Einzelverkehre auf der Strecke vermutet werden oder, dass aufgrund objektiver Umstände davon auszugehen ist, dass potentiell vielzählige Verkehre erfasst werden können.

Zu Absatz 4

Die Regelung übernimmt den bisherigen § 19 Absatz 9.

Zu Absatz 5

Die Regelung schafft – insoweit klarstellend, da ein solcher Einsatz auch nach dem geltenden Recht bereits möglich, nicht aber ausdrücklich geregelt war – eine Befugnis für den Bundesnachrichtendienst zum gemeinsamen Betrieb technischer Mittel zur Durchführung der strategischen Aufklärung mit ausländischen Nachrichtendiensten, um eine effiziente Nutzung der jeweils vorhandenen Fähigkeiten und Kapazitäten zu ermöglichen. Eine arbeitsteilige Zusammenarbeit mit ausländischen Nachrichtendiensten ist im Bereich der strategischen Aufklärung angesichts vielfältiger Bedrohungen, zunehmender technischer Komplexität und Diversität und Telekommunikationsnetzen sowie knapper Ressourcen unabdingbar, da dem Bundesnachrichtendienst andernfalls ein Ausschluss aus den auch perspektivisch immer relevanter werdenden Zusammenarbeitsformen mit internationalen Partnern droht. Der gemeinsame Betrieb kann im Rahmen der jeweiligen Möglichkeiten und technischen Gegebenheiten arbeitsteilig an einem Standort oder an mehreren Standorten zur Erhebung räumlich dislozierter Telekommunikationsnetze erfolgen.

In Abgrenzung zu den im weiteren Verlauf geregelten „Kooperationen“ liegt die Besonderheit bei der Durchführung nach Absatz 5 darin, dass gerade keine Erhebung „nur“ durch den Bundesnachrichtendienst erfolgt und die Daten sodann weiterübermittelt werden. Vielmehr ist hier – jedenfalls in rechtlicher Hinsicht – bereits auf Ebene der Erhebung eine Zweiteilung zwischen dem Bundesnachrichtendienst und dem jeweiligen Partner (sei er aus- oder inländisch) angelegt und die Erhebung richtet sich nach dem jeweiligen Rechtsregime der erhebenden Stelle.

Falls die Erhebung auf dem Bundesgebiet stattfindet, stellt Satz 2 sicher, dass die Daten von Deutschen, Inländern und inländischen juristischen Personen nur vom Bundesnachrichtendienst erhoben werden können. Dies stellt sicher, dass der besondere Schutz dieser Personen vollumfassend gewahrt bleibt.

Zu Absatz 6

In Absatz 6 findet sich eine der sog. causa-sui (Annex-)Befugnisse, welche dem Bundesnachrichtendienst im Rahmen seiner aufklärenden Tätigkeit und Auftragserfüllung (ausnahmsweise) eine gefahrenabwehrrechtliche Kompetenz gewähren. Es wird ergänzend auf die Begründung zu § 28 Absatz 3 verwiesen.

Entsprechend der allgemeinen Systematik dieser Befugnisse ist es tatbestandlich erforderlich, dass tatsächliche Anhaltspunkte für eine unmittelbar bevorstehende Gefahr für ein besonders gewichtiges Rechtsgut erkannt werden und keine andere Behörde als der Bundesnachrichtendienst in der Lage ist, diese Gefahr gleich effektiv abzuwehren. Die konkreten zulässigen Maßnahmen finden sich in den Nummern 1 bis 3.

Zu § 32 (Erhebung von Daten im Rahmen von strategischen Aufklärungsmaßnahmen)

Die Erhebung (im weiteren Sinne, also einschließlich der Erhebung im engeren Sinne, der (vorübergehende) Speicherung und der Einsichtnahme (§§ 33, 34) von personenbezogenen Kommunikationsdaten im Wege der strategischen Aufklärung ist nur zulässig im Rahmen von strategischen Aufklärungsmaßnahmen, welche die strategische Aufklärung in ihrer Zielsetzung begrenzen und zugleich eine wirksame objektivrechtliche Kontrolle ermöglichen.

Zu Absatz 1

In Absatz 1 wird die eigentliche Befugnis für die Erhebung von personenbezogenen Daten durch Maßnahmen der strategischen Aufklärung geregelt.

Insoweit wird auch weiterhin an einer materiellen Eingriffsschwelle festgehalten, da eine Erhebung im Rahmen einer strategischen Aufklärungsmaßnahme nur zulässig ist, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist. Damit wird die Verhältnismäßigkeit, insoweit über die (verfassungsgerichtlich für zulässig erklärte) allein final angeleitete Befugnis ohne materielle Eingriffsschwellen hinausgehend (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 178), gewährleistet: Obwohl das Bundesverfassungsgericht eine Befugnis zur strategischen Aufklärung grundsätzlich auch „anlasslos“ (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, a.a.O.) für verhältnismäßig erklärt hat und insoweit durch das überragende öffentliche Interesse an einer wirksamen Auslandsaufklärung gerechtfertigt ansieht, trifft das BND-Gesetz (weiterhin) strengere Voraussetzungen und verlangt, dass die Erhebung zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist. Eine „globale und pauschale Überwachung“ (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 168) scheidet, neben der bereits in § 31 Absatz 3 enthaltenen Begrenzung, durch die Notwendigkeit der Erhebung für die nachrichtendienstliche Auslandsaufklärung (und den insoweit angelegten Bezug zu der Früherkennung von Bedrohungen gegen besonders gewichtige Rechtsgüter) bereits aus.

Hierdurch wird zudem sichergestellt, dass keine „uferlose“ Erfassung von solchen personenbezogenen Daten („andere mithilfe von Telekommunikationstechniken über Distanz transportierte Daten“, BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Rn. 91) erfolgt, welche dem Schutzbereich des Fernmeldegeheimnisses unterfallen, ohne Inhalts- oder Metadaten zu sein. Die Erhebung im engeren Sinne solcher Daten setzt gleichsam eine Begrenzung durch eine strategische Aufklärungsmaßnahme, welche der Vorabkontrolle durch den Unabhängigen Kontrollrat unterliegt, voraus. Indes richtet sich die Weiterverarbeitung dieser Daten, im Anschluss an ihre Erhebung nach den allgemeinen Weiterverarbeitungsvorschriften sowie den Kooperationsvorschriften.

Zu Absatz 2

Die Vorschrift übernimmt im Wesentlichen den bisherigen § 19 Absatz 6 und regelt, dass die Erhebung personenbezogener Daten durch die strategische Aufklärung auch in der Weise möglich ist, dass der Bundesnachrichtendienst sich mit technischen Mitteln Zugang zu einem Anbieter von Telekommunikationsdiensten oder digitalen Diensten verschafft, um die strategische Aufklärung durchzuführen.

Die Vorschrift ermächtigt den Bundesnachrichtendienst zur Durchführung eines Eingriffs in informationstechnische Systeme. Hierin liegt – unabhängig davon, ob eine Datenerhebung erfolgt – indes kein Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-System-Grundrecht). Der Schutzbereich dieses Grundrechts ist nämlich „nur“ eröffnet, soweit der Betroffene das informationstechnische System „als eigenes“ nutzt und deshalb „den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt“ (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07 u.a., Rn. 206). Bei den von § 32 Absatz 2 (einzig) betroffenen IT-Systemen von Anbietern von Telekommunikationsdiensten oder Digitalen Diensten handelt es sich in keinem Fall um ein solches „eigenes“ IT-System, d.h. um ein solches, dass „personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten“ (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07 u.a., Rn. 203).

Im Vergleich zum bisherigen § 19 Absatz 6 enthält die Regelung einige Unterschiede: So ist die Vorschrift in ihrem Wortlaut rechtssystematisch angepasst, um klarzustellen, dass es sich letztlich nur um eine besondere Art der Durchführung der strategischen Aufklärung handelt. Hiermit geht zugleich einher, dass eine gesonderte Anordnung für eine Maßnahme nach § 32 Absatz 2 nicht erforderlich ist; vielmehr ist sie – wie im geltenden Recht – von einer angeordneten strategischen Aufklärungsmaßnahme mit umfasst.

Zweitens wurde die Vorschrift insoweit verändert, als nicht länger nur ein Eingriff in die informationstechnischen Systeme von ausländischen Anbietern von Telekommunikationsdiensten oder digitalen Diensten im Ausland zulässig ist, sondern – in drei Fallvarianten – auch gegenüber inländischen Anbietern: Dies betrifft den Fall, dass ein ausländisches Unternehmen einen beherrschenden Einfluss über den inländischen Anbieter ausübt. Hintergrund hierfür ist, dass eine Vielzahl von entsprechenden Anbietern – die auch im Inland operieren – dem Bundesnachrichtendienst entgegen ihrer Verpflichtung zur Ausleitung der Daten eine Kooperation verweigern, insbesondere weil sie von ihren Konzernmüttern oder anderen beherrschenden ausländischen Unternehmen dazu angehalten werden. Der Bundesnachrichtendienst soll insoweit befähigt werden, in diesen Fällen eine anderweitig zulässige strategische Aufklärung gleichwohl durchzuführen. Ebenso ist ein Eingriff möglich, wenn der inländische Anbieter einem verpflichtenden Auskunftsersuchen nicht nachkommt; es handelt sich hier um einen Weg der Ersatzvornahme einer rechtmäßig bestehenden Verpflichtung durch den Bundesnachrichtendienst. Zuletzt kann es ausnahmsweise auch aus operativ-sicherheitlichen Gründen geboten sein, einen Eingriff durchzuführen, etwa,

weil tatsächliche Anhaltspunkte dafür bestehen, dass der Anbieter ein entsprechendes Ersuchen öffentlich machen würde.

Darüber hinaus wurde der maximal zulässige Zeitraum nach Erhebung der Daten durch den Anbieter von Telekommunikationsdiensten von 48 auf 72 Stunden erhöht, um dem Umstand Rechnung zu tragen, dass Verarbeitungsprobleme auch über das Wochenende auftreten und erst am nächsten Werktag behoben werden können. Schließlich wurde auch die Möglichkeit eröffnet, beim Anbieter von Telekommunikationsdiensten gespeicherte Bestandsdaten ohne zugrundeliegende Suchbegriffe zu erheben, da es sich bei Bestandsdaten nicht um Daten handelt, die dem Schutzbereich des Artikel 10 Absatz 1 des Grundgesetzes unterfallen und damit eine Begrenzung auf eine nur suchbegriffsbasierte Erhebung nicht geboten erscheint.

Zu Absatz 3

Absatz 3 bestimmt, dass eine Erhebung von Kommunikationsdaten aus rein inländischen Übertragungen – also Kommunikationen, bei denen keine Ausländer im Ausland beteiligt sind – im Wege der strategischen Fernmeldeaufklärung grundsätzlich unzulässig ist (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 170f.). Dabei werden von dieser Vorschrift nur „Kommunikationsdaten“ erfasst; nicht also solche Daten, welche zwar dem Schutz des Fernmeldegeheimnisses unterfallen, aber keine Inhalts- oder Metadaten einer interpersonellen Kommunikation sind. Diese, „andere mithilfe von Telekommunikationstechniken über Distanz transportierten Daten“ (BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Rn. 91) unterfallen nicht der vom Bundesverfassungsgericht aufgestellten Vorgabe der Aussonderung von „reinen Inlandsverkehren“. Dies folgt bereits daraus, dass in diesen Fällen – da es sich begrifflich nicht um personenbezogene Daten aus interpersonellen Kommunikationsvorgängen (d.h. Inhalts- oder Metadaten) handelt – keine besondere Schutzbedürftigkeit der Kommunikation zwischen zwei, sich auf dem Gebiet der Bundesrepublik befindlichen, Personen besteht. Vielmehr ist in diesen Fällen gerade die Kommunikation zwischen einer Person und einer Maschine oder zwischen zwei Maschinen betroffen. Die physische Belegenheit einer Maschine indes rechtfertigt keine wertungsmäßige Entsprechung zu der besonderen Schutzbedürftigkeit der inländischen Kommunikation. Dies folgt weiter auch daraus, dass der physische Ort eines Servers oder eines sonstigen IT-Systems oftmals beliebig ist und insbesondere für den einzelnen Nutzer nicht im Vorfeld zu erahnen ist. Dies würde eine Ausfilterung von Verkehren aufgrund gänzlich arbiträrer Umstände machen.

Die Vorschrift enthält – dem § 19 Absatz 7 Satz 2f. des bisherigen Rechts im Wortlaut entsprechende – Vorgaben für die erforderliche Ausfilterung der reinen Inlandskommunikation. Daten, die nicht unter die in den Nummern 1 bis 4 statuierten Ausnahmen der ausnahmsweise zulässigen Datenerhebung fallen, werden bei der Durchführung der strategischen Aufklärung bei Datenerhebung ausgefiltert, d.h. unverzüglich und automatisiert gelöscht.

Eine Ausnahme von dem Verbot der Erhebung und dem Gebot der Löschung von (rein) inländischen Kommunikationsdaten im Wege der strategischen Aufklärung ist nur in den explizit genannten Konstellationen der Nummern 1 bis 4 vorgesehen. Dabei erfolgt eine Erhebung in den Nummern 2 und 3 zwingend durch Verwendung von Suchbegriffen – also bereits auf Ebene der ersten Datenausleitung – da nur so sichergestellt werden kann, dass die jeweilige reine Inlandskommunikation dieser Variante unterfällt (Beispiel: Verwendung einer Telefonnummer eines Entführungsopfers, um dem o.g. automatisierten Filter vorgeschaltet eine ausnahmsweise Ausleitung zu ermöglichen). Damit scheidet eine „retrospektive“ Erkenntnisgewinnung durch Einsichtnahme in Daten, die „auf Verdacht“ gespeichert wurden, in diesen Fällen aus. Auch bei Nummer 1 wird dies regelmäßig der Fall sein, wobei insoweit nicht ausgeschlossen ist, dass ein solcher Fall auch ohne Verwendung von Suchbegriffen erkannt wird (etwa aufgrund verdächtigter Datenverkehre von bestimmten Servern), sodass eine Ausleitung auch hierauf basierend erfolgen kann. Die Daten nach

Nummer 4 dürfen demgegenüber – sofern eine sofortige Anonymisierung und damit eine verlässliche Entfernung des Personenbezugs erfolgt – ausgeleitet und gespeichert werden.

In die Daten darf nach Maßgabe des § 33 Einsicht genommen werden, ohne dass sie wie personenbezogene Kommunikationsdaten mit qualifizierten Inlandsbezug behandelt werden. Dem Ausnahmecharakter dieser Konstellationen wird durch die in Satz 3 verankerte, besondere Zweckbindungsbestimmung entsprochen. Diese Zweckbindung gilt dabei wiederum nicht für die Daten, welche im Sinne von Satz 1 Nummer 4 „unkenntlich gemacht“ wurden, da es sich insoweit schon nicht mehr um personenbezogene Daten handelt.

Zu Nummer 1

Bei Übertragungen im Rahmen eines terroristischen, staatlichen oder internationalen kriminellen Angriffs auf ein informationstechnisches System ist eine Erhebung der personenbezogenen Daten ausnahmsweise auch dann zulässig, wenn es sich um eine reine Inlandsübertragung handelt. Hintergrund dieser Ausnahme ist der Umstand, dass maliziöse Akteure häufig sog. Botnetzwerke (also eine Vielzahl von „fremden“ Geräten, deren Eigentümer keine Kenntnis davon haben, dass ihre Systeme für Angriffe genutzt werden) verwenden, um koordiniert groß angelegte Angriffe durchzuführen. Dabei werden – zumal wenn es sich um ein Ziel in der Bundesrepublik handelt – auch infizierte Systeme im Inland genutzt. Für eine wirkungsvolle Aufklärung solcher Angriffe ist es von essentieller Bedeutung, dass in diesen Fällen auch personenbezogene Daten aus der Inlandsübertragung durch den Bundesnachrichtendienst erhoben werden, um Angriffsvektoren, Ziele, Verwundbarkeiten, Methoden und Akteure aufklären zu können.

Zu Nummer 2

Eine Ausnahme von dem grundsätzlichen Verbot der Erhebung reiner Inland-Inland-Kommunikation ist zudem dann geboten, wenn dies im Interesse der betroffenen Person geschieht.

Dies ist zuvorderst der Fall, wenn der Schutz der betroffenen Person eine Einsichtnahme erfordert. Hierunter fallen insbesondere Fälle einer akuten Gefahrensituation für Leib oder Leben einer Person, z.B. im Falle von Geiselnahmen oder ähnlichen Bedrohungslagen. Darüber hinaus ist eine Einsichtnahme auch möglich, wenn die betroffene Person hierin eingewilligt hat, was etwa bei Mitarbeiterinnen und Mitarbeitern von Sicherheitsbehörden der Fall ist, die ein besonderes Interesse daran haben, den Bundesnachrichtendienst zu befähigen, etwaige Übermittlungen ausgehend von ihren Endgeräten im Blick zu behalten. Weiter betrifft dies etwa die Kommunikation von Angehörigen der zuerst genannten Personen, z.B. von Familienmitgliedern im Falle von Entführungen. Insbesondere für die zuletzt genannte Personengruppe kann zudem – wenn ihr Einverständnis nicht rechtzeitig eingeholt werden kann – auf ihre mutmaßliche Einwilligung abgestellt werden.

Zu Nummer 3

Eine Erhebung ist auch dann zulässig, wenn tatsächliche Anhaltspunkte dafür bestehen, dass hierdurch eine unmittelbar bevorstehende Gefahr für ein besonders gewichtiges Rechtsgut abgewendet werden kann. Diese Regelung greift die vormals in § 19 Absatz 7 Satz 6 enthaltene Bestimmung auf und sieht aber statt einer „erheblichen“ Gefahr nunmehr – wie im Gesetz einheitlich verwendet – eine „unmittelbar bevorstehende Gefahr“ vor. Hierbei handelt es sich (hier wie an anderen Stellen, wo dieser Begriff Verwendung findet) um einen dem allgemeinen Polizeirecht entlehnten Gefahrbegriff, der darauf abstellt, dass eine Gefahr nach allgemeiner Erfahrung sofort oder in aller nächster Zeit als gewiss anzusehen ist. Auch insoweit sind tatsächliche Anhaltspunkte hinreichend. Denkbare Fälle sind etwa konkrete Anschlagsplanungen. Auch wenn dabei der Anschlag selbst in zeitlicher Hinsicht noch nicht unmittelbar bevorstehen, ist in diesen Gefahren die Gefahr.

Zu Nummer 4

Eine Erhebung reiner Inlandsverkehre ist zudem zulässig, wenn unverzüglich nach Erhebung (dies setzt also denknotwendigerweise eine vorübergehende, flüchtige Speicherung voraus) die enthaltenen personenbezogenen Daten unkenntlich gemacht werden, da in diesem Fall der durch die Erhebung erfolgte Grundrechtseingriff aufgrund der unverzüglichen Unkenntlichmachung des Personenbezugs minimal ist. Hintergrund der Notwendigkeit der Regelung ist die Möglichkeit der Erkennung internationaler Kommunikationsnetzwerke, die auch oder ausschließlich über inländische Kommunikation miteinander in Beziehung gesetzt werden können. In der Praxis erfolgt diese Unkenntlichmachung unmittelbar nach Erfassung durch automatisierte Prozesse.

Die Unkenntlichmachung darf auch dergestalt erfolgen, dass die Eindeutigkeit der Daten erhalten bleibt. Die Erhaltung der Eindeutigkeit ist nach der Regelung möglich, jedoch nicht gesetzlich gefordert, wobei eine Eindeutigkeit im Sinne der Vorschrift auch dann erreicht sein kann, wenn die Wahrscheinlichkeit so hoch ist, dass ernsthafte Zweifel nicht mehr bestehen. Dies gilt auch für den Begriff der Unmöglichkeit. Bestimmte Anforderungen an das Verfahren zur Unkenntlichmachung werden durch den Gesetzgeber nicht vorgegeben, die Wahl des Verfahrens zur Unkenntlichmachung der Daten bleibt dem Bundesnachrichtendienst überlassen.

Zu § 33 (Einsichtnahme in Kommunikationsdaten im Rahmen von strategischen Aufklärungsmaßnahmen)

Die Vorschrift regelt die (nunmehr) zweite Stufe der Erhebung personenbezogener Daten im Wege der strategischen Aufklärung durch den Bundesnachrichtendienst. Sie bestimmt die Voraussetzungen für die Einsichtnahme in diejenigen kommunikationsbezogenen personenbezogenen Daten, die mittels der strategischen Aufklärung nach § 31 im Rahmen einer strategischen Aufklärungsmaßnahme nach § 32 erhoben und vorübergehend zwischengespeichert wurden.

Die mit dieser Einsichtnahme einhergehenden Eingriffe in die Grundrechte betroffener Personen (insbesondere das Grundrecht aus Artikel 10 Absatz 1 des Grundgesetzes) werden dabei normativ durch erhöhte Eingriffsschwellen, durch eine Reihe verfahrenssichernder und einschränkender Maßgaben und insbesondere durch das Erfordernis einer objektivrechtlichen und unabhängigen Kontrolle durch den Unabhängigen Kontrollrat gerechtfertigt. Die insoweit vorgesehenen Schranken der Verarbeitung von personenbezogenen Daten im Rahmen der strategischen Aufklärung entsprechen dabei im Wesentlichen den bereits im bisherigen Gesetz getroffenen Vorgaben, die wiederum die Rechtsprechung des Bundesverfassungsgerichts (hierzu insbesondere BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17) aufgreifen.

Für die Einsichtnahme in kommunikationsbezogene Inhaltsdaten mit qualifiziertem Inlandsbezug gelten ergänzend die Einschränkungen des § 34.

Zu Absatz 1

Entsprechend der geltenden Rechtslage unterscheidet das Gesetz (nunmehr auf Ebene der Einsichtnahme) zwischen der inhaltlichen Auswertung von kommunikationsbezogenen Metadaten und der von kommunikationsbezogenen Inhaltsdaten. Dabei wird die vormals angelegte Unterscheidung zwischen „politischer Unterrichtung“ und „Gefahrenfrüherkennung“ (vgl. den bisherigen § 19 Absatz 1) in der nunmehr angelegten gesetzlichen Systematik aufgelöst: Eine Erhebung zur politischen Unterrichtung ist nicht länger gesondert geregelt; auch insoweit stellt das Gesetz jetzt vielmehr darauf ab, dass eine Erhebung von Informationen der Früherkennung von Bedrohungen für besonders gewichtige Rechtsgüter dient. Diese Vereinheitlichung bildet die tatsächliche Arbeit des Bundesnachrichtendienstes ab, da letztlich eine nachrichtendienstliche Erhebung nie ohne Bezug zu einer potenziellen Bedrohung erfolgt – jedenfalls mögliche Bedrohungen für die außenpolitische

Handlungsfähigkeit rechtfertigen dabei regelmäßig auch eine Erhebung von Informationen zu z.B. politischen Entwicklungen im Ausland, humanitären Krisen im Ausland, Naturereignissen etc.

Die vormals angelegte erleichterte Erhebung (und aufgrund der Einstufigkeit des bisherigen Rechts auch erleichterte inhaltliche Auswertung) wird durch Absatz 1 für kommunikationsbezogene Metadaten insoweit abgebildet, als eine Einsichtnahme insoweit schon zulässig ist, wenn dies (die Einsichtnahme) zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist.

Für den Zeitpunkt der Einsichtnahme ist auf das Erstellen einer Meldung abzustellen, da erst zu diesem Zeitpunkt eine inhaltliche Bewertung möglich ist.

Zu Absatz 2

Die Regelung schafft die (Regel-)Befugnis des Bundesnachrichtendienstes, in die mittels der strategischen Aufklärung nach § 31 im Rahmen einer strategischen Aufklärungsmaßnahme nach § 32 erhobenen kommunikationsbezogenen Inhaltsdaten Einsicht zu nehmen (vgl. zur Reichweite dieses Begriffes oben). Dabei ist – wie im bisherigen § 19 Absatz 1 – eine vorherige Anordnung, welche der Kontrolle durch den Unabhängigen Kontrollrat unterliegt, erforderlich. Diese Anordnung hat insoweit künftig sowohl Angaben zu der Erhebung von personenbezogenen Daten als auch zu der anschließend beabsichtigten Einsichtnahme zu enthalten. Dies ist schon deshalb geboten, um eine umfangreiche objektivrechtliche Kontrolle des von der Einsichtnahme ausgehenden (besonders gewichten, vgl. hierzu oben) Grundrechtseingriff zu rechtfertigen.

Der Wegfall der Nennung der notwendigen Beauftragung durch das Bundeskanzleramt im Vergleich zum geltenden Recht folgt daraus, dass dieses Erfordernis nunmehr in § 18 Absatz 1 Nummer 2 für den Einsatz aller nachrichtendienstlichen Mittel vorgesehen ist, die zur nachrichtendienstlichen Auslandsaufklärung eingesetzt werden.

Zu Nummer 1

Die Regelung entspricht dem bisherigen § 19 Absatz 1 Nummer 2 in Verbindung mit § 19 Absatz 4 insoweit als sie die konkreten Eingriffsschwellen für die Einsichtnahme in kommunikationsbezogene Inhaltsdaten aus strategischen Aufklärungsmaßnahmen zur Früherkennung von Bedrohungen regelt. Entsprechend den obigen Ausführungen wurden diese Eingriffsschwellen dabei der allgemeinen Systematik des Gesetzes angepasst, sodass keine eigenen Kataloge von Gefahrenbereichen (bisheriger § 19 Absatz 4 Nummer 1) und Rechtsgütern (bisheriger § 19 Absatz 4 Nummer 2) mehr vorgesehen sind, sondern stattdessen an die in § 3 Absatz 1 definierten erheblichen Bedrohungen angeknüpft wird. Diese Änderung ist auch begrifflich vorgesehen, da nunmehr auf die Früherkennung von Bedrohungen abgestellt wird. Hierdurch wird insgesamt die Gesetzessystematik vereinheitlicht und das Verständnis der Regelungen für Rechtsanwender und Betroffene erleichtert. Der Begriff der Bedrohungen im Nachrichtendienstrecht soll auch in sprachlicher Hinsicht die nachrichtendienstliche Aufgabe der Vorfeldaufklärung verdeutlichen, die weit im Vorfeld des – insbesondere in polizeilichen Kontexten gebräuchlichen Gefahrenbegriffs – anzusiedeln ist. Auch bislang wurde der Begriff der „Gefahren/Gefahrenbereiche“ im BND-Gesetz als Bedrohung im Sinne einer Vorfeldaufklärung ausgelegt. Eine wesentliche inhaltliche Änderung geht mit dieser Anpassung nicht einher; vielmehr entspricht der Bedrohungskatalog inhaltlich im Wesentlichen den unter den bisherigen Katalog von Gefahrenbereichen und Rechtsgütern subsumierten Sachverhalten.

Mittels der Einsichtnahme erfolgt die inhaltliche Sicherung der erhobenen Daten. Soweit tatsächliche Anhaltspunkte dafür vorliegen, dass dies - also die inhaltliche Sichtung selbst, nicht schon die jeweiligen Daten, deren Ergiebigkeit der Bundesnachrichtendienst vor Einsichtnahme nicht bewerten kann - erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen zu erlangen, dürfen also alle kommunikationsbezogenen Inhaltsdaten

inhaltlich gesichtet werden. Im Anschluss an diese Einsichtnahme folgt die Weiterverarbeitung sodann den allgemeinen Vorschriften. Dies bedeutet, dass eine Weiterverarbeitung (nach § 52 Absatz 1) möglich ist, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Weiterverarbeitung zumindest zur nachrichtendienstlichen Auslandslaufklärung erforderlich ist. Damit bildet die erste Qualifikationsstufe die tatbestandliche Rechtfertigung für das (erhöhte) Eingriffsgewicht der Einsichtnahme; der allgemeinen Systematik folgend sind jedoch auch Zufallsfunde, die im Rahmen dieser Einsichtnahme vorgefunden werden und welche diese Qualifikationsstufe nicht erreichen, der Weiterverarbeitung zugänglich.

Zu Nummer 2

Eine Einsichtnahme ist ferner zulässig, wenn dies im Interesse der betroffenen Person geschieht. Dies ist zuvorderst der Fall, wenn der Schutz der betroffenen Person eine Einsichtnahme erfordert. Hierunter fallen insbesondere Fälle einer akuten Gefahrensituation für Leib oder Leben einer Person, z.B. im Falle von Geiselnahmen oder ähnlichen Bedrohungslagen. Darüber hinaus ist eine Einsichtnahme auch möglich, wenn die betroffene Person hierin eingewilligt hat, was etwa bei im Ausland eingesetzten Mitarbeiterinnen und Mitarbeitern des Bundesnachrichtendienstes oder anderer Behörden der Fall, die ein besonderes Interesse daran haben, den „eigenen Dienst“ zu befähigen, etwaige Übermittlungen ausgehend von ihren Endgeräten im Blick zu behalten. Weiter betrifft dies etwa die Kommunikation von Angehörigen der zuerst genannten Personen, z.B. von Familienmitgliedern im Falle von Entführungen. Insbesondere für die zuletzt genannte Personengruppe kann zudem – wenn ihr Einverständnis nicht rechtzeitig eingeholt werden kann – auf ihre mutmaßliche Einwilligung abgestellt werden.

Zu Nummer 3

Auf die Begründung zu § 32 Absatz 3 Nummer 3 wird verwiesen.

Zu Absatz 3

Die Regelung übernimmt im Wesentlichen die Regelung des bisherigen § 19 Absatz 5, wobei die Beschränkung des Zugriffs auf Inhaltsdaten durch Suchbegriffe nun normenklar als Bestandteil der zweiten Stufe der Erhebung geregelt ist. Entbehrlich ist die Beschränkung dann, wenn eine unmittelbar bevorstehende Gefahr vorliegt – da in diesen Fällen auch im bisherigen Recht eine Übermittlung „aus der Eignungsprüfung“ hinaus möglich war, stellt dies indes keine Erweiterung, sondern eine systematische Überführung dar.

Wie im geltenden Recht ist eine Prüfung der Suchbegriffe durch das gerichtsähnliche Kontrollorgan des Unabhängigen Kontrollrates im Rahmen der Vorabkontrolle dabei nicht angezeigt. Entsprechend der Komplementarität von Vorabkontrolle und nachgelagerter Kontrolle im Rahmen von strategischen Aufklärungsmaßnahmen erfolgt die Qualifizierung eines Aufklärungsthemas als erhebliche Bedrohung in der Vorabkontrolle, die Prüfung der Suchbegriffe anhand diese Aufklärungsthemas im Rahmen der nachgelagerten Kontrolle (vgl. hierzu auch die Begründung zu § 47).

Faktisch kann eine Prüfung nach Satz 2 regelmäßig nur dergestalt erfolgen, dass das jeweilige Aufklärungsziel, dem der individuelle Suchbegriff zugeordnet ist, Gegenstand der Prüfung bildet.

Für die Prüfung, ob eine Einsichtnahme gerechtfertigt ist, stellt das „Treffen“ eines Suchbegriffes, welcher einer nachrichtendienstlich relevanten Person zugeordnet ist, zugleich einen wesentlichen tatsächlichen Anhaltspunkt dar.

Zu Absatz 4

Die Bestimmung geeigneter Suchbegriffe oder Telekommunikationsnetze ist nach wie vor von immenser praktischer Bedeutung für den Bundesnachrichtendienst, da nur so eine wirksame Zielsetzung von strategischen Aufklärungsmaßnahmen möglich ist.

Wie bislang ist dem Bundesnachrichtendienst die Möglichkeit eröffnet, die strategische Aufklärung auch im Rahmen von Maßnahmen der sog. Eignungsprüfung (§ 30 Nummer 1) durchzuführen. Insoweit geht die Regelung dem in § 31 Absatz 1 geregelten Grundsatz, dass eine Weiterverarbeitung nur nach Einsichtnahme nach § 33 Absatz 1 und § 34 Absatz 2 zulässig ist, vor. Diese Befugnis ist essentiell, um strategische Aufklärungsmaßnahme vorzubereiten, da der Bundesnachrichtendienst in der Lage sein muss, geeignete – das heißt nachrichtendienstlich relevante – Telekommunikationsnetze und Suchbegriffe im Rahmen von strategischen Aufklärungsmaßnahmen zu identifizieren. Geboten ist dabei weiterhin, dies wird durch Satz 2 sichergestellt, dass die so erhobenen kommunikationsbezogenen Daten nur für die Zwecke der Eignungsprüfung genutzt werden dürfen.

Durch die nunmehr vorgesehene Möglichkeit einer kurzfristigen Speicherung der erhobenen Daten, wird der Bundesnachrichtendienst künftig auch befähigt, die Suchbegriffe, die er im Rahmen der Eignungsprüfung als nachrichtendienstlich relevant identifiziert hat, in begrenztem Rahmen in eine laufende strategische Aufklärungsmaßnahme zu „überführen“ und die bereits als nachrichtendienstlich relevant erkannten Kommunikationsinhalte so nutzbar zu machen und diese nicht – wie bislang – verwerfen zu müssen. Diese Möglichkeit ist von großer Wichtigkeit für die wirksame Auslandsaufklärung, da es bei der paketvermittelten Übertragung immer vom Zufall abhängt, auf welchen Leitungen die Verkehre übertragen werden, d.h. es kann nicht vorausgesagt werden, ob auch zukünftig relevante Verkehre mit dem erkannten Suchbegriff auf den überwachten Strecken übertragen werden. Vor diesem Hintergrund ist es notwendig, relevante Erkenntnisse weiterverarbeiten zu können.

§ 33 Absatz 3 baut auf dem bisherigen § 24 auf. Dabei konnte die Vorschrift des bisherigen § 24 allerdings infolge der systematischen Veränderungen insgesamt vereinfacht werden: Der bisherige § 24 Absatz 2 Satz 1 ist entbehrlich geworden, da die dort genannten Schwellen nunmehr schon dadurch gewahrt sind, dass der Bundesnachrichtendienst ohnehin die strategische Aufklärung nur bei tatsächlichen Anhaltspunkten, dass dies für die nachrichtendienstliche Auslandsaufklärung erforderlich ist, durchführen darf. Auch der bisherige § 24 Absatz 4 ist entbehrlich, da die Mitwirkungspflichten von sog. Providern ebenfalls schon für die erste Stufe der Datenerhebung geregelt sind. Die im bisherigen § 24 Absatz 5 Satz 1 enthaltene Zweckbeschränkung ist in Satz 2 geregelt, der Verweis auf das BSI-Gesetz erübrigt sich schon aufgrund der allgemeinen Regelungen zur Verarbeitung von Daten, die den Kernbereich privater Lebensgestaltung betreffen. Zuletzt ist der bisherige § 24 Absatz 7 nicht länger Bestandteil der Regelung zur „Eignungsprüfung“, sondern nunmehr – da es sich um eine Übermittlungsvorschrift handelt – sachgerecht in Abschnitt 5 enthalten. Nicht länger erforderlich ist die gesonderte Anordnung der Eignungsprüfung durch die Behördenleitung des Bundesnachrichtendienstes oder einer von ihr bestimmten Vertretung (bisheriger § 24 Absatz 4). Die Entbehrlichkeit folgt bereits daraus, dass die Eignungsprüfung nur im Rahmen von strategischen Aufklärungsmaßnahmen zulässig ist, die wiederum angeordnet werden muss (und sowohl bezüglich der Erhebung als auch der Einsichtnahme außerhalb der Eignungsprüfung der Zustimmung des Unabhängigen Kontrollrates bedarf).

Die Eignungsprüfung kann insbesondere – wie sich systematisch bereits aus der Norm selbst ergibt – auch ohne Verwendung von Suchbegriffen erfolgen.

Für kommunikationsbezogene Inhaltsdaten mit qualifiziertem Inlandsbezug ist eine Einsichtnahme zur Eignungsprüfung unzulässig. Dies bedurfte dabei keiner expliziten

gesetzlichen Regelung, da die Einsichtnahme in kommunikationsbezogene Inhaltsdaten mit qualifiziertem Inlandsbezug abschließend in § 34 geregelt ist.

Zu Absatz 5

Die Regelung übernimmt im Wesentlichen die Regelung des bisherigen § 20 Absatz 3 (vgl. dazu die Begründung zu § 20 Absatz 3 in BT-Drs. 19/26103). Die Regelung enthält als Folgeanpassung zudem den Verweis auf die neu gefasste Befugnis des § 35, der die Befugnis zu einer individualisierenden Überwachung der Telekommunikation enthält. Ist für den Bundesnachrichtendienst erkennbar, dass die Datenerhebung mittels der strategischen Aufklärung zur Erhebung der gesamten Kommunikation einer Person führt, richtet sich die Datenerhebung nach § 30. In diesem Fall ist die individualisierende Überwachung auch im Rahmen der strategischen Aufklärung zulässig. Spiegelbildlich hierzu ist dem Bundesnachrichtendienst auch die alternative Möglichkeit eröffnet, eine Maßnahme der Telekommunikationsüberwachung in der Weise durchzuführen, dass die Anschlusskennungen als Suchbegriffe in der strategischen Aufklärung verwendet wurde.

Zu § 34 (Besondere Vorgaben für die Einsichtnahme in Kommunikationsdaten mit qualifiziertem Inlandsbezug)

Durch die Auflösung des Artikel 10-Gesetzes ist eine Überführung der dortigen Erhebungsbefugnisse in die nachrichtendienstliche Fachgesetze erforderlich geworden. In § 34 wird nunmehr die strategische Inland-Ausland-Fernmeldeaufklärung nach §§ 5, 8 des Artikel 10-Gesetzes in die Systematik des BND-Gesetzes überführt. Durch diese Überführung ist – den Regelungen der strategischen Aufklärung entsprechend – eine Zweistufigkeit des Erhebungsprozesses auch für die Kommunikationsdaten von Deutschen, inländischen juristischen Personen und Inländern im Sinne des § 30 Nummer 6 (der sog. „qualifizierte Inlandsbezug“) vorgesehen: Im Rahmen der ersten Stufe der Datenerhebung (die „Erhebung“ im engeren Sinne) werden die kommunikationsbezogenen Inhaltsdaten mit qualifiziertem Inlandsbezug zunächst miterhoben und zunächst „nur“ gekennzeichnet. Engere Vorgaben sieht § 34 dann für die Einsichtnahme in die erhobenen kommunikationsbezogenen Inhaltsdaten mit qualifiziertem Inlandsbezug vor. Im Rahmen dieser Vorgaben erfolgt zugleich und insbesondere auch eine Lösung von den in §§ 5, 8 des Artikel 10-Gesetzes vorgesehenen Gefahrenbereichen.

Der besonderen Schutzbedürftigkeit der vom Schutzbereich des Artikel 10 des Grundgesetzes erfassten Daten von Deutschen, inländischen juristischen Personen und Inländern (auch im Vergleich zu den Daten von Ausländerinnen und Ausländern im Ausland, vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 104), die nunmehr im Rahmen der Begriffsbestimmung des § 30 Nummer 6 als Daten „mit qualifiziertem Inlandsbezug“ bezeichnet werden, wird dabei im Rahmen der angepassten Systematik in mehrerer Hinsicht entsprochen. Zunächst ist die Erhebung von Kommunikationsdaten aus reinen Inlandsverkehren grundsätzlich unzulässig und nur in eng begrenzten Ausnahmefällen möglich (vgl. § 32 Absatz 3). Kommunikationsdaten mit qualifiziertem Inlandsbezug, bei denen es sich um sog. Ausland-Inland-Verkehre handelt, sind durch den Einsatz geeigneter Filter zu identifizieren und nach § 64 Absatz 2 entsprechend zu kennzeichnen. Weiter ist die Einsichtnahme in kommunikationsbezogenen Inhaltsdaten mit qualifiziertem Inlandsbezug im Rahmen der Eignungsprüfung nicht zulässig.

Werden Kommunikationsdaten mit qualifiziertem Inlandsbezug entgegen der Vorgaben des § 34 Absatz 2 verarbeitet oder erlangt der Bundesnachrichtendienst zu einem späteren Zeitpunkt Kenntnis von diesem Umstand, so sind die erhobenen Daten nach § 66 Absatz 3 unverzüglich zu löschen. Zudem ist die Einsichtnahme und Löschung bei kommunikationsbezogenen Inhaltsdaten mit qualifiziertem Inlandsbezug gemäß § 67 zu dokumentieren.

Zu Absatz 1

In Absatz 1 wird zunächst die grundsätzliche Einschränkung einer Einsichtnahme kommunikationsbezogener Inhaltsdaten von Deutschen, inländischen juristischen Personen und Inländern, die im Wege der strategischen Aufklärung erhoben wurden, geregelt: Die Einsichtnahme in kommunikationsbezogene Metadaten mit qualifiziertem Inlandsbezug ist nach Maßgabe des § 33 Absatz 1 auch ohne den Einsatz von Suchbegriffen zulässig. Der praktische Bedarf dieser Erweiterung gegenüber dem bisherigen Recht liegt darin, dass nur durch die umfassende Analyse von Metadaten bislang unerkannte Personen, die sich z.B. geheimdienstlich betätigen, ausgemacht werden können. So kann durch eine Metadatenanalyse anhand spezifischer Standorte beispielsweise festgestellt werden, wo sich verdächtige Personen aufgehalten haben, die ins Ausland kommunizierten.

Zu Absatz 2

Die Eingriffsschwelle für die Einsichtnahme in kommunikationsbezogene Inhaltsdaten mit qualifiziertem Inlandsbezug entspricht der Einsichtnahme in kommunikationsbezogene Metadaten mit qualifiziertem Inlandsbezug (bzw. zugleich den Voraussetzungen für eine Einsichtnahme in kommunikationsbezogene Inhaltsdaten nach § 33 Absatz 2) – erforderlich sind mit anderen Worten tatsächliche Anhaltspunkte dafür, dass Informationen über eine erhebliche Bedrohung gewonnen werden können.

Wie in § 33 Absatz 3 ist auch im Rahmen der Einsichtnahme in kommunikationsbezogene Inhaltsdaten mit qualifiziertem Inlandsbezug zudem vorgesehen, dass diese Einsichtnahme nur anhand von Suchbegriffen erfolgen darf, solange hiernach nicht ausnahmsweise eine Einsicht auch ohne Verwendung von Suchbegriffen zulässig ist (konkret in den Fällen des § 33 Absatz 2 Nummer 3).

Dem besonderen Schutzgehalt der Daten von Deutschen/Inländern entspricht Absatz 2 Satz 2, der sicherstellt, dass entsprechend dem bisherigen § 5 Absatz 2 des Artikel 10-Gesetzes keine gezielte Erfassung von Telekommunikationsanschlüssen von Deutschen oder Inländern erfolgt (vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 186).

Die von dem in Absatz 1 geregelten Grundsatz vorgesehenen Ausnahmen entsprechen den in § 32 Absatz 3 Nummer 1 bis 3 enthaltenen Sonderfällen, bei denen eine Erfassung rein innerdeutscher Verkehre zulässig ist. Erst recht muss es in diesen Fällen möglich sein, auf erfasste und gespeicherte Inland-Ausland Kommunikation auch unter Verwendung von Suchbegriffen deutscher/inländischer Teilnehmer zurückzugreifen. Ergänzend wird auf die o.g. Begründung Bezug genommen.

Zu § 35 (Telekommunikationsüberwachung)

Die in § 35 geregelte Befugnis zur Erhebung von personenbezogenen Daten mittels der Telekommunikationsüberwachung wird erstmals im BND-Gesetz aufgenommen. Hierdurch wird zum einen die vormals in § 3 des Artikel 10-Gesetzes enthaltene Befugnis, einer Inlands-Telekommunikationsüberwachung in das BND-Gesetz überführt. Zudem wird nun auch der Einsatz dieses nachrichtendienstlichen Mittels gegenüber Ausländern im Ausland geregelt.

Anders als im Rahmen der strategischen Aufklärung ist hier aufgrund der Zielgerichtetheit der Maßnahme nicht zwischen der Erhebung und Einsichtnahme in die erhobenen Daten zu unterscheiden. Vielmehr geht mit der Befugnis zur Erhebung sogleich die Befugnis zur Einsichtnahme einher, wobei die besondere Notwendigkeit der Relevanzprüfung auf nachrichtendienstliche Inhalte nach § 65 Absatz 2 für kommunikationsbezogene Inhaltsdaten zu berücksichtigen ist.

Zu Absatz 1

In § 35 Absatz 1 ist die Befugnis des Bundesnachrichtendienstes zur Durchführung von Maßnahmen der Telekommunikationsüberwachung, mittels derer personenbezogene Daten erhoben werden, geregelt. Die Telekommunikationsüberwachung ist die „individualisierende Überwachung und Aufzeichnung der Telekommunikation“ (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 189) und zielt – in Abgrenzung zur strategischen Aufklärung, die auf die „personenunabhängige“ Erhebung von Daten abstellt und lediglich durch die Verwendung formeller Suchbegriffe eine Zielrichtung vorsieht – gerade auf die Erfassung aller Kommunikationsverkehre individuell bestimmbarer Personen. Die Umsetzung der Telekommunikationsüberwachung erfolgt hierbei grundsätzlich durch Ausleitung personenbezogener Daten anhand von Anschlusskennungen durch Anbieter von Telekommunikationsdiensten (siehe § 30 Nummer 12).

Die für dieses nachrichtendienstliche Mittel erforderliche Eingriffsschwelle differenziert zwischen kommunikationsbezogenen Meta- und Inhaltsdaten. Erstere darf der Bundesnachrichtendienst erheben, wenn tatsächliche Anhaltspunkte vorliegen, dass dies für die nachrichtendienstliche Auslandsaufklärung erforderlich ist. Die – einem höheren Schutz unterliegenden Inhaltsdaten – darf der Bundesnachrichtendienst hingegen erfordern das Vorliegen von tatsächlichen Anhaltspunkten dafür, dass die Maßnahme im Einzelfall erforderlich ist, um Informationen zu zumindest erheblichen Bedrohungen im Sinne des § 3 Absatz 1 zu erlangen.

Die Befugnis erstreckt sich dabei auch auf Maßnahmen der Telekommunikationsüberwachung gegenüber Ausländern, mit denen als „Beifang“ die Kommunikation von Deutschen, inländischen juristischen Personen und Inländern (deren Kommunikationsdaten - der allgemeinen Systematik folgend – solche mit qualifiziertem Inlandsbezug sind) erfasst werden. Kommt es zu einer entsprechenden Erfassung, sind die jeweiligen Verkehre indes im Rahmen der verfahrenssichernden Vorgaben auch wie Kommunikationsdaten mit qualifiziertem Inlandsbezug zu behandeln, das heißt entsprechend zu kennzeichnen und zu prüfen.

Zu Absatz 2

In § 35 Absatz 2 wird die Befugnis zur Durchführung von Telekommunikationsmaßnahmen mit zusätzlichen Einschränkungen versehen, wenn sich die Maßnahme gegen deutsche Staatsangehörige, inländische juristische Personen oder Inländer richtet.

Die genannten kommunikationsbezogenen Inhaltsdaten unterliegen dabei (vgl. zur gebotenen Abstufung bei der Überwachung von Verkehrs- und Inhaltsdaten bereits grundlegend BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 107) einer besonderen Schutzbedürftigkeit. Diese leitet sich vornehmlich daraus ab, dass die betroffenen Personen in einem besonderen Näheverhältnis zur deutschen Staatsgewalt stehen, sodass die von der Telekommunikationsüberwachung ausgehenden Eingriffe in die Grundrechte (d.h. insbesondere in Artikel 10 Absatz 1 des Grundgesetzes) schwerer wiegen. Um dieses besondere Eingriffsgewicht zu kompensieren, ist die Erhebung von kommunikationsbezogenen Metadaten nur zulässig, wenn tatsächliche Anhaltspunkte für eine erhebliche Bedrohung vorliegen, und die Erhebung von Inhaltsdaten nur zulässig, wenn tatsächliche Anhaltspunkte für eine Bedrohung von herausgehobener Bedeutung vorliegen.

Richtet sich die Maßnahme gegen einen Ausländer im Ausland (Absatz 1) und handelt es sich bei der erfassten (inhaltlichen) Kommunikation von Personen mit qualifiziertem Inlandsbezug um einen bloßen „Zufallstreffer“, so gelten die erhöhten Eingriffsschwellen des Absatz 2 hingegen nicht. In diesem Fall greifen indes gleichwohl die besonderen Vorgaben zur Kennzeichnung, Prüfung und Löschung von Inlandskommunikationsdaten.

Zu Absatz 3

Die Befugnis zur Telekommunikationsüberwachung wird in § 35 Absatz 3 von der Möglichkeit flankiert, diese im Wege der strategischen Aufklärung durchzuführen. Hiermit ist gemeint, dass der Bundesnachrichtendienst bei einer angeordneten und im Rahmen der Vorabkontrolle durch den Unabhängigen Kontrollrat genehmigten Telekommunikationsüberwachung auch Suchbegriffe (von Deutschen) im Rahmen von strategischen Aufklärungsmaßnahmen zur Einsichtnahme nutzen kann. Diese Befugnis ist einerseits notwendig, um die Providerausleitung (insbesondere bei ausländischen Providern, die oftmals nicht oder nur schwer durchsetzbar sind) zu ermöglichen. Zugleich ist aufgrund der weniger starken Zielgerichtetheit der strategischen Aufklärungsmaßnahmen hiermit auch ein für die mit einer Telekommunikationsüberwachung in den Blick genommenen Person geringerer Grundrechtseingriff verbunden. Die strategische Aufklärung stellt insoweit ein „behelfsmäßiges Minus“ zu einer individualisieren Überwachung durch eine Maßnahme der Telekommunikationsüberwachung im engeren Sinne dar. Es handelt sich hierbei um eine „bloße“ Durchführungsvorschrift, sodass auch diese Art der Durchführung durch die Anordnung einer Telekommunikationsüberwachung jedenfalls erfasst ist und nicht im Einzelnen bezeichnet werden muss.

Dem Bundesnachrichtendienst ist es erlaubt, auch im Wege der Amtshilfe für das Bundesamt für den Verfassungsschutz oder den Militärischen Abschirmdienst eine Telekommunikationsüberwachung im Wege der strategischen Aufklärung nach diesen Maßgaben durchzuführen.

Zu Absatz 4

In Absatz 4 ist geregelt, gegen wen Maßnahmen der Telekommunikationsüberwachung eingesetzt werden dürfen. Hierbei ist zunächst das Verantwortlichkeitsprinzip maßgebend, d.h. die Maßnahme darf gegen Personen erfolgen, die für die aufzuklärende (erhebliche) Bedrohung verantwortlich ist oder diese fördert (Nummer 1). Für Nummer 2 wird auf die Begründung zu § 13 Absatz 2 Nummer 3 Bezug genommen. Auch hier ist ein Zusammenhang mit dem Aufklärungsziel, der Grund zu der Annahme gibt, dass aufklärungsrelevante Informationen gewonnen werden können, insbesondere dann gegeben, wenn sich die Maßnahme gegen Nachrichtenmittlerinnen oder Nachrichtenmittlern richten (Buchstabe a), wobei auch die unbewusste oder nicht-willentliche Mitteilung entsprechender Nachrichten umfasst ist, oder wenn sich die Maßnahme gegenüber Personen richtet, deren Anschlüsse von den eigentlichen Verursachern genutzt werden, richtet (Buchstabe b). Ein alleiniges Abstellen auf die Anschlüsse ist dabei nicht hinreichend, da mit der (personengerichteten) Telekommunikationsüberwachung grundsätzlich alle Anschlüsse der betroffenen Person überwacht werden können und ein Rückgriff auf einzelne Anschlüsse (deren Kennungen insoweit individuell vorliegen müssen) regelmäßig zu kurz griffe.

Um eine Aufklärung von abgeschlossenen Netzwerken (insbesondere sog. Chatgruppen oder Angreifernetzwerken im Bereich der Cyberkriminalität) zu ermöglichen, die dem Zweck dienen, eine erhebliche Bedrohung zu unterstützen, darf der Bundesnachrichtendienst mittels der Telekommunikationsüberwachung auch Anschlüsse überwachen, die Teil eines abgegrenzten Netzwerks sind (Nummer 2 Buchstabe c). Dabei ist insoweit eine Modifikation des Verantwortlichkeitsprinzips geboten, da hierbei nicht die Verantwortlichkeit einer einzelnen Person (bzw. eines individuellen Anschlussnutzers) in Rede steht, sondern die von dem Netzwerk als solches ausgehende Bedrohung. Der Bundesnachrichtendienst darf insoweit Maßnahmen der Telekommunikationsüberwachung einsetzen, um die Mitglieder dieses Netzwerks insgesamt aufzuklären, solange tatsächliche Anhaltspunkte dafür bestehen, dass diese das Netzwerk ausschließlich oder ganz überwiegend nutzen, um die erhebliche Bedrohung zu unterstützen. Eine ganz überwiegende Nutzung ist insoweit anzunehmen, wenn über das Kommunikationsnetzwerk nur vereinzelt Inhalte übermittelt werden, die nicht der Unterstützung einer erheblichen Bedrohung dienen, oder das Netzwerk mit dem expliziten Ziel geschaffen wurde, um als Kommunikationsbasis für eine Gruppe

von Personen zu dienen, welche sich der Verwirklichung oder Unterstützung einer erheblichen Bedrohung verschrieben haben.

Zu § 36 (Erhebung technischer Spuren aus informationstechnischen Systemen bei informationstechnischen Angriffen)

Maßnahmen, die auf die Erhebung technischer Spuren gerichtet sind, sind in Bezug auf die informationelle Selbstbestimmung typischerweise eher gering eingreifend. Für den Fall der Erhebung der Kopie einzelner Teile eines informationstechnischen Systems, bei denen denkbarerweise in einem größeren Umfang Daten auch Nichtbetroffener erhoben werden, wird gleichwohl die unabhängige Vorabkontrolle durch den Unabhängigen Kontrollrat vorgesehen. Die Mitteilungspflichten sind zentral in § 100 geregelt, Löschpflichten in § 56. Weitere Vorgaben zur Durchführung finden sich in § 39 Absatz 2, 3, 4 und 5.

Zu Absatz 1

Die in Absatz 1 enthaltene Befugnis ergänzt § 14 um die Möglichkeit einer Selbstvornahme. Die Befugnis ist auf die Fälle begrenzt, in denen erforderliche Informationen nicht oder nicht ohne Gefährdung des Erhebungszwecks durch Auskunft des Anbieters nach § 14 erlangt werden können. Die Gefährdung des Erhebungszwecks durch die Verpflichtung des Anbieters ist insbesondere dann anzunehmen, wenn Anhaltspunkte dafür vorliegen, dass der Anbieter selbst an dem Angriff mitwirkt oder die Vertraulichkeit nicht gewährleistet ist, also das Risiko besteht, dass der Angreifer davon erfährt, dass sein Angriff im Fokus der Aufklärung ist. Solche Sachverhalte sind zwar die Ausnahme, eine wirksame Aufklärung muss aber auch für solche Sondersachverhalte das geeignete Aufklärungsmittel erhalten.

Zu Absatz 2

Der Absatz regelt eine neue, besondere Befugnis des Bundesnachrichtendienstes, jenseits einer bloßen Datenerhebung auch „einwirkend“ tätig zu werden. Die Vorschrift bildet einen Spezialfall des – allgemeineren – § 39 Absatz 4 ab. Die dortige Befugnis knüpft daran an, dass im Rahmen der aufklärenden Tätigkeit eine unmittelbar bevorstehende Gefahr für ein besonders gewichtiges Rechtsgut ausgemacht wird. Demgegenüber ist die hier vorgesehene Befugnis daran geknüpft, dass sich die Gefahr bereits in einer Störung realisiert hat, die nunmehr aber – nur, eine Subsidiarität ist vorgesehen – durch den Bundesnachrichtendienst beseitigt werden kann. Es wird ergänzend auf die Begründung zu § 28 Absatz 3 verwiesen.

Dem Bundesnachrichtendienst können nur Aufgaben und Befugnisse übertragen werden, die eine außen- und sicherheitspolitische Bedeutung haben und damit eine internationale Dimension aufweisen (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 127). Indes können dem Bundesnachrichtendienst als eigene Aufgabe auch die Früherkennung von aus dem Ausland drohenden Gefahren anvertraut werden, wenn diese eine hinreichend internationale Dimension aufweisen (BVerfG, a.a.O., Rn. 128). Gleiches muss für die hier in Rede stehende Befugnis nicht nur zur Aufklärung, sondern zur aktiven „Abwehr“ einer aus dem Ausland drohenden Gefahr mit einer hinreichend internationalen Dimension gelten, wenn diese von keiner anderen Behörde geleistet werden kann. Die von der Fallgruppe erfassten informationstechnischen Angriffe erfasst gerade die vom Bundesverfassungsgericht genannte Fallgruppe von außen gesteuerter Cyberangriffe (BVerfG, a.a.O., Rn. 128).

Die Befugnis schafft damit letztlich Raum für „Nothilfemaßnahmen“, wenn der Bundesnachrichtendienst gelegentlich seiner Aufklärung von Angriffsspuren im Server des Host-Providers auch Angriffstools oder dort gepufferte - womöglich noch nicht zum Angreifer weitergeflossene - Beutedaten feststellt. Eine solche Intervention in das Störungsgeschehen gehört nicht zum grundsätzlichen Aufgabenprofil des Nachrichtendienstes, sie stellt vielmehr eine Art der Nothilfe dar. Stellt der Bundesnachrichtendienst beispielsweise während einer Observation fest, dass die Zielperson eine andere Person angreift, ist legitim, dass die observierenden Mitarbeiterinnen oder Mitarbeiter des Bundesnachrichtendienstes oder

Personen ihrer Absicherung dem Opfer zu Hilfe eilen. Entsprechend verhält es sich vorliegend, wenn die gegenwärtige Gefahr nicht gleichermaßen wirksam durch eine polizeiliche Intervention zu beenden ist, was regelmäßig schon allein wegen des Zeitverzugs ausscheidet. In den Fällen des Absatzes 1 scheidet ebenso die Information des Host-Providers – zur Störungsbeseitigung durch diesen – aus, da die Maßnahme hier gerade verdeckt durchgeführt werden muss, um ihren Zweck nicht zu gefährden. Sofern die Löschung der Beutedaten – möglichst vor einem Abfluss – nicht gelingt, ohne den Zweck der Maßnahme zu gefährden, ist es ggf. möglich, für den Angreifer zumindest die Verwendbarkeit der Beutedaten einzuschränken, etwa durch ein Unkenntlichmachen der Daten.

Die Herstellung einer Sicherungskopie liegt grundsätzlich auch im fachlichen Interesse der Sachverhaltsauswertung, ist aber nach Satz 2 entbehrlich. Hintergrund ist, dass die Anfertigung einer solchen lagebedingt unter Umständen unpraktikabel sein kann, speziell wenn bei großen Datenmengen einer längerdauernde Verbindung nötig ist, die dem Angreifer zuglich die Ausforschung der vom Bundesnachrichtendienst genutzten Infrastruktur eröffnet oder bei groß angelegten Cyberangriffs-Kampagnen eine Vielzahl von Vorgängen in kürzester Zeit zu bearbeiten sind.

Zu § 37 (Erhebung von Daten aus informationstechnischen Systemen)

Der Zugriff auf und die Erhebung von Daten aus informationstechnischen Systemen ist für die Aufgabenerfüllung des Bundesnachrichtendienstes unverzichtbar. Diese Methodik zählt zum absoluten Standard der nachrichtendienstlichen Auslandsaufklärung weltweit. § 37 stellt eine Befugnisregelung für eingriffsintensive Maßnahmen dieser Art dar. Daneben sind auch weniger eingriffsintensive Maßnahmen des Zugriffs auf ein informationstechnisches System – auch mit damit verbundener Datenerhebung – denkbar, die nicht unter diese Regelung fallen, etwa wenn damit kein Eingriff in das IT-System-Grundrecht verbunden ist. In Abkehr vom bisherigen § 34 wird die Erhebung von Daten aus informationstechnischen Systemen mit dieser Neufassung des BND-Gesetzes weiter entsprechend der verfassungsrechtlichen Rechtsprechung ausgestaltet und die Rechtssicherheit und Rechtsklarheit für entsprechende Maßnahmen des Bundesnachrichtendienstes erhöht.

Nach wie vor ermöglicht der Zugriff auf informationstechnische Systeme angesichts der weltweit weiter zunehmenden Digitalisierung im Vergleich zu anderen nachrichtendienstlichen Mitteln die Erlangung zielgenauer Informationen und trägt daher wesentlich zur Bewältigung außen- oder sicherheitspolitischer Herausforderungen bei. Die mit diesen Maßnahmen erlangten Informationen leisten einen äußerst wichtigen Beitrag im Rahmen der Versorgung der Bundesregierung mit Informationen von außen- oder sicherheitspolitischer Bedeutung zur Früherkennung von Bedrohungen und der bundesdeutschen Sicherheitsarchitektur und spielt eine wichtige Rolle im Hinblick auf die Kooperationsfähigkeit des Bundesnachrichtendienstes.

Die mittels der in § 37 geregelten Maßnahmen erlangten Informationen können regelmäßig nicht durch ein milderes Mittel gewonnen werden, so nehmen beispielsweise parallel zum technologischen Fortschritt im Bereich der Digitalisierung und zunehmender Verbreitung die Möglichkeiten der Verschlüsselung signifikant zu. Es stehen heute etwa hochkomplexe, kaum lösbare Verschlüsselungsmethoden und -systeme jedermann zur Verfügung, so dass die Erhebung auftragsrelevanter Daten mit Mitteln der strategischen (Fernmelde-)Aufklärung in bestimmten Auftragsfeldern des Bundesnachrichtendienstes nur noch in stark reduziertem Maße möglich ist. Auch andere nachrichtendienstliche Mittel lassen regelmäßig die Erlangung solcher qualitativ hochwertigen und wichtigen Informationen nicht in vergleichbarem Maße zu.

Die Regelung ermächtigt den Bundesnachrichtendienst dazu, in ein informationstechnisches System einzugreifen (sog. Hacking) wie auch dazu, unter Nutzung von Zugangsdaten gegen den Willen des Berechtigten in ein informationstechnisches System einzugreifen, auch wenn hier nicht in gleicher Art und Weise die Integrität des Systems betroffen wird

(vgl. BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 180/23, Trojaner II, Rn. 227: wonach das IT-System-Grundrecht „jedenfalls“ bei einer auf diesem Weg - mittels des Zugriffs mit technischen Mitteln - erfolgenden Datenerhebung betroffen ist). Der Tatbestand der Vorschrift knüpft entsprechend nicht daran an, dass der Eingriff „mit technischen Mitteln“ erfolgt. Auch mittels der Nutzung einer Zugangskennung kann insbesondere bei cloudbasierten informationstechnischen Systemen „so zugegriffen [werden], dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können“ – vgl. BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Trojaner I Rn. 99, 124).

Von der Regelung ebenso umfasst ist auch der Fall, in dem der Bundesnachrichtendienst unter Zugriff auf die und ggf. Nutzung der Leistungen und Funktionalitäten des informationstechnischen Zielsystems dort erzeugte Daten erhebt. Von der Regelung nicht umfasst ist dagegen der Fall, wenn der Bundesnachrichtendienst sich nicht tatsächlich einen Zugriff auf das Zielsystem verschafft, mit dem er völlig eigenständig die Leistungen, Funktionen und Speicherinhalte nutzen kann. So ist etwa typischerweise das Versenden eines sogenannten Ping, eines Links oder Dokuments mit einer Trackingfunktion oder auch sogenanntes Phishing kein dieser Regelung unterfallendes Vorgehen.

Anders als die Vorgängerregelung des bisherigen § 34 orientieren sich die Vorgaben der einzelnen Absätze der Neufassung daran, wie eingriffsintensiv die jeweilige Maßnahme zu bewerten ist, etwa mit welcher Intensität die Maßnahme jeweils in Grundrechte eingreift und geben dementsprechend differenzierte materielle Voraussetzungen und differenzierte Verfahrenssicherungen vor. Nicht jede Befugnis, die in das IT-System-Grundrecht eingreift, ist an den strengen Anforderungen zu messen, die etwa für eine Online-Durchsuchung gelten. Vgl. BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Trojaner I, Rn. 124.

Bei dem Eingriff in informationstechnische Systeme handelt es sich um eine nachrichtendienstliche Vorgehensweise, bei der sich erst aus der konkreten Fallgestaltung ergibt, in welcher Intensität in Grundrechte der Betroffenen eingegriffen wird (a.a.O Trojaner I, Rn. 124). Der Eingriff in informationstechnische Systeme ist gerade im nachrichtendienstlichen Aufgabenbereich der weltweiten Vorfeldaufklärung von Bedrohungen geprägt durch eine Vielzahl denkbarer Anwendungsfälle und verschiedenartiger Sachverhalte. Dabei ist zu bedenken, dass nicht jedes informationstechnische System im technischen Sinn rechtlich in gleicher Art und Weise zu schützen ist. Dies ergibt sich bereits aus der Rechtsprechung des Bundesverfassungsgerichts zur Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07 und 1 BvR 595/07 (120, 274ff), vgl. hierzu insbesondere Rn. 202) und wird durch die jüngsten Entscheidungen des Bundesverfassungsgerichts (Trojaner I und Trojaner II) bestätigt und weiter ausgeführt. Bei der rechtlichen Einordnung der nachrichtendienstlichen Nutzung dieser Methodik kann daher nicht generell davon ausgegangen werden, dass mit dieser Methodik pauschal ein Grundrechtseingriff von höchstem Gewicht einhergeht.

Auch ist zu beachten, dass entsprechend der Feststellung des Bundesverfassungsgerichts in der Entscheidung vom 19. Mai 2020, 1 BvR 2835/17 (154, 152), Rn. 186) sich das Eingriffsgewicht in Grundrechte im Inland und Ausland unterscheiden kann. Die gesetzlichen Vorgaben für Eingriffe in informationstechnische Systeme bei einem Tätigwerden gegenüber Ausländerinnen oder Ausländern im Ausland können damit im Vergleich zu denen bei vergleichbaren Eingriffen in von Personen mit deutscher Staatsangehörigkeit oder sich im Bundesgebiet aufhaltenden Personen als eigene genutzte informationstechnische Systeme abgesenkt sein (vgl. Absatz 2 gegenüber Absatz 3).

Im Vergleich zur Vorgängerregelung wird hier aus systematischen Gründen auf den Zusatz „einschließlich Inhalte und Umstände der laufenden Kommunikation“ verzichtet und die Formulierung „zugreifen und dort verarbeitete personenbezogene Daten erheben“ verwendet. Mit dieser Formulierung umfasst die Regelung eindeutig sowohl gespeicherte Daten, wie auch laufende Kommunikation oder sonstige mittels der Leistungen oder Funktionalitäten

des informationstechnischen Systems – ggf. auch durch den Bundesnachrichtendienst veranlasst – erzeugte Daten.

Ebenso wurde auf die Formulierung „ohne Wissen des Betroffenen“ verzichtet. Dies aufgrund der systematischen Überlegung, dass es grundsätzlich dem Wesenskern nachrichtendienstlicher Mittel entspricht, dass selbige ohne Wissen der betroffenen Personen – heimlich – zur Anwendung kommen. Eine inhaltliche Bedeutungsänderung zur Vorgängerregelung ist damit nicht verbunden; die Heimlichkeit wird grundsätzlich bei den Befugnisnormen zur Anwendung nachrichtendienstlicher Mittel vorausgesetzt.

Zu Absatz 1

Absatz 1 regelt die Erhebung von personenbezogenen Daten mittels des Zugriffs auf informationstechnische Systeme, die mit großem Funktionsumfang, personenbezogene Daten vielfältiger Art erfassen und speichern können. Diese Systeme zeichnen sich dadurch aus, dass sie – allein oder in ihrer technischen Vernetzung - ein breites Spektrum von Nutzungsmöglichkeiten eröffnen, also eine Vielzahl von Nutzungsmöglichkeiten bieten, die mit der Erzeugung, Verarbeitung und Speicherung von (personenbezogenen) Daten verbunden sind (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07 und 1 BvR 595/07 (120, 274ff.), Rn. 178, 231 sowie bestätigend BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Trojaner I, Rn. 97).

Davon abzugrenzen sind informationstechnische Systeme, die nach ihrer technischen Konstruktion – und mangels entsprechender technischer Vernetzung – lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen enthalten („einfache“ informationstechnische Systeme). In einem solchen Fall reicht der Schutz durch das Recht auf informationelle Selbstbestimmung aus, um die Geheimhaltungsinteressen des Betroffenen zu wahren (vgl. BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07 und 1 BvR 595/07 (120, 274ff.), Rn. 202). Ein staatlicher Zugriff in solche Systeme unterscheidet sich also - auch wenn er mit technischen Mitteln durchgeführt wird - aus verfassungsrechtlicher Sicht qualitativ nicht von anderen nachrichtendienstlichen Datenerhebungen, die ebenfalls einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen.

Fallkonstellationen, in denen der Bundesnachrichtendienst in informationstechnische Systeme eingreift, die keine oder die nach deren technischer Konstruktion und mangelnder Vernetzung lediglich Daten mit punktuellem Bezug zu typischerweise einem Lebensbereich einer Person enthalten, jedenfalls also *keine* informationstechnischen Systeme sind, die mit großem Funktionsumfang personenbezogene Daten vielfältiger Art erfassen (komplexe informationstechnische Systeme) und so einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zulassen (Stichwort: „Gläserner Mensch“ - vgl. a.a.O., Rn. 203 sowie BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Trojaner I, Rn. 97) fallen nicht unter die Regelungen in dieser Norm. Die entsprechende Rechtsgrundlage findet sich dann in § 18.

Für die endgültige rechtliche Einordnung des Zielsystems spielt aber zusätzlich auch die Art der Nutzung eine entscheidende Rolle. Erst damit entscheidet sich, inwieweit alle weiteren Voraussetzungen erfüllt sind, um nach der Rechtsprechung des Bundesverfassungsgerichts vom sachlichen oder persönlichen Schutzbereich des IT-System-Grundrechts erfasst zu sein. Den Zielsystemen, die unter Absatz 1 fallen, fehlt es nämlich möglicherweise an der Nutzung dieser Systeme durch eine Person als eigenes, was zu einer Verarbeitung, insbesondere auch Speicherung, einer großen Vielzahl und auch Vielfalt an personenbezogenen Daten einer Person führt, die es ermöglichen, mit einem Zugriff ein aussagekräftiges Persönlichkeitsbild dieser Person zu erstellen (siehe dazu auch die Ausführungen nachfolgend zu Absatz 2).

Die Maßnahmen nach Absatz 1 zielen also nicht auf das Ausforschen eines von einer natürlichen Person zu ihrer privaten Lebensführung genutzten informationstechnischen

Endgeräts. Bei Maßnahmen im Sinne dieses Absatzes 1 handelt es sich vielmehr typischerweise um Eingriffe in anderen Staaten oder ausländischen juristischen Personen zuzurechnende informationstechnische Systeme. Also etwa Server oder auch Netzwerkelemente einer militärischen Einrichtung eines anderen Staates, aber auch sonstige dienstliche bzw. geschäftliche informationstechnische Systeme, die Mitarbeitenden zur Nutzung im beruflichen Kontext übertragen werden. Da es sich dabei grundsätzlich um komplexe informationstechnische Systeme handelt, können diese eine Vielzahl von personenbezogenen Daten verschiedener Personen enthalten, z.B. Namen und (typischerweise dienstliche / geschäftliche) Korrespondenz von Mitarbeiterinnen und Mitarbeitern in ausländischen staatlichen öffentlichen Stellen oder in Firmen. Das informationstechnische Zielsystem, nämlich beispielsweise der Server, den ein ausländischer Staat für die informationstechnischen Prozesse einer oder mehrerer seiner staatlichen Stellen nutzt, ist jedoch nicht vom Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erfasst. Staatliche Stellen sowie ausländische juristische Personen sind nicht grundrechtsberechtigt. Inländische juristische Personen können dagegen zwar grundsätzlich grundrechtsberechtigt sein, jedoch begründet sich die besondere Schwere der Eingriffe in informationstechnische Systeme in der einschlägigen Rechtsprechung des Bundesverfassungsgerichts aus der Möglichkeit der Erstellung eines umfangreichen Persönlichkeitsbildes einer Person. Diese besondere persönlichkeitsrechtliche Gefährdungslage ist mit Blick auf Unternehmen jedenfalls nicht in gleichem Maße gegeben.

Die von der Maßnahme im Rahmen ihrer Nutzung der dienstlichen oder geschäftlichen informationstechnischen Systeme mitbetroffenen Mitarbeiterinnen und Mitarbeiter sowie sonstige mitbetroffene Dritte sind – soweit von diesen überhaupt punktuelle personenbezogene Daten – im Zugriff der Maßnahme sind, lediglich in ihrem Grundrecht auf informationelle Selbstbestimmung betroffen. Eine Betroffenheit des IT-System-Grundrechts liegt nicht in dem Maße vor, wie wenn diese Personen das informationstechnische System als eigenes, selbstbestimmt zur ihrer privaten Lebensführung nutzen (vgl. dazu die Ausführungen zum nachfolgenden Absatz 2). Entsprechend der Lebens- und Behörden- bzw. Unternehmenswirklichkeit darf davon ausgegangen werden, dass die hier beschriebenen Zielsysteme im Regelfall durch Mitarbeitende oder durch sonstige Dritte nicht genutzt werden, um jeweils eigene persönliche Daten in einem solchen Umfang und breiten Spektrum zu verarbeiten wie z.B. auf einem zur privaten Lebensführung zu Hause genutzten privaten Personalcomputer oder dem privaten mobilen Endgerät. Typischerweise sind behördliche oder firmeneigene informationstechnische Systeme bis hin zu einem sogenannten Dienst-handy/Firmenhandy oder Dienst- bzw. Firmenlaptop durch entsprechende Vorgaben gerade einer umfangreichen Nutzung durch Mitarbeitende für deren eigene Persönlichkeitsentfaltung entzogen, sei es durch entsprechende Anweisungen, typischerweise häufig aber schon durch vorgenommene technische Einschränkungen seitens des Arbeitgebers. Dienstliche oder betriebliche informationstechnische Geräte sind typischerweise dadurch gekennzeichnet, dass der Mitarbeitende nicht selbstbestimmt darüber verfügen darf, so sind regelmäßig bestimmte Konfigurationen (Hardware oder Software), z.B. auch zur Nutzung oder Nichtnutzung bestimmter Apps, voreingestellt und vorgegeben, so dass hier keine selbstbestimmte Nutzung des Geräts erfolgen kann (vgl. zur selbstbestimmten Nutzung etwa BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07 und 1 BvR 595/07 (120, 274ff.), Rn. 206).Die Entfaltung der eigenen Persönlichkeit in ganzer Breite im virtuellen Raum (vgl. BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Trojaner I, Rn. 101) findet typischerweise nicht mittels dienstlicher oder geschäftlicher informationstechnischer Systeme statt. Jedenfalls reichen Überwachungsmaßnahmen dienstlicher oder geschäftlicher informationstechnischer Systeme nicht vergleichbar tief in das Privatleben hinein, wie die Überwachung eines privat genutzten Endgeräts, mit der Folge, dass ein staatlicher Zugriff unter geringeren Anforderungen zulässig ist (vgl. dazu a.a.O. Trojaner I, Rn. 126).

Einzelne personenbezogene Daten im Zusammenhang mit dem beruflichen Lebensbereich oder auch punktuelle private Korrespondenz sowie weitere einzelne personenbezogene Daten der Mitarbeitenden oder Dritter z.B. durch die Internetnutzung auf dem staatlichen oder dem firmeneigenen informationstechnischen System, vermögen indes keinen

erhöhten grundrechtlichen Schutzbedarf durch die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu begründen. Diese personenbezogenen Daten sind insbesondere durch das informationelle Selbstbestimmungsrecht oder auch durch Artikel 10 Absatz 1 des Grundgesetzes geschützt.

Im Rahmen der konkreten Maßnahme sind jedoch atypische Sachverhalte, z.B. der Eingriff in das informationstechnische System eines inländischen Einzelunternehmers, der sein informationstechnisches System dienstlich und zugleich auch als eigenes privates Endgerät zur persönlichen Lebensführung nutzt, in ihrer Atypik zu bewerten und entsprechend rechtlich einzuordnen. D.h. wird für den Bundesnachrichtendienst erkennbar, dass es sich um einen atypischen Fall handelt, in dem dienstliche informationstechnische Systeme von einer Person zugleich auch als eigene private informationstechnische Systeme genutzt werden, ist nach Absatz 4 zu verfahren.

Die Maßnahmen im Sinne des Absatzes 1 zeichnen sich aber dadurch aus, dass durch einen Eingriff in komplexe informationstechnische Systeme seitens des Bundesnachrichtendienstes jedenfalls potentiell eine größere Menge personenbezogener Daten einer Vielzahl von Personen erfasst werden können. Zwar wirken diese Maßnahmen nicht besonders grundrechtsintensiv mit Blick auf *eine* von der Maßnahme betroffenen (Ziel-)Person und durch die mangelnde Eigennutzung auch nicht grundrechtsintensiv mit Blick auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, dennoch wird aber hier - in Ansehung der potentiell mit dieser Maßnahme erfassbaren Menge an Daten - diese Maßnahme als eingriffsintensiv eingeordnet. Daher findet diese Maßnahme nur unter der erhöhten materiellen Schwelle der ersten Qualifikationsstufe statt. Anders als bei Maßnahmen der strategischen (Fernmelde-)Aufklärung handelt es sich jedoch um eine zielgenauere Maßnahme mit geringerer Streubreite, so dass hier die bei der strategischen Aufklärung auch im Rahmen der ersten Qualifikationsstufe vorgegebene Vorabkontrolle durch den Unabhängigen Kontrollrat nicht vorgesehen ist.

Der physische Belegenheitsort einzelner nachrichtendienstlicher Handlungen oder des informationstechnischen Zielsystems ist, insbesondere wenn sich um in Cloudsystemen betriebene informationstechnische Verarbeitungs- und Speichersysteme handelt, nicht maßgeblich. In anderen Fällen kann er ein Indiz für den Aufenthaltsort der betroffenen Zielperson sein. Deren Aufenthaltsort ist für die grundrechtliche Einordnung maßgebend, nicht jedoch der (häufig willkürliche) Speicherort von Daten.

Zu Absatz 2

Absatz 2 regelt den Eingriff in komplexe informationstechnische Systeme, die von einer Ausländerin oder einem Ausländer im Ausland (natürliche Person) als eigenes privat genutzt werden. Es geht also um informationstechnische Endgeräte, wie beispielsweise den als eigenen zur digitalen privaten Lebensführung genutzten (mobilen) Personalcomputer oder das als eigenes zur privaten Lebensführung genutzte Smartphone einer Person. Umfasst sind aber auch die Fälle, bei denen als informationstechnisches Endgerät zwar nicht ein physisches Objekt wie etwa ein Laptop genutzt wird, sondern beispielsweise Cloud-Computing zur digitalen privaten Lebensführung betrieben wird, die Person also anstelle eines Laptops vor Ort eine cloudbasierte Datenverarbeitung „als eigenes“ zur Erstellung und Speicherung sowie weiteren Verarbeitung ihrer vielfältigen privaten Daten nutzt.

Nach der Rechtsprechung des Bundesverfassungsgerichts ist für ein erhöhtes grundrechtliches Schutzbedürfnis durch das IT-System-Grundrecht neben dem Erfordernis der Komplexität des informationstechnischen Systems als zweite Komponente für die rechtliche Einordnung auch die Eigennutzung des informationstechnischen Systems von Bedeutung. D.h. eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht nur in den Fällen, in denen die betroffene Person das informationstechnische System ausschließlich oder überwiegend als eigenes nutzt und damit ein grundrechtlich besonders anzuerkennendes Vertraulichkeitsinteresse an den in seinem System erzeugten,

verarbeiteten und gespeicherten Daten hat – BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07 und 1 BvR 595/07 (120, 274ff.), Rn. 206. Denn nur aufgrund der Nutzung „als eigenes“ sind typischerweise im informationstechnischen System eine Vielzahl von Daten mit Bezug verschiedenen Lebensbereichen einer Person (persönliche Verhältnisse, soziale Kontakte, ausgeübte Tätigkeiten) enthalten, die weitreichend Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung zulassen (vgl. a.a.O. Rn. 178 sowie Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Trojaner I, Rn. 97, 124). Nutzt eine Person ein komplexes informationstechnisches System als eigenes, benutzt sie dieses typischerweise bewusst und unbewusst zum Speichern auch persönlicher Daten von gesteigerter Sensibilität, etwa in Form von Text-, Bild- oder Tondateien aus verschiedenen Lebensbereichen (vgl. BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07 und 1 BvR 595/07 (120, 274ff.), Rn. 231). Derartige Systeme können typischerweise personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten, so dass ein Zugriff auf das System es ermöglicht, einen Eindruck in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen, ein aussagekräftiges Bild der Persönlichkeit einer Person zu erhalten. Es handelt sich bei dem Zielsystem also um ein als eigenes genutztes informationstechnisches System mit großem Funktionsumfang, das personenbezogene Daten vielfältiger Art erfassen und speichern kann. Nicht umfasst sind hingegen beruflich oder dienstlich genutzte Geräte, auch wenn sie der betroffenen Person zur ausschließlichen Nutzung überlassen wurden und gelegentlich auch privat genutzt werden. Weder führt die gelegentliche private Nutzung eines Arbeitsgeräts dazu, dass dieses den strengen Anforderungen des Absatzes 3 unterfällt, noch führt die gelegentliche dienstliche Nutzung eines privaten Arbeitsgeräts dazu, dass dieses den strengeren Anforderungen des Absatz 3 entzogen wird.

Ferner können im Einzelfall Anhaltspunkte nahelegen, dass ein – vordergründig als privat eigengenutzt erscheinendes – informationstechnisches System oder auch eine virtuelle Maschine in einem System vornehmlich für Vorgänge im Zusammenhang mit Bedrohungen genutzt wird. Dann sind solche Systeme nicht als eigengenutzt private informationstechnische Systeme zu qualifizieren, denn insoweit führt gerade der aufklärungsveranlassende Sozialbezug nicht zu einer Ausforschung von zu schützender Privatheit. Beispielsweise statten fremde Mächte ihre Agenten oftmals mit spezieller Informationstechnik für ihre geheimdienstliche Tätigkeit aus, die auch nicht für (tatsächliche) private Zwecke genutzt werden darf, eine „private“ Nutzung stellt regelmäßig eine Legendenhandlung dar. Ähnliche Methoden der Absicherung klandestiner Operationen sind auch in „professionellen“ extremistischen und terroristischen Zusammenhängen realitätsnah. Durch die Aufklärung eines solchen informationstechnischen Systems ist kein aussagekräftiges Bild der Persönlichkeit einzelner Betroffener zu erhalten.

Absatz 2 legt die Voraussetzungen dafür fest, ein als eigenes privat genutztes informationstechnisches System vollumfänglich als Informationsquelle zur nachrichtendienstlichen Auslandsaufklärung nutzen zu dürfen (zu begrenzten Nutzungen: § 38). Solche Maßnahmen dürfen nur unter den Voraussetzungen der zweiten Qualifikationsstufe vorgenommen werden, da in diesen Fallkonstellationen auch bei einer Ausländerin oder einem Ausländer im Ausland von einem erhöhten grundrechtlichen Schutz ausgegangen wird. Die Ausgestaltung der gesetzlichen Befugnis in Absatz 2 trägt aber insbesondere im Vergleich zu den Regelungen in Absatz 3 dem Umstand Rechnung, dass die nachrichtendienstliche Maßnahme gegenüber einer Ausländerin oder einem Ausländer im Ausland ein geringeres Eingriffsgewicht aufweist. Diese Personengruppe unterliegt typischerweise nicht dem Zugriff deutscher Behörden und ist damit in deutlich verringertem Ausmaß Folgemaßnahmen ausgesetzt. Vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17 (154, 152), Rn. 186. Für die rechtliche Einordnung der Maßnahme ist damit maßgeblich, wer das komplexe informationstechnische System als eigenes nutzt; der Belegenheitsort einzelner nachrichtendienstlicher Handlungen oder beispielsweise des cloudbasierten informationstechnischen Systems ist dagegen nicht maßgeblich (s.o. am Ende zu Absatz 1).

Als verfahrensrechtliche Sicherung einer solchen Maßnahme des Bundesnachrichtendienstes erfolgt in diesen Fällen die Rechtmäßigkeitsprüfung durch den Unabhängigen

Kontrollrat als Vorabkontrolle vor der Durchführung der Maßnahme. Die Vorabkontrolle durch den Unabhängigen Kontrollrat (vgl. § 97) ersetzt für die Maßnahmen des Bundesnachrichtendienstes zur Auslandsaufklärung den Richtervorbehalt.

Zu Absatz 3

Absatz 3 regelt den Eingriff in bzw. den Zugriff auf komplexe informationstechnische Systeme, die von einem deutschen Staatsangehörigen oder einer sich im Bundesgebiet aufhaltenden Person als eigenes privat genutzt werden. Abzustellen ist dabei auf die Person des Nutzers / der Nutzerin sowie auf deren Aufenthaltsort. Der Ort, von dem aus – speziell beim sogenannten Cloud-Computing – die Datenverarbeitungsfunktionen angeboten werden (Belegenheitsort eines Servers), ist unerheblich (s.o. am Ende zu Absatz 1).

Derartige Maßnahmen dürfen nur unter den in diesem Absatz genannten Voraussetzungen vorgenommen werden. Bei dem Eingriff in komplexe, also mit einem großen Funktionsumfang ausgestattete, als eigene für die private Lebensführung genutzte informationstechnische Systeme mit ihrer typischerweise sehr breiten Datensammlung zu einer Person, handelt es sich um einen intensiven Grundrechtseingriff, der hohe Eingriffsvoraussetzungen erfordert.

Entsprechend der Ausführungen des Bundesverfassungsgerichts erlangt hier bereits die nachrichtendienstliche Maßnahme eine Intensität, die dazu führt, dass an die gesetzliche Ermächtigung grundsätzlich qualitativ vergleichbare Anforderungen wie an polizeiliche Befugnisnormen zu stellen sind (Nummer 1). Eine andere Betrachtung ist in verfassungskonformer Auslegung aufgrund der der Maßnahme eigenen Intensität, die für sich bereits das Risiko einer weitgehenden staatlichen Ausspähung der Persönlichkeit birgt, nicht möglich. Dass Bundesnachrichtendienst und Polizeibehörden unterschiedliche Aufgaben und Befugnisse haben und in der Folge Maßnahmen mit unterschiedlicher Eingriffstiefe vornehmen können, ist für die rechtliche Gewichtung des heimlichen Zugriffs auf das informationstechnische System grundsätzlich ohne Belang, vgl. dazu BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17 (162), Rn. 166, 168; BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07 und 1 BvR 595/07 (120, 274ff.) Rn. 242, 254.

In Nummer 2 ist festgelegt, dass der Bundesnachrichtendienst nur tätig wird, wenn eine gleichwertige Maßnahme einer zuständigen Polizeibehörde nicht oder nicht rechtzeitig möglich ist. Ein gleichwertiges Handeln einer Polizeibehörde kann beispielsweise auch dann nicht (rechtzeitig) möglich sein, wenn der Bundesnachrichtendienst die die Maßnahme begründenden Informationen von einem ausländischen Partnerdienst erhalten hat und diese nicht an Polizeibehörden weitergeben darf (Third Party Rule), eine Aufklärung der Bedrohung aber dennoch zum Schutz der besonders gewichtigen Rechtsgüter der Bundesrepublik Deutschland und ihrer Bürgerinnen und Bürger geboten ist.

Ferner sieht der Gesetzgeber in Satz 2 vor, dass ein Zugriff des Bundesnachrichtendienstes auf informationstechnische Systeme von sich im Bundesgebiet aufhaltenden deutschen Staatsangehörigen oder sich im Bundesgebiet aufhaltenden Ausländerinnen/Ausländern einen Ausnahmefall darstellt, der an besondere Voraussetzungen geknüpft ist. Damit ist sichergestellt, dass deutsche Staatsangehörige oder andere Personen, die ihren Aufenthaltsort im Inland haben, mit ihren informationstechnischen Geräten nicht ohne Weiteres Ziel einer auslandsnachrichtendienstlichen Aufklärungsmaßnahme werden. Das Ziel der Aufklärungsmaßnahme ist auch bei einem Tätigwerden des Bundesnachrichtendienstes gegenüber deutschen Staatsangehörigen oder anderer sich im Bundesgebiet aufhaltenden Personen immer die Früherkennung und Aufklärung von Bedrohungen aus dem Ausland und trifft daher nur Personen, bei denen ein besonderer Bezug zu einer aus solchen Bedrohungen erwachsenden konkretisierten Gefahr besteht. Eine grenzüberschreitende Tätigkeit im Sinne dieser Regelung können etwa die Tätigkeit für einen fremden Nachrichtendienst oder eine fremde Macht, aber auch Auslandskontakte und -aufenthalte oder

Auslandsreisetätigkeiten sein, wenn und solange die aufzuklärende Gefahr in unmittelbarem Zusammenhang mit dieser Tätigkeit steht.

Als verfassungsrechtlich geforderte verfahrensrechtliche Sicherung dieser Aufklärungsmaßnahme des Bundesnachrichtendienstes erfolgt in diesen Fällen die Rechtmäßigkeitsprüfung durch den Unabhängigen Kontrollrat als Vorabkontrolle vor der Durchführung der Maßnahme. Die Vorabkontrolle durch den Unabhängigen Kontrollrat (vgl. § 97) ist insoweit für die Maßnahmen des Bundesnachrichtendienstes zur Auslandsaufklärung (das Ziel der Maßnahme ist auch bei einem Tätigwerden gegenüber einem deutschen Staatsangehörigen oder einer sich im Bundesgebiet aufhaltenden Person die Auslandsaufklärung) *die funktionale Entsprechung des Richtervorbehaltes* (vgl. hierzu umfassend zu § 29). Für die hier in Rede stehenden Vorschriften der technischen Aufklärung mittels Zugriffen in informationstechnische Systeme gilt dabei die Erwägung, dass der Unabhängige Kontrollrat regelmäßig über ein weit umfangreicheres Wissen verfügen wird – zumal unter Einbeziehung technischer Experten des administrativen Kontrollorgans – als ein Richter eines ordentlichen Gerichts.

Die Befugnis solche Maßnahmen auch gegenüber deutschen Staatsangehörigen oder einer sich im Bundesgebiet aufhaltenden Person durchzuführen, ist eine Erweiterung gegenüber den bisherigen Befugnissen des Bundesnachrichtendienstes. Diese Erweiterung schließt eine Lücke, die die wirksame Erfüllung des gesetzlichen Aufklärungsauftrags des Bundesnachrichtendienstes bislang beschränkt hat. Es war ohne diese Befugnis nur eingeschränkt möglich, dem gesetzlichen Auftrag nachzukommen, da es auch Inländerinnen oder Inländer sowie deutsche Staatsangehörige im Ausland gibt, die in einem Sachverhaltskomplex agieren, der der Auslandsaufklärung und damit dem gesetzlichen Aufklärungsauftrag des Bundesnachrichtendienstes zuzurechnen ist. Beispiele für solche Sachverhaltskomplexe sind Agenten fremder Mächte, die ein europäisches Spionagenetzwerk unterhalten und sich zeitweise dafür auch im Bundesgebiet aufhalten, deutsche Jihadisten im Ausland oder deutsche Staatsangehörige, die in Tätigkeiten der Sanktionsumgehung verstrickt sind. In solchen Fällen ist es faktisch so, dass ausländische Partnerdienste entsprechende Maßnahmen ohne Kenntnis des Bundesnachrichtendienstes gegen Personen im Bundesgebiet oder mit Bezug zu deutschen Staatsangehörigen im Ausland durchführen und gegebenenfalls von sich aus dem Bundesnachrichtendienst bedeutsame Erkenntnisse übermitteln. Das Fehlen einer eigenen Befugnis für solche Maßnahmen führte also zu einer erheblichen Einbuße an staatlicher Souveränität bei der nachrichtendienstlichen Aufklärung von Bedrohungen aus dem Ausland. Ferner verminderte es auch wesentlich die Kooperationsfähigkeit des Bundesnachrichtendienstes mit europäischen Partnern in paneuropäischen Bedrohungsszenarien, da der Bundesnachrichtendienst keinen Beitrag bei der Aufklärung von Teilvorgängen dieser Sachverhalte im Bundesgebiet oder mit Bezug zu deutschen Staatsangehörigen leisten konnte, dies aber im Rahmen von Kooperationen typischerweise gerade erwartet wird. Die Erweiterung der Befugnis für den Bundesnachrichtendienst führt daher zu dem Ergebnis, dass deutsche Sicherheitsbehörden gerade bei Bedrohungsszenarien im Inland oder mit Beteiligung von deutschen Staatsangehörigen nunmehr nicht mehr in so hohem Maße wie bisher auf Interventionen ausländischer Partner angewiesen sind.

Zu Absatz 4

Die Einordnung des Zielsystems in die einzelnen Absätzen dieser Norm (oder, wenn es sich um ein einfaches informationstechnisches System handelt, unter die Grundnorm nachrichtendienstlicher Datenerhebungen in § 18) geregelten Kategorien erfolgt anhand tatsächlicher Anhaltspunkte vor Durchführung der Maßnahme. So kann beispielsweise davon ausgegangen werden, dass es sich um ein dienstliches bzw. geschäftliches Mobiltelefon handelt, wenn die zugehörige Telefonnummer im Internetauftritt der Behörde bzw. des Unternehmens veröffentlicht ist. Aufgrund tatsächlicher Anhaltspunkte kann also eine Prognoseentscheidung getroffen werden, wobei die der erforderlichen Prognose zugrunde liegenden Anknüpfungspunkte typischerweise auch eine Unschärfe aufweisen können.

Absatz 4 trägt daher dem Umstand Rechnung, dass bei Durchführung der Maßnahme Erkenntnisse gewonnen werden können, die die ursprüngliche Bewertung anhand der zunächst zugrunde gelegten tatsächlichen Anhaltspunkte ändern. So kann beispielsweise die Konfiguration des Zielsystems Hinweise auf eine rein oder ganz wesentlich private Nutzung des Zielsystems als eigenes zur privaten Lebensführung geben. Auch kann sich herausstellen, dass sich zwar dienstliche Informationen auf dem infiltrierten System befinden, dessen Nutzung für private Belange de facto aber deutlich überwiegt. Hierbei geht es nicht um eine rein quantitative Betrachtung, erforderlich ist vielmehr eine Bewertung des jeweiligen nutzerorientierten Schwerpunkts. Diese Feststellung gilt analog für Akteure, die sich im strafbewährten Bereich – wie z.B. Terrorismus oder Schleuseraktivitäten – bewegen und im Rahmen dieser Tätigkeit mobile Endgeräte nutzen.

Insofern stellt dieser Absatz sicher, dass Maßnahmen, bei denen für den Bundesnachrichtendienst erst in deren Durchführungsverlauf erkennbar wird, dass es sich um eine andere Fallkonstellation handelt, als bei Beginn der Maßnahme aufgrund der Umstände des Einzelfalls angenommen, nur fortgesetzt werden, wenn die materiellen Voraussetzungen der jeweils zum vorgefundenen Zielsystem passenden Regelung vorliegen. In diesem Fall hat der Bundesnachrichtendienst (falls es aufgrund der gesetzlichen Bestimmungen erforderlich ist) dem Unabhängigen Kontrollrat schnellstmöglich eine Anordnung vorzulegen. Bis zu deren Bestätigung darf er die bereits erhobenen Daten nicht (weiter) auswerten oder anderweitig nutzen. Sofern der Unabhängige Kontrollrat die Anordnung nicht bestätigt, hat der Bundesnachrichtendienst die erhobenen Daten unverzüglich zu löschen.

Zu § 38 (Abgegrenzte Erhebung von Daten aus informationstechnischen Systemen)

Es handelt sich hier um die Befugnis für eine gegenständlich beschränkte Datenerhebung aus den in einem informationstechnischen System erzeugten, verarbeiteten oder gespeicherten Daten. Die Befugnis eröffnet die Möglichkeit einer teilweisen Informationserhebung aus dem Zielsystem unter gegenüber § 37 abgesenkten Voraussetzungen, insbesondere regelt § 38 die sogenannte Quellen-Telekommunikationsüberwachung (bisher in § 11a des Artikel 10-Gesetzes geregelt). Daneben umfasst der Anwendungsbereich der Regelung des § 38 auch andere gegenständlich beschränkte Eingriffe, die ähnlich gewichtig sind - erst recht jedoch auch weniger gewichtige, ggf. enger begrenzte Zugriffe als derjenige begrenzt auf Telekommunikation.

Nach der Rechtsprechung des Bundesverfassungsgerichts (Beschluss vom 24. Juni 2025, 1 BvR 2466/19 „Trojaner I“ sowie Beschluss vom 24. Juni 2025, 1 BvR 180/23 „Trojaner II“) ist nicht jeder Eingriff in den Schutzbereich des IT-System-Grundrechts an den strengen Anforderungen zu messen, die etwa für eine Online-Durchsuchung gelten; vielmehr ist für das insoweit zu berücksichtigende Eingriffsgewicht insbesondere maßgeblich, welche Daten letztlich im Rahmen der konkreten Maßnahme genutzt werden dürfen (a.a.O. Trojaner I Rn. 124). Es wirkt eingriffsmindernd, wenn nicht alle auf einem informationstechnischen System erzeugten, verarbeiteten und gespeicherten oder von dort aus zugänglichen Daten vollständig überwacht werden (a.a.O. Trojaner II, Rn. 199).

Zu Absatz 1

Absatz 1 regelt die Eingriffsschwelle für abgegrenzte Eingriffe in informationstechnische Systeme, die durch das IT-System-Grundrecht geschützt sind. Er entkoppelt den auf bestimmte Daten beschränkten und damit gegenüber eines Zugriffs mit der vollumfänglichen Erhebung aller Daten eines informationstechnischen Systems weniger gewichtigen Eingriff in das IT-System-Grundrecht von den besonders strengen materiellen Voraussetzungen, wie sie in § 37 Absatz 2 oder 3 vorgegeben sind. Maßgeblich ist dabei, dass die Maßnahme nicht darauf zielt, das Informationspotenzial eines als eigenes privat genutzten informationstechnischen Systems durch Erkenntnisse über die Vielzahl und Vielfalt der Daten der privaten Lebensführung des Nutzers auszuschöpfen, sondern nur bestimmte Sachverhalte

oder Lebensvorgänge aufklären soll und der Bundesnachrichtendienst dabei auch nur die dazu erforderlichen Daten nutzen darf (siehe Absatz 3 Satz 2).

Absatz 1 regelt das Tätigwerden des Bundesnachrichtendienstes gegenüber Ausländern im Ausland wie auch das Tätigwerden gegenüber deutschen Staatsangehörigen und sich im Bundesgebiet aufhaltenden Personen, soweit es sich diesen gegenüber *nicht* um eine sogenannte Quellen-Telekommunikationsüberwachung oder eine vergleichbar gewichtige sektorale, also jedenfalls nicht umfassende Datenerhebung des gesamten Datenbestandes eines privat genutzten informationstechnischen Systems, und damit gegenständlich beschränkte Maßnahme handelt. Die Quellen-Telekommunikationsüberwachung gegenüber deutschen Staatsangehörigen und sich im Bundesgebiet aufhaltenden Personen sowie die begrenzte Erhebung von Daten, die vergleichbar gewichtige Einblicke in die Lebensführung ermöglichen oder ihrer Art nach höchstprivat sind, sind in Absatz 2 geregelt. Vgl. dazu die Ausführungen zu Absatz 2.

Ein Beispiel für einen gegenständlich begrenzten (abgegrenzten) Eingriff ist die Erhebung einer thematisch abgrenzbaren Datei, wie etwa allein der Kontaktdaten („Adressbuch“) auf einem informationstechnischen System. Ein weiteres Beispiel für einen solchen gegenständlich begrenzten Eingriff ist etwa die Erhebung nur solcher Daten (z.B. technischer Spuren) auf einem privat genutzten informationstechnischen System, die in Verbindung mit einem informationstechnischen Angriff stehen etwa, weil das informationstechnische System im Rahmen eines solchen Angriffs z.B. als Bot genutzt wurde. Möglich wäre weiter auch die ausschließliche Erhebung von Zugangsdaten. Auch denkbar ist, dass nur solche Daten, die im Zusammenhang mit einer hybriden Einflussnahme angefallen sind, erhoben werden.

Zu Absatz 2

Als besonders gewichtigen beschränkten abgegrenzten Eingriff, der gleichwohl aber hinter dem Gewicht einer vollumfänglichen Maßnahme nach § 37 Absatz 2 oder 3 zurückbleibt, ist in Nummer 1 leitbildhaft die Telekommunikationsüberwachung (in der Form der Quellen-Telekommunikationsüberwachung) genannt (a.a.O. Trojaner II; Rn. 199).

Die Quellen-Telekommunikationsüberwachung im Sinne dieser Regelung ist als schwerwiegender Eingriff sowohl in das IT-System-Grundrecht als auch in Artikel 10 Absatz 1 des Grundgesetzes zudem an die - im Vergleich zur herkömmlichen Telekommunikationsüberwachung - zusätzliche Vorgabe gebunden, dass anderenfalls die Erforschung des Sachverhaltes auf andere Weise aussichtslos oder wesentlich erschwert wäre (vgl. a.a.O. Trojaner II, Rn. 200) – siehe § 39 Absatz 1 Satz 1.

Zu Weiterverarbeitung laufender Telekommunikation im Sinne des Artikel 10 Absatz 1 des Grundgesetzes siehe die Regelungen in § 64 Absatz 1 (Kennzeichnung) und § 66 Absatz 4 Nummer 2 (Löschung).

Zu Nummer 1

Absatz 2 sieht hier eine erhöhte Eingriffsschwelle bei einem gegenständlich beschränkten Eingriff gegenüber deutschen Staatsangehörigen oder sich im Bundesgebiet aufhaltenden Personen vor, soweit es sich um Maßnahmen der Überwachung der (laufenden) Telekommunikation oder vergleichbar gewichtige Maßnahmen handelt.

Zu Nummer 2

Zu Buchstabe a

Als besonders gewichtigen gegenständlich beschränkten Eingriff, der gleichwohl aber hinter dem Gewicht einer vollumfänglichen Maßnahme nach § 37 Absatz 2 oder 3

zurückbleibt, ist unter Buchstabe a die Telekommunikationsüberwachung (in der Form der Quellen-Telekommunikationsüberwachung) benannt (a.a.O. Trojaner II, Rn. 199).

Zu Weiterverarbeitung laufender Telekommunikation im Sinne des Artikel 10 Absatz 1 des Grundgesetzes siehe die Regelungen in § 64 Absatz 1 (Kennzeichnung) und § 66 Absatz 4 Nummer 2 (Löschung).

Zu Buchstabe b

Buchstabe b regelt, dass auch einer Telekommunikationsüberwachung vergleichbar gewichtige Eingriffe in die private Lebensführung gegenüber deutschen Staatsangehörigen oder sich im Bundesgebiet aufhaltenden Personen unter die erhöhten Voraussetzungen des Absatz 2 fallen. Es handelt sich hier um eine abstrakt gehaltene Regelung, die angesichts der Vielgestaltigkeit in Betracht kommender Sachverhalte des gegenständlich begrenzten Eingriffs in ein informationstechnisches System angemessen erscheint. Die Telekommunikationsüberwachung bildet dabei den heranziehbaren Vergleichsmaßstab.

Zu Absatz 3 und Absatz 4

Absätze 3 und 4 treffen ergänzende Verfahrensmaßgaben. Für die in Absatz 3 verankerte Pflicht sicherzustellen, dass nur diejenigen Arten von Daten aus denjenigen abgegrenzten Teilen der Datenverarbeitung des informationstechnischen Systems erhoben werden, auf die die Maßnahme zielt, ist zu berücksichtigen, dass dies einer Erhebung von solchen Daten nicht entgegensteht, die aus faktischen Gründen zwingend erhoben werden müssen, um die Maßnahme durchzuführen. Die Ausnahmeregelung in Satz 2 lehnt sich an die Regelung zum Kernbereichsschutz an (§ 21 Absatz 5), die sogar für derart sensible Bezüge Standard der Bundesgesetzgebung ist (vgl. auch ständige Rechtsprechung, z.B. BVerfGE 162, 1, Rn. 284). Danach sind verfügbare informationstechnische Sicherungen einzusetzen, jedoch eröffnet die Befugnis eine bedarfsangepasste Flexibilität, da sich diese Sicherung technisch nicht durchgängig abbilden lässt. Demgemäß enthält Satz 1 ein Prinzip als zu optimierende Grundregel, die aber nach Satz 2 offen für sachbedingte Ausnahmen ist (Einsatz verfügbarer Werkzeuge).

Zu § 39 (Vorgaben für die Erhebung von Daten aus informationstechnischen Systemen)

Die Regelung enthält weitere Vorgaben zur Durchführung des Zugriffs auf informationstechnische Systeme nach §§ 36, 37 und 38. Vorgaben zur Kennzeichnung finden sich in § 64 Absatz 2 Satz 3 und zur Löschung in § 66 Absatz 4 Nummer 2.

Zu Absatz 1

Soweit es sich um eine nachrichtendienstliche Maßnahme nach § 37 Absatz 2 oder 3 handelt, darf sie nur durchgeführt werden, wenn die Aufgabenerfüllung ansonsten aussichtslos oder wesentlich erschwert wäre und sich nur gegen den in diesem Absatz genannten Personenkreis richten. Es handelt es sich hier um einen gesondert geregelten Fall des Einsatzes eines nachrichtendienstlichen Mittels gegen eine Person (vgl. zur allgemeinen Regelung des Einsatzes eines nachrichtendienstlichen Mittels gegen eine Person § 20). Ziel der Maßnahme ist zwar ein komplexes informationstechnisches System, rechtlich abzustellen ist aber auf die Eingriffswirkung hinsichtlich der Person, die dieses informationstechnische System als eigenes privat nutzt. Da es sich hier um eine spezielle, in besonderer Art und Weise in die Persönlichkeitsrechte des Betroffenen eingreifende Maßnahme handelt, ist in § 39 Absatz 1 die Voraussetzung für die gegen eine Person gerichtete Maßnahme zur Erhebung gespeicherter Daten aus informationstechnischen Systemen im Sinne von § 37 Absatz 2 oder 3 gesondert – vorrangig gegenüber der Grundnorm des § 20 – geregelt.

Für die Nummer 2 wird auf die Begründung zu § 13 Absatz 2 Nummer 3 Bezug genommen. Auch hier ist ein Zusammenhang mit dem Aufklärungsziel, der Grund zu der Annahme gibt,

dass die Maßnahme zur Aufklärung erforderlich ist, insbesondere dann gegeben, wenn sich die Maßnahme gegen Nachrichtenmittlerinnen oder Nachrichtenmittlern richtet, wobei auch die unbewusste oder nicht-willentliche Mitteilung entsprechender Nachrichten umfasst ist, oder die Maßnahme auf ein bedrohungsunterstützendes Netzwerk abzielt.

Zu Absatz 2

Absatz 2 berücksichtigt, dass ein Eingriff in ein informationstechnisches System typischerweise aufgrund der Vielzahl und Vielfalt dort verarbeiteter Daten verschiedene Personen betroffen sein können. Auf einem komplexen informationstechnischen System können personenbezogene Daten einer Vielzahl von Personen gespeichert sein, welche somit durch den Eingriff mitbetroffen sein. Es können personenbezogene Daten von Personen, auch solchen mit deutscher Staatsangehörigkeit, von Inländerinnen oder Inländern oder auch inländischen juristischen Personen, auf dem Zielsystem aus einer Vielzahl von Gründen gespeichert sein, z.B. als Personaldatum eines Mitarbeitenden, als Adressliste von Korrespondenzpartnern, als im Herrschaftsbereich des Empfängers abgespeicherte E-Mail oder sonstige gespeicherte Korrespondenz eines Kommunikationspartners, als Vertragsinhalt, als Notiz etc. Hierbei handelt es sich personenbezogene Daten, die dem informationellen Selbstbestimmungsrecht unterfallen und deren weitere Verarbeitung unter Berücksichtigung der Regelungen des §§ 52ff. zulässig ist.

Eine Drittbetroffenheit im Sinne dieses Absatzes kann auch im Hinblick auf die Daten in einem anderen informationstechnischen System oder dessen Integrität bestehen, wenn die Maßnahme nicht über einen direkten Eingriff in das relevante informationstechnische System umsetzbar ist, sondern ein Vorschritt notwendig ist. Dies ist beispielsweise der Fall, wenn der Zugriff auf den Server eines extremistischen oder terroristischen Netzwerks erst durch ein Passwort erlangt werden kann, welches zuvor auf dem informationstechnischen System des Netzwerkadministrators erhoben werden muss. Ein anderes Beispiel ist die Nutzung fremder IT-Systeme als notwendiges Zwischenziel, um Schutzmechanismen des informationstechnischen Zielsystems zu umgehen (sog. „Jump-Hosts“).

Satz 2 stellt klar, dass die Maßnahme nur dann erfolgen darf, wen der mit ihr verfolgte Zweck nicht erkennbar außer Verhältnis zum Nachteil für den oder die Betroffenen steht.

Zu Absatz 3

Die in Absatz 3 enthaltenen Regelungen entsprechen im Wesentlichen dem bisherigen § 34 Absatz 4. Sie gelten für alle Maßnahmen der Eingriffe in informationstechnische Systeme gleichermaßen; indes nur, wenn der Einsatz durch technische Mittel (und nicht z.B. durch eine nachrichtendienstliche Verbindung) erfolgt.

Ferner entspricht die Regelung im Wesentlichen den vergleichbaren Vorschriften in § 11 Absatz 1a des Artikel 10-Gesetzes und § 100a Absatz 5 der Strafprozessordnung. Eine Modifikation erfolgt dabei insoweit, als dass die „technische Befähigung“ des eingesetzten Mittels zur Erfassung von (nur) zulässigen Inhalten nicht länger eine Tatbestandsvoraussetzung ist. Dies ist dem Umstand geschuldet, dass aufgrund der fortschreitenden technischen Veränderungen und der besonderen Schwierigkeiten eines Einsatzes eines nachrichtendienstliche Mittels praktische Hürden reduziert werden müssen. Zudem ist zu berücksichtigen, dass der Bundesnachrichtendienst auch befugt ist, andere als diese Daten auf einem Endgerät zu erheben, sodass es nicht zweckdienlich wäre, auf technischer Ebene zwei verschiedene Eingriffsinstrumente vorhalten zu müssen. Damit ist allerdings keine Schlechterstellung der betroffenen Personen verbunden.

Nummer 1 enthält die bisherige Regelung, dass an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenverarbeitung unerlässlich sind. Hierbei sind auch solche Veränderungen zulässig, die die Erhebung von entschlüsselten Daten ermöglichen.

Nummer 2 stellt klar, dass (nur) solche Veränderungen rückgängig gemacht werden müssen, die die Integrität des IT-Systems beeinträchtigen, und eine Veränderung unterbleiben kann, falls tatsächliche Anhaltspunkte dafür vorliegen, dass hierdurch der Zweck der Maßnahme gefährdet würde. Letzteres wäre z.B. dann anzunehmen, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Rückgängigmachung von dem Betroffenen wahrgenommen werden könnte. Beispiel für diese Regelung sind solche Veränderungen, die von Natur aus temporär begrenzt sind und deren aktive Beseitigung auf dem informationstechnischen System ein höheres Risiko der Entdeckung birgt.

Darüber hinaus findet sich in Nummer 2 nunmehr die Möglichkeit, eine Veränderung zunächst dann nicht rückgängig zu machen (sondern gleichsam „ruhend zu stellen“), wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Veränderung zu einem späteren Zeitpunkt erneut (aus-)genutzt werden soll. So könnten etwa Hinweise vorliegen, dass durch eine geplante Aktualisierung der Zugriff auf das informationstechnische System auffallen könnte. In diesem Fall kann es zielführend sein, ihn vorübergehend ruhend zu stellen. Außerdem kann es aus Verhältnismäßigkeitsgründen geraten sein, erst nur eine Teilmenge zu erheben und diese zu analysieren, währenddessen den Zugang jedoch ruhend zu stellen, um einer Entdeckung zuvorzukommen. Wenn die erhobene Datenmenge darauf hinweist, dass eine weitere Erhebung gewinnbringend sein wird, kann der Zugang wieder aktiviert werden. Ein komplett neuer wiederholter Ansatz zum Zugriff begegnete mindestens den Schwierigkeiten und Risiken des Erstzugriffs, wäre ggf. sogar schwieriger zum Erfolg zu bringen. Denn Verbringungsmethoden lassen sich in der Regel nicht oder nur unter Inkaufnahme eines erheblichen operativen und persönlichen Risikos replizieren. Ist beispielsweise eine Art von Mitwirkung des Betroffenen erforderlich, sinkt die Erfolgswahrscheinlichkeit mit der Anzahl der Versuche. Auch könnte die bisher genutzte Schwachstelle im informationstechnischen Zielsystem zwischenzeitlich geschlossen worden sein.

Zu Absatz 4

In Absatz 4 findet sich eine weitere der sog. „Annex-Befugnisse“, welche zur informationsbeschaffenden Tätigkeit des Bundesnachrichtendienst außerhalb des Abschnittes 4 hinzutreten und es ihm ermöglichen, eine unmittelbar bevorstehende Gefahr, deren Abwehr durch keine andere Behörde geleistet werden kann, abzuwehren. Insbesondere im Bereich der Cyber-Angriffe, bei der Angreifer oft die Systeme argloser Nutzer befallen und diese für ihre Angriffe nutzen, ist ein schnelles Einschreiten zum Schutz der Opfer und der Eigentümer solch zweckentfremdeter Systeme von großer Bedeutung. Der Bundesnachrichtendienst muss in der Lage sein, die Angriffe umzulenken, durch aktives Einwirken zu beenden und nötigenfalls die angreifenden Systeme (bzw. die zweckentfremdeten Geräte) vollständig abzuschalten. Insbesondere bei letztgenannter Variante wird der Verhältnismäßigkeitsgrundsatz – welcher normativ erneut klargestellt wird – streng zu beachten sein. Ergänzend wird auf die Begründung zu § 28 Absatz 3 Bezug genommen.

Zu Absatz 5

Die Regelung stellt klar, dass auch im Bereich der Erhebung von personenbezogenen Daten aus informationstechnischen Systemen – wie bei der Durchführung anderer nachrichtendienstlicher Maßnahmen auch – eine gemeinsam mit anderen Stellen durchgeführte Operation möglich ist. Eine gleichberechtigt gemeinsam durchgeführte nachrichtendienstliche Maßnahme bedingt naturgemäß, dass die gleichberechtigt erhobenen Daten dem ungefilterten, gleichzeitigen Zugriff der beteiligten Stellen unterliegt. Umfasst sind sowohl inländische wie auch ausländische öffentliche Stellen.

Zu § 40 (Datenerhebung durch eine ausländische öffentliche Stelle)

Die Regelung übernimmt im Wesentlichen die Regelungen des bisherigen § 28. Im Rahmen der BND-Gesetzesnovelle (BT-Drs. 19/26103) wurde das Kooperationsregime für Maßnahmen der strategischen Ausland-Fernmeldeaufklärung bereits eingeführt. Nun werden dort

geregelte Grundsätze entsprechend der Neukonzeption des BND-Gesetzes auch auf die Maßnahmen der Telekommunikationsüberwachung sowie auf Maßnahmen zur Erhebung von gespeicherten Daten aus informationstechnischen Systemen übertragen, um für den Bundesnachrichtendienst auch in Bezug auf diese technischen Maßnahmen einen rechtssicheren Handlungsrahmen für Kooperationen zu schaffen.

Auch im Bereich der Telekommunikationsüberwachung oder der Aufklärungsmaßnahmen durch Zugriff auf informationstechnische Systeme sollen die zur Verfügung stehenden Kapazitäten auch ausländischer Nachrichtendienste genutzt werden, um eine effektive Ausnutzung vorhandener Kapazitäten zu gewährleisten (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 243 im Zusammenhang mit Kooperationen im Bereich der strategischen Fernmeldeaufklärung). Gerade im Zusammenhang mit diesen Maßnahmen ist die Arbeitsteilung und Zusammenarbeit mit ausländischen Nachrichtendiensten angesichts vielfältiger, komplexer Bedrohungen und knapper Ressourcen unabdingbar. Die internationale Kooperationsfähigkeit des Bundesnachrichtendienstes ist von zentraler Bedeutung. Bei allen technischen Maßnahmen nach diesem Unterabschnitt ist eine Zusammenarbeit mit ausländischen Nachrichtendiensten im gesamten Spektrum der nachrichtendienstlichen Bedrohungen besonders wichtig, da ansonsten ein Ausschluss aus den auch perspektivisch immer relevanter werdenden internationalen Kooperationsformaten im Bereich der technischen Aufklärung droht.

Absatz 2 entspricht dem geltenden Recht, welches terminologisch – der allgemeinen Systematik folgend – insoweit angepasst wurde, als nunmehr auf die „Weiterverarbeitung“ und Übermittlung abgestellt wird. Dies ist dem Umstand geschuldet, dass die (Erst-)Erhebung gerade nicht durch den Bundesnachrichtendienst erfolgte, sondern durch die ausländische öffentliche Stelle. Zwar gelten insoweit für die Erhebung die Vorgaben des BND-Gesetzes (vgl. Absatz 4), sodass eine Umgehung von tatbestandlichen Voraussetzungen ausgeschlossen ist, dies macht die Erhebung indes in rechtlicher Hinsicht (etwa im Rahmen von § 31 Absatz 3) nicht zu einer Erhebung des Bundesnachrichtendienstes.

Gestrichen wurde dabei in Absatz 3 das vormalige Regelungssystem für die Verwendung von Suchbegriffen des Bundesnachrichtendienstes durch ausländische Partner. Diese Regelungen waren in der Praxis faktisch nicht durchsetzbar und wurde entsprechend entfernt. Der Austausch von Suchbegriffen ist der Zusammenarbeit immanent und wird entsprechend von der allgemeinen Befugnis mitumfasst.

Absatz 4 enthält die (neu geschaffene) Vorgabe der Einbindung der Behördenleitung für Maßnahmen der Telekommunikationsüberwachung oder der Erhebung von gespeicherten Daten aus informationstechnischen Systemen durch eine ausländische öffentliche Stelle auf Ersuchen des Bundesnachrichtendienstes, um der Eingriffsintensität der Maßnahme gerecht zu werden. Hierbei handelt es sich um ein Ersuchen, da der Bundesnachrichtendienst keine Kenntnis davon hat, wie der ausländische Partner genau die jeweilige Maßnahme durchführen wird. Satz 2 stellt klar, dass ein solches Ersuchen nur möglich ist, wenn die Voraussetzungen für die jeweilige Maßnahme auch vorliegen. Insoweit wird sichergestellt, dass auch im Falle der Einbindung einer ausländischen Stelle die gesetzlichen Voraussetzungen zur Durchführung einer solchen Maßnahme durch den Bundesnachrichtendienst gewährleistet werden. Dies schließt eine mögliche vorherige Feststellung der Rechtmäßigkeit der Maßnahme durch den Unabhängigen Kontrollrat nach § 97 ein.

Zu § 41 (Kooperation mit ausländischen öffentlichen Stellen bei der technischen Aufklärung)

Die Regelung übernimmt im Wesentlichen die Regelungen des bisherigen § 31 Absatz 1 bis 3; enthält aufgrund der Neufassung des BND-Gesetzes jedoch Folgeanpassungen. So beziehen sich die Regelungen nunmehr auch auf die Telekommunikationsüberwachung sowie die Aufklärungsmaßnahmen nach §§ 37 und 38. Ebenso wird bei der

Übernahme des bisherigen § 31 Absatz 3 die Legaldefinition der erheblichen Bedrohungen in § 3 Absatz 1 berücksichtigt.

Kooperationen dürfen Kommunikationsdaten mit qualifizierten Inlandsbezug grundsätzlich nicht umfassen. Sollte es im Rahmen der Kooperation zu einer Übermittlung von Kommunikationsdaten mit qualifiziertem Inlandsbezug gekommen sein – etwa, weil dies für den Bundesnachrichtendienst nicht erkennbar war –, so ist der Kooperationspartner unverzüglich zur Löschung der Daten aufzufordern. Ausnahmsweise ist es gemäß Absatz 2 Satz 2 – wie auch im Rahmen der Regelungen zur strategischen Aufklärung selbst – gleichwohl zulässig, in bestimmten Fällen auch Kommunikationsdaten mit qualifiziertem Inlandsbezug in die Kooperation aufzunehmen.

Die Absätze 5 und 6 entsprechen den bisherigen § 32 Absatz 2 und Absatz 4. Sie wurden, da es sich um allgemeine Vorgaben für die Kooperationen des Bundesnachrichtendienstes handelt, nunmehr in die „allgemeine“ Vorschrift des § 41 verschoben. Zudem wurde in Absatz 6 klargestellt, dass die dortige Vorgabe – dies ist aufgrund der Gesetzessystematik geltendes Recht – (nur) im Rahmen von Kooperationen gilt.

Zu § 42 (Absichtserklärung für Kooperationen mit ausländischen öffentlichen Stellen bei der technischen Aufklärung)

Die Regelung übernimmt im Wesentlichen die Regelungen des bisherigen § 31 Absatz 4 bis 7.

In Absatz 1 findet sich in Nummer 3 Buchstabe c eine Anpassung dahingehend, dass auch die Möglichkeit einer Verstrickung nach § 22 Absatz 2 Berücksichtigung findet. Dabei obliegt die Entscheidung, ob es sich um eine „nicht-schützenswerte“ Person handelt, nicht dem ausländischen Partner, sondern schon aus Gründen der Rechtssicherheit dem Bundesnachrichtendienst. Die explizite Regelung ist insoweit klarstellend. Die Anpassung in Buchstabe h) – Verlängerung des Zeitraums auf zwölf Monate – ist der Verlängerung der Speichermöglichkeiten für Metadaten geschuldet. Es wird auf die Begründung zu § 66 Absatz 4 Nummer 1 verwiesen.

Der Wortlaut der in Absatz 2 genannten Kooperationszwecke wird als Folgeanpassung an die Formulierungen in den erheblichen und herausgehobenen Bedrohungen in §§ 3 und 4 angeglichen. Eine wesentliche inhaltliche Änderung geht damit und der Anpassung der Reihenfolge nicht einher, so dass bereits abgeschlossene Absichtserklärungen keiner Änderung bedürfen; siehe dazu auch die Regelung in § 140. Eine rein redaktionelle Änderung ist dabei auch die der Wegfall des Wortlauts zur Früherkennung von Gefahren; dass das allgemeine Ziel der Auslandsaufklärung die Früherkennung von Bedrohungen für besonders gewichtige Rechtsgüter ist, ist einleitend nunmehr bereits in § 2 Absatz 1 verankert. Insbesondere bleibt die Möglichkeit erhalten, auch andere – qualitativ vergleichbare – Kooperationszwecke zu setzen (siehe Nummer 11 und vgl. bisher § 31 Absatz 5 Nummer 11). Neu abzuschließende Absichtserklärungen richten sich nach dem nunmehr gültigen Wortlaut des Absatz 2.

Absatz 4 wird im Sinne einer Verfahrensstraffung vereinfacht. Zustimmungsebenen innerhalb des Bundeskanzleramtes werden nunmehr nicht länger auf gesetzlicher Ebene geregelt.

Mit Absatz 5 wird eine Regelung für den Eilfall eingeführt. Insbesondere im Bereich der hier geregelten Fälle der technischen Aufklärung ist es denkbar, dass Maßnahmen mit Kooperationspartnern sehr schnell durchgeführt werden müssen, z.B. zur Aufklärung eines Cyberangriffs. Insofern ist es in diesen Fällen ausreichend, dass die Voraussetzungen der Kooperation im Bereich des Eingriffs in informationstechnische Systeme den Kooperationspartnern vor Abschluss einer Absichtserklärung mitgeteilt werden und diese die Einhaltung dieser Vorgaben bestätigen. Dies ist durch den Bundesnachrichtendienst in geeigneter

Weise zu dokumentieren. Die formale und schriftliche Abfassung der Absichtserklärung erfolgt dann im Nachgang.

Zu § 43 (Übermittlung von selektierten Kommunikationsdaten im Rahmen von Kooperationen zur strategischen Aufklärung)

Die Überschrift der §§ 43 bis 44 wurden gegenüber den bisherigen Regelungen (§§ 32 bis 33) angepasst. Einerseits um klarzustellen, dass es sich bei den Kooperationsvorschriften letztlich um (besondere) Übermittlungsbefugnisse handelt (entsprechend wurde der Wortlaut der Vorschriften auch angepasst, sodass nunmehr einheitlich die „Übermittlung“ geregelt ist). Andererseits, da durch die Aufnahme von Telekommunikationsüberwachung und Aufklärungsmaßnahmen nach §§ 37 und 38 in die Kooperationsregime nunmehr eine Klarstellung erforderlich war, welche Vorschriften sich auf die strategische Aufklärung beziehen.

Die Änderung des Absatz 1 Satz 1 stellt klar, dass – der neuen Systematik der strategischen Aufklärung folgend – nur Kommunikationsdaten (also kommunikationsbezogene Inhalts- und Metadaten) Gegenstand der Regelung sind. Sonstige im Wege der strategischen Aufklärung erhobene personenbezogene Daten können (nur) nach § 41 Absatz 1 übermittelt werden. Auch Absatz 1 Satz 2 bis 4 wird gegenüber der bisherigen Regelung geändert. Der Bundesnachrichtendienst selektiert Daten auch anhand sogenannter „weicher“ Suchbegriffe wie Ländervorwahlen etc. Mit dieser Änderung können Verkehrsdaten nach dieser Norm verarbeitet werden, die anhand von Suchbegriffen mit einem höheren Abstraktionsgrad selektiert wurden. Satz 4 gilt nur für solche Suchbegriffe, die zur Erhebung von Inhaltsdaten verwendet werden, für diese gilt das ergänzende Kriterium der hinreichenden Bestimmtheit. Es wird somit unterschieden zwischen Suchbegriffen, die zur Erhebung von Inhaltsdaten genutzt werden und Suchbegriffen, die zur Selektion bei der Verkehrsdatenerfassung genutzt werden und die nicht bestimmt genug sind, um die Voraussetzungen des § 33 Absatz 3 zu erfüllen wie z.B. die Landeskenner bei Telefonnummern.

Die Übermittlung von mittels der genannten „weichen“ Suchbegriffe selektierten Verkehrsdaten ist weniger eingriffsintensiv als die unselektierte Übermittlung von Verkehrsdaten gemäß § 44 und auch als die Übermittlung von selektierten Inhaltsdaten nach § 43. Insofern ist eine Abgrenzung dieser Fälle von der unselektierten Übermittlung nach § 44 und die Absenkung des Maßstabs für die hinreichende Bestimmtheit gegenüber Suchbegriffen zur Erhebung von Inhaltsdaten (die Suchbegriffe müssen zwar geeignet und erforderlich, aber nicht hinreichend bestimmt sein) zulässig.

Die in Absatz 3 geregelten Ausnahmen von der Zulässigkeit einer automatisierten Übermittlung von selektierten Daten bleiben bestehen, werden aber terminologisch an die neue Systematik angepasst. Dabei gilt weiterhin, dass eine Filterung anhand der Kriterien (nur) erfolgen muss, soweit dies technisch möglich ist.

Die ehemaligen Absätze 2 und 5 konnten entfallen, da diese Vorgaben nun in der allgemeinen Vorschrift für Kooperationen enthalten ist (vgl. oben). Ebenso konnte Absatz 8 entfallen, da infolge der neuen Systematik der strategischen Aufklärung nunmehr eine Speicherung der erhobenen Daten im für einen begrenzten Zeitraum ohnehin möglich ist.

Zu § 44 (Übermittlung unselektierter kommunikationsbezogener Metadaten im Rahmen von Kooperationen bei der strategischen Aufklärung)

Der bisherige § 33 wurde an die neue Systematik des BND-Gesetzes angepasst (nunmehr Katalog erheblicher Bedrohungen in § 3 auf den in § 44 Absatz 2 Nummer 1 verwiesen wird). Es handelt sich hier wie bisher auch um eine Sonderform der Kooperation, die insoweit selbstverständlich auch das Vorliegen der allgemeinen Voraussetzungen für Kooperationen voraussetzt.

Die Durchführung von Kooperationen im Bereich der Ausland-Fernmeldeaufklärung mit ausländischen Nachrichtendiensten ist Teil des do-ut-des-Prinzips und zeichnet sich

dadurch aus, dass der Bundesnachrichtendienst für einen ausländischen Nachrichtendienst zur Erreichung der Kooperationsziele Fernmeldeaufklärung betreibt. Die Informationsbedarfe des ausländischen Nachrichtendienstes sind – bedingt durch dessen anders gelagerten gesetzlichen Auftrag, andere Interessensschwerpunkte und Aufklärungsziele - nicht zwingend in Gänze deckungsgleich mit denen des Bundesnachrichtendienstes. Aus diesem Grund wurde die Bindung der Kooperation an die strategischen Aufklärungsmaßnahmen des Bundesnachrichtendienstes gelöst.

Besondere Voraussetzung dieser Regelung ist dabei nach wie vor das Ziel, konkreten Bedrohungen entgegenzuwirken und die Handlungsfähigkeit diesbezüglich zu sichern.

Die qualifizierten Aufklärungsbedarfe unterliegen weiterhin einer Anordnungspflicht und der Vorabkontrolle.

Zu § 45 (Übermittlung personenbezogener Daten im Rahmen von Kooperationen zur Telekommunikationsüberwachung oder der Erhebung gespeicherter Daten aus informationstechnischen Systemen)

Hier werden Regelungen zur Verarbeitung personenbezogener Daten bei Kooperationen zur Telekommunikationsüberwachung oder der Erhebung gespeicherter Daten aus informationstechnischen Systemen getroffen. Anders als bei Kooperationen im Rahmen der strategischen Aufklärung wird hierbei nicht zwischen „selektierten“ oder „unselektierten“ Daten unterschieden (vgl. oben § 43 und § 44). Hintergrund dieser Regelungen sind Vorgaben des Bundesverfassungsgerichts speziell zu der Verarbeitung von Daten aus der strategischen Aufklärung. Diese besonderen Vorgaben knüpft das Bundesverfassungsgericht daran, dass die Daten aus einer strategischen Aufklärung stammen, also nicht aus einer Maßnahme, die sich wie die in § 42 in Bezug genommenen Maßnahmen auf ein hinreichend bestimmtes Ziel richtet. Die besonderen Regelungen aus der strategischen Aufklärung sind daher nicht pauschal übertragbar.

Zu Absatz 1

Absatz 1 beinhaltet die Befugnis des Bundesnachrichtendienstes, personenbezogene Daten im Rahmen von Kooperationen mit ausländischen Nachrichtendiensten zu verarbeiten. Die Übermittlung ist nur zulässig, wenn sie erforderlich ist, um die in der Absichtserklärung mit dem Kooperationspartner vereinbarten Kooperationszwecke zu erreichen.

Zu Absatz 2

Die personenbezogenen Daten dürfen den Kooperationspartnern unverzüglich zur jeweils eigenen Weiterverarbeitung automatisiert übermittelt werden. Insbesondere bei Maßnahmen zur Erhebung gespeicherter Daten aus informationstechnischen Systemen können die Daten auch auf sonstige Weise zugänglich gemacht werden, d.h. beispielsweise der direkte und unmittelbare Zugang zu einem dem Bundesnachrichtendienst zuzurechnenden Ablageort gewährt werden - der modus operandi kann sich hierbei in den jeweiligen Einzelfällen aufgrund praktischer und operativ-sicherheitlicher Bedürfnisse stark unterscheiden. Eine vorherige Prüfung oder Filterung der Daten ist nicht erfolgen, da es sich um Daten aus vorab angeordneten und hinreichend bestimmten Zielen handelt und der Kooperationsrahmen des § 42 die Einbindung der Datenverarbeitung in einen rechtsstaatlichen Rahmen absichert (vgl. dazu BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 247 sowie Rn. 259ff. im Zusammenhang mit Kooperationen im Bereich der strategischen Fernmeldeaufklärung). Es handelt sich hierbei um eine spezielle Übermittlungsregelung im Rahmen von Kooperationen, andere Regelungen zur Übermittlung von Daten sind nicht einschlägig.

Um sicherzustellen, dass im Rahmen von Eingriffen nach § 37 Absatz 3 die verfassungsgerichtlichen Vorgaben zur Weiterverarbeitung von Daten aus Maßnahmen der sog. „Online-Durchsuchung“ gegenüber Inländern/Deutschen nicht unterlaufen werden, ist eine

Übermittlung nur zulässig, wenn auch im Zeitpunkt der Übermittlung die erhebungsrechtfertigende konkretisierte Gefahr besteht.

Zu Unterabschnitt 4 (Anordnungen)

In Unterabschnitt 4 finden sich die Vorgaben für diejenigen Maßnahmen, welche einer vorherigen Anordnung durch die Behördenleitung (bzw. einer Vertretung) bedürfen. Diese Anordnungen haben zwei Funktionen: Einerseits sorgen sie für eine behördeninterne Kontrollmöglichkeit und stellen sicher, dass eine Mehrfachprüfung der Rechtmäßigkeit bereits durch den Bundesnachrichtendienst selbst erfolgt. Außerdem bilden sie den Ausgangspunkt für die Rechtmäßigkeitsprüfung durch den Unabhängigen Kontrollrat.

Anordnungen können mündlich und schriftlich ergehen. Dabei wird aufgrund des Umfangs und der Komplexität der erforderlichen Ausführungen im Regel eine schriftliche Anordnung erforderlich sein. Ergehen sie aber (etwa bei Gefahr im Verzug) mündlich, sind sie umgehend in Schriftform abzufassen, um sie einer späteren Kontrolle zugänglich zu machen.

Es können verschiedene Anordnungen miteinander „kombiniert“ werden. Nicht erforderlich ist es, für verschiedene Maßnahmen jeweils eigene Anordnungen zu treffen. Dies gilt auch, wenn verschiedene Maßnahmearten vorliegen; insbesondere können Maßnahmen nach § 46 und nach § 48 miteinander verbunden werden.

Zu § 46 (Anordnung des Einsatzes nachrichtendienstlicher Mittel)

Die Regelung führt querschnittliche Vorgaben zu Anordnungen zusammen. Ein Schrifterfordernis besteht für Anordnungen (insgesamt) nicht. Bei Gefahr im Verzug kann der Bundesnachrichtendienst die Anordnung für sofort durchführbar erklären (vgl. hierzu das Gesetz über die Rechtskontrolle durch den Unabhängigen Kontrollrat (UKRatG). Der Beginn der Laufzeit der Anordnungen kann sich auch auf einen Zeitpunkt, der dem Erlass der Anordnung vorgelagert ist, beziehen.

Zu Absatz 1

Absatz 1 legt die Anordnungszuständigkeit für die in diesem Abschnitt geregelten eingriffsintensiven Maßnahmen fest, worunter neben den eingriffsintensiven nachrichtendienstlichen Mitteln, welche konkret in Unterabschnitt 2 geregelt sind, auch der besondere (eingriffsintensive) Einsatz nachrichtendienstlicher Mittel nach § 19 fällt. Zuständig ist die Behördenleitung des Bundesnachrichtendienstes oder eine von ihr bestimmte Vertretung. Die Vorschrift trifft keine unmittelbare Regelung dazu, bis zu welcher Granularität eine Delegation der Zuständigkeit im Einzelnen zulässig ist – dies bleibt grundsätzlich dem Bundesnachrichtendienst vorbehalten, wobei sicherzustellen ist, dass dies im Ergebnis einer Person von gesteigerter Verantwortung verbleibt. Regelmäßig setzt dies die Entscheidung einer Direktoratsleiterin oder eines Direktoratsleiters voraus.

Zu Absatz 2

Absatz 2 legt die notwendigen Inhalte der Anordnung des Einsatzes eingriffsintensiver nachrichtendienstlicher Mittel fest.

Nach Satz 1 Nummer 1 sind im Fall einer gegen eine Person oder eine Personengruppe gerichteten Maßnahme nach § 20, soweit möglich, Name und Anschrift der Person anzugeben. Sind Name und Anschrift nicht bekannt, kann die Angabe folglich entfallen. Dies gilt nicht für Maßnahmen, die gegen eine mögliche oder bereits bestehende nachrichtendienstliche Verbindung durchgeführt werden. Einer Offenlegung dieser Daten stehen sowohl sicherheitliche Gründe als auch die schutzwürdigen Interessen der betroffenen Person entgegen.

Die Dauer der Maßnahme nach Satz 1 Nummer 2 ist die maximale Laufzeit des konkreten Einsatzes eines nachrichtendienstlichen Mittels, bei einer Observation beispielsweise sechs Wochen, die Befristung der Maßnahme nach Satz 1 Nummer 3 in Verbindung mit Absatz 3 dagegen ist der zeitliche Rahmen, innerhalb derer das nachrichtendienstliche Mittel eingesetzt werden darf, im Falle der Observation beispielsweise zwischen dem 1. Oktober und dem 31. Dezember eines Jahres. In Nummer 4 findet sich, dem § 46 Absatz 5 Nummer 5 des Bundeskriminalamtsgesetzes nachgebildet, die im Rahmen der Anordnung einer Wohnraumüberwachung erforderlichen Angaben zur überwachten Wohnung. In Nummer 5 ist festgelegt, dass die Anordnung zu begründen ist.

Zu Absatz 3

Absatz 3 regelt die Befristung der Anordnung. Die Anordnung gibt den erforderlichen Einsatz eines nachrichtendienstlichen Mittels für einen bestimmten Zeitraum frei. Hiervon zu unterscheiden ist die Durchführung der Maßnahme, die einsatztaktischen und situativen Gesichtspunkten folgt, etwa wie eine Maßnahme durchführbar ist und wann sie wertige Erkenntnisse erwarten lässt. Eine Anordnung kann also beispielsweise lauten, dass in den kommenden sechs Monaten Observationen gegen eine bestimmte Person auch länger als 48 Stunden (aber weniger als eine Woche) durchgeführt werden dürfen. Die Einsatzentscheidung wird dann in dem mit der Anordnung eröffneten Einsatzrahmen nach operativen Erfordernissen in den dazu zuständigen Organisationseinheiten getroffen. Dort ist auch über eine vorfristige Beendigung zu entscheiden.

Entsprechend der jeweiligen Gewichtung des Eingriffs und in Abwägung mit praktischen Erwägungen (letzteres insbesondere bezüglich Nummer 1) folgt auch die Befristung einem gestuften System, bei der die Wohnraumüberwachung (als besonders eingriffsintensives Instrument) auf einen Zeitraum von maximal einem Monat zu befristen ist.

Verlängerungen sind möglich, die Dauer der Verlängerung richtet sich gleichermaßen nach dem gestuften System.

Zu Absatz 4

Absatz 4 bestimmt die Voraussetzungen, zu denen eine Maßnahme in jedem Fall zu beenden ist, obwohl die in Absatz 3 genannte Frist noch nicht verstrichen ist. Dies ist (in Nummer 2 und 3) letztlich Ausfluss des Grundsatzes der Verhältnismäßigkeit, wonach eine Maßnahme nicht länger erforderlich und angemessen ist, wenn der Zweck der Maßnahme erreicht ist oder nicht länger erreicht werden kann.

Zu Absatz 5

Absatz 5 enthält die (neue) Möglichkeit, dass Anordnungen einen (gesondert zu begründenden und zu prüfenden) Zusatz enthalten, nach dem die Maßnahme auch gegen andere Personen gerichtet werden kann. Ergänzend wird auf die Ausführungen zu § 17 Absatz 4 verwiesen.

Zu Absatz 6

Absatz 6 regelt die Dokumentation von Anordnung und Durchführung. Zur Begründung der Anordnung gehören auch Angaben, die die Erforderlichkeit der Maßnahme erschließen, also einerseits Erkenntnisbedarf und Erkenntnisziele des Einsatzes sowie andererseits Eignung des Einsatzes und ggf. sonstige Zugangslage. Die Durchführungsdokumentation muss nicht gesondert erfolgen, sondern kann sich mit den angefallenen Materialien erschließen. Nach dem Grundsatz der Wirtschaftlichkeit (§ 7 BHO) sind Dokumentationsaufwände möglichst gering zu halten. Bei technischen Maßnahmen sind jedenfalls Beginn und Ende festzuhalten.

Zu § 47 (Anordnungen im Zusammenhang mit strategischen Aufklärungsmaßnahmen)

Die Regelung entspricht in ihrem Regelungsgegenstand dem bisherigen § 23, enthält indes eine Reihe von nachfolgend dargestellten Veränderungen und greift insbesondere die veränderte Systematik der gesetzlichen Grundlagen der strategischen Aufklärung auf. Die Überschrift der Vorschrift verdeutlicht, dass es nicht nur um Anordnungen von strategischen Aufklärungsmaßnahme geht, sondern dass auch die „Sonderanordnungen“ in den Absätzen 4 und 6 Berücksichtigung finden.

Nicht Gegenstand der Anordnung – und damit auch nicht Gegenstand der Vorabkontrolle – sind einzelne Telekommunikationsteilnehmer und ihnen zugeordnete Telekommunikationsmerkmale oder sonstige Suchbegriffe. Diese müssen zwar die Voraussetzungen des § 33 Absatz 3 erfüllen, also insbesondere im Hinblick auf das in der Anordnung durch das gerichtsähnliche Kontrollorgan des Unabhängigen Kontrollrats als erhebliche Bedrohung bestätigte Aufklärungsthema bestimmt, geeignet und erforderlich sein; die diesbezügliche Prüfung obliegt indes dem Bundesnachrichtendienst selbst bzw. der nachgelagerten einer etwaigen Kontrolle durch das administrative Kontrollorgan des Unabhängigen Kontrollrates.

Zu Absatz 1

In Absatz 1 ist zunächst – wie auch im Rahmen der übrigen Anordnungsvorschriften – geregelt, dass die Anordnung durch die Behördenleitung des Bundesnachrichtendienstes oder einer von ihr bestimmten Vertretung zu erfolgen hat. Auf die obigen Ausführungen zu § 46 Absatz 1 wird insoweit verwiesen.

Zu Absatz 2

Die Anordnung bedarf nicht länger zwingend der Schriftform (hierzu schon oben). Insbesondere aufgrund des abstrakten Charakters von Anordnungen zur strategischen Aufklärung wird hier jedoch eine schriftliche Anordnung die Regel sein.

Den Veränderungen in der Systematik der gesetzlichen Grundlagen der strategischen Aufklärung entsprechend sind im Rahmen der erforderlichen Angaben für die Anordnung von strategischen Aufklärungsmaßnahmen zur Vorabkontrolle künftig angepasste Angaben zu machen. Die Würdigung des Aufklärungsthemas bleibt dabei weiterhin die Grundlage der Vorabkontrolle durch den Unabhängigen Kontrollrat, jedoch insbesondere unter Berücksichtigung der neuen Schwellensystematik. In aller Regel werden beide Stufen der Datenerhebung (ersten Stufe der Datenerhebung als Erhebung im engeren Sinne) und die zweite Stufe (Einsichtnahme in erhobene Daten) in einer einheitlichen Anordnung angeordnet werden, schon weil eine Erhebung von Daten ohne die Möglichkeit einer späteren Einsichtnahme nur ausnahmsweise einen Nutzen bringen wird.

Zu Nummer 1

Es sind weiterhin die Angaben des bisherigen § 26 Absatz 2 Nummer 2 bis 4 aufzunehmen, also das Aufklärungsthema (Buchsstabe a) und soweit gesetzlich vorgesehen der geographische Fokus (Buchsstabe b).

Das Aufklärungsthema rekurriert auf die vom Bundesverfassungsgericht statuierte Pflicht einer inhaltlichen Begrenzung der Erhebung (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 179) Dabei sind die vom Bundesverfassungsgericht festgelegten Kautelen („Erkenntnisziele“ bzw. „aufzuklärende Art der Gefahr“) unbestimmt. Damit die notwendige Begrenzung Wirkung entfaltet, darf das Aufklärungsthema vom Bundesnachrichtendienst nicht ohne weitere Konturierung gewählt werden. So wäre etwa ein Aufklärungsthema "Bedrohungen in Asien“ ungeeignet, da es eine kontinentweite Erhebung zu allen möglichen, sehr unterschiedlichen Themenbereichen zulassen würde. Zugleich kann ein Aufklärungsthema auch nicht so eng verstanden werden, dass die final angeleitet auf die

Früherkennung (also gerade auch potentiellen Nährboden einer Bedrohung in den Blick nehmende Aufklärung) von Bedrohungen für besonders gewichtige Rechtsgüter gerichtete strategische Aufklärungsmaßnahme zu einem individuellen Instrument würde. So wäre etwa das Aufklärungsthema „Wirken von Boko Haram im Nordosten Nigerias“ oder „Proliferation durch geheimdienstliche Strukturen in Russland“ deutlich zu eng gefasst. Sachgerecht wäre etwa eine strategische Aufklärungsmaßnahme, welche (als Beispiel für eine territoriale, also geographisch abgrenzbare Maßnahme) für die „Bedrohungen durch Staat X“ oder für die „ Bedrohungen durch die krisenhafte Entwicklungen in Staat oder Region X“ gilt, oder (als Beispiel für eine globale Maßnahme idR ohne geographischen Fokus, hierzu nachfolgend) die „Bedrohungen durch den Islamistischen Terrorismus und Fundamentalismus“ oder die „Bedrohungen durch den Internationalen Rauschgifthandel“ zum Gegenstand hat.

Im Rahmen der Begründung der Anordnung ist hinsichtlich des Aufklärungsthemas weiter auszuführen, weshalb bezüglich dieses Themas eine Früherkennung von Bedrohungen für besonders gewichtige Rechtsgüter geboten ist (siehe hierzu auch Ausführungen zu Nummer 2). Hierfür wird regelmäßig darzulegen sein, dass eine Bedrohung für eines oder mehrere besonders gewichtige Rechtsgüter bereits eingetreten ist oder realistischerweise im weiteren Verlauf mit der Manifestierung einer solchen Bedrohung gerechnet werden kann. Dabei ist sicherzustellen, dass die aufzuklärende Bedrohung stets auch der angeordneten Maßnahme unterfällt – so wäre es etwa unzulässig, eine mögliche Bedrohung der außenpolitischen Handlungsfähigkeit der Bundesrepublik im Rahmen einer strategischen Aufklärungsmaßnahme aufzuklären, wenn die zugehörige Aufklärungsmaßnahme keinen Bezug zur außenpolitischen Handlungsfähigkeit enthält. Es ist nicht erforderlich, dass eine Bedrohung für ein besonders gewichtiges Rechtsgut inhaltlich weiter unterteilt wird; so ist es etwa nicht erforderlich, dass bei einer für ein Aufklärungsthema einmal festgestellten Bedrohung für ein oder mehrere besonders gewichtige Rechtsgüter, wie etwa der hybriden Einflussnahme, noch weiter danach differenziert werden muss, ob und inwiefern diese Bedrohungen durch bestimmte Handlungen oder Umstände eingetreten sind oder wahrscheinlich eintreten werden, wie etwa Einflussnahmen auf europäische Nachbarstaaten, durch direkte hybride Maßnahmen oder sonstige Propaganda. Vergleichbar wäre bei einer Bedrohung für das besonders gewichtige Rechtsgut Leib und Leben im Rahmen einer strategischen Aufklärungsmaßnahme zum „Islamistischen Terrorismus und Fundamentalismus“ nicht erforderlich, die Bedrohung für einzelne Terrorgruppen differenziert darzustellen. In der jeweiligen Anordnung einer strategischen Maßnahme können aber derartige Einzel- oder Teilsachverhalte zur Verdeutlichung der Bedrohung herangezogen werden.

Die Notwendigkeit zu Angaben zum geographischen Fokus des Aufklärungsthemas entfällt, wenn tatsächliche Anhaltspunkte bestehen, dass eine geographische Fokussierung nicht sinnvoll möglich ist. Hiervon werden insbesondere solche Bedrohungen erfasst, die sich aufgrund ihres globalen Charakters einer regionalen Einordnung entziehen, wie etwa globale Cyberbedrohungen, weltweit vernetzte Terrornetzwerke und der internationale Drogenhandel, aber auch Daten, die der Bundesnachrichtendienst zur Eigenbefähigung flächendeckend benötigt, wie Informationen zu eingesetzter Telekommunikationstechnik im Ausland. Die Möglichkeit einer solchen Befreiung von der Notwendigkeit einer geographischen Fokussierung folgt aus der Rechtsprechung des Bundesverfassungsgerichts, das Angaben zum geographischen Fokus „in der Regel“ für notwendig erachtet, insoweit also Raum für die nunmehr geregelten Ausnahmen belässt (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 179).

Zu Nummer 2

In Nummer 2 finden sich die nunmehr notwendigen Angaben zu der zweiten Stufe der Datenerhebung; der Einsichtnahme in die personenbezogenen Daten. Die Anordnung einer strategischen Aufklärungsmaßnahme befugt den Bundesnachrichtendienst auch zur Einsichtnahme in personenbezogene Daten, wobei gleichermaßen eine Einsichtnahme

„unmittelbar nach Erhebung“ als auch eine Einsichtnahme zu einem späteren Zeitpunkt vom Rahmen der neuen Speicherbefugnis umfasst ist.

Die vormals gesetzlich angelegte Unterscheidung zwischen der politischen Unterrichtung und der Früherkennung von Bedrohungen ist nicht länger vorgesehen, da der Erhebungszweck der „politischen Unterrichtung“ nicht länger im Gesetz enthalten ist. Insoweit ist in Entsprechung der bundesverfassungsgerichtlichen Rechtsprechung (BVerfG, Beschluss vom 29. September 2022, 1 BvR 2354/13 sowie BVerfG, Urteil vom 26. April 2022) zu den Übermittlungsvorschriften nunmehr geklärt, dass die Übermittlung nachrichtendienstlich erhobener Informationen einer eigenen Schwellensystematik folgt, die im Wesentlichen den Grundsatz der hypothetischen Datenneuerhebung abbildet. Für die vormalige Privilegierung einzelner Datenkategorien der strategischen Fernmeldeaufklärung besteht insoweit keine Notwendigkeit mehr. Stattdessen erfolgt eine Einsichtnahme nunmehr (einheitlich) regelmäßig zur Früherkennung von Bedrohungen, die als Früherkennungsmaßnahme naturgemäß auch das politische Interesse an einer frühzeitigen Unterrichtung über Sachverhalte von außen- oder sicherheitspolitischer Bedeutung umfasst.

Entsprechend ist in Buchstabe a geregelt, dass die Anordnung einer strategischen Aufklärungsmaßnahme Angaben zu der jeweiligen erheblichen Bedrohung oder den jeweiligen erheblichen Bedrohungen (da auch mehrere Bedrohungen gemeinsam Grundlage der Aufklärungsmaßnahme sein können) enthalten muss. Dies folgt dem Umstand, dass mit einer strategischen Aufklärungsmaßnahme in der Regel eine Einsichtnahme in kommunikationsbezogene Inhaltsdaten nach §§ 33ff. bezweckt ist. In diesem Regelfall ist (nur) das Vorliegen der Voraussetzungen einer erheblichen Bedrohung nach § 3 in Bezug auf das relevante Aufklärungsthema darzulegen. Auch hier gilt, dass das Vorliegen der ersten Qualifikationsstufe immer auch den Einsatz von nachrichtendienstlichen Mitteln der Grundstufe (nachrichtendienstliche Auslandsaufklärung) rechtfertigt; weitere Darlegungen zum Vorliegen der Voraussetzungen nach § 32 Absatz 1 oder § 33 Absatz 1 erübrigen sich in einem solchen Fall.Liegt dem Aufklärungsthema eine erhebliche Bedrohung zugrunde, eröffnet eine entsprechende Bestätigung durch das gerichtsähnliche Kontrollorgan des Unabhängigen Kontrollrates dem Bundesnachrichtendienst die jeweiligen Befugnisse nach §§ 32ff., wobei die Prüfung des Vorliegens der Voraussetzungen der jeweiligen Erhebung und Einsichtnahme im konkreten Einzelfall weiterhin der nachgelagerten Kontrolle durch das administrative Kontrollorgan des Unabhängigen Kontrollrates vorbehalten bleibt.

Dabei ist zu berücksichtigen, dass die strategische Aufklärung – wie die Tätigkeit des Bundesnachrichtendienstes insgesamt – schon der Früherkennung von Bedrohungen dient, also schon den potentiellen Nährboden für Bedrohungen in den Blick nehmen muss. Dies gilt für „erhebliche Bedrohungen“ gleichermaßen, sodass es für eine Begründung der Erforderlichkeit einer Einsichtnahme nicht geboten ist, darzulegen, dass die erheblichen Bedrohungen faktisch bereits vorliegen. Vielmehr ist auszuführen, weshalb die Einsichtnahme erforderlich ist, um solche (erheblichen) Bedrohungen möglichst früh zu erkennen. Eine solche Begründung muss notwendigerweise prognostische und heuristische Elemente enthalten, deren Prüfung insoweit auf eine Plausibilität beschränkt ist. Zu den Anforderungen an die Begründung, ob ein Aufklärungsthema sich als eine solche erhebliche ‚Bedrohung qualifiziert, wird weitergehend auf die obigen Ausführungen zu Nummer 1 verwiesen.

In den Buchstaben b und c finden sich die Erfordernisse neuer, bislang nicht vorgesehener Angaben. Dies ist zum einen die – aus der Überführung der strategischen Inland-Ausland-Fernmeldeaufklärung des Artikel 10-Gesetzes folgende – Pflicht einer Angabe zur beabsichtigten Einsichtnahme in die personenbezogenen Daten von deutschen Staatsangehörigen, inländischen juristischen Personen und sich im Bundesgebiet aufhaltenden Personen (Buchstabe b). Hierdurch wird sichergestellt, dass der Bundesnachrichtendienst die Intention dieser Einsichtnahme bereits dezidiert mitteilt. Nicht der Vorabkontrolle unterliegen freilich individuelle Akte der Einsichtnahme – es wäre schlechterdings auch nicht möglich, zum Zeitpunkt der Anordnung die tatbestandlichen Voraussetzungen etwaiger Einsichtnahmeakte zu prüfen. Buchstabe b erfüllt vielmehr (nur) eine Hinweisfunktion und ermöglicht dem

Unabhängigen Kontrollrat eine spätere zielgerichtete Kontrolle der Einsichtnahme in Kommunikationsdaten mit qualifiziertem Inlandsbezug durch den Bundesnachrichtendienst. In der Praxis wird eine solche Einsichtnahme die Regel sein und bedarf, wenn sie sachgerecht ist, keiner besonderen materiellen Qualifikation. Entscheidend ist (nur), dass in der Anordnung die Angabe enthalten ist, dass auch in kommunikationsbezogene Inhaltsdaten Einsicht genommen werden soll. Dies soll insbesondere dem Zweck dienen, der gerichtsähnlichen Kontrollorgan eine spezifische Erteilung von Prüfaufträgen zu ermöglichen, die eine nachgelagerte Kontrolle durch das administrative Kontrollorgan anleitet, welches sodann die individuellen Einsichtnahmeakte und das Vorliegen der hierfür erforderlichen tatbestandlichen Voraussetzungen prüft.

In Buchstabe c ist darüber hinaus auch die aus der Rechtsprechung des Europäischen Gerichtshof für Menschenrechte folgende Notwendigkeit umgesetzt, dass in der Anordnung auch Angaben zur Verwendung sog. „starker Selektoren“ (EGMR, Urteil vom 25.05.2021, Az. 58170/13 u.a), also solcher Suchbegriffe, die einen konkreten Personenbezug haben, enthalten sein müssen. Dabei ist weiterhin nicht erforderlich, dass die Suchbegriffe selbst in der Anordnung genannt werden. Stattdessen sind Angaben dazu hinreichend, dass eine Verwendung von Suchbegriffen, die sich auf bestimmbare Personen beziehen, beabsichtigt ist. In Buchstabe c ist zudem festgeschrieben, dass auch das „Ausmaß“ der genannten Einsichtnahme / Suchbegriffverwendung angegeben wird. Hierbei ist es weder erforderlich, dass der Bundesnachrichtendienst eine konkrete Zahl oder auch nur eine bestimmte Relation angibt. Vielmehr ist es hinreichend, wenn allgemeine Angaben gemacht werden, also etwa ob eine Einsichtnahme / Suchbegriffverwendung in „geringem Ausmaß“, in „substantiellen Ausmaß“ oder einem „überwiegendem Ausmaß“ erfolgen soll. Dabei dürfte eine fast ausschließliche Verwendung solcher Suchbegriffe die Regel sein. Dies ist unschädlich, da die Angabe den Unabhängigen Kontrollrat gleichwohl befähigt, diesen Umstand im Rahmen seiner Vorabkontrolle mit einzubeziehen. Auch insoweit unterliegt der Vorabkontrolle dabei „nur“ die abstrakte Angabe, dass eine Einsichtnahme anhand von Suchbegriffen, die sich auf bestimmbare Personen beziehen, beabsichtigt ist. Dies ist im Rahmen der abstrakten Verhältnismäßigkeitsprüfung zu berücksichtigen; eine darüberhinausgehende konkrete Vorabkontrolle einzelner Suchbegriffe oder Einsichtnahmen scheidet hingegen aus. Dies erfolgt im Rahmen der nachgelagerten Kontrolltätigkeit.

Zu Absatz 3

Absatz 3 regelt die Befristung der Anordnung. Dabei wird der maximale Zeitraum festgelegt, in dem Verkehre erhoben werden dürfen und in dem eine Einsicht in die jeweils erhobenen Verkehre genommen werden darf. Anders als in § 46 muss bei strategischen Aufklärungsmaßnahmen im Übrigen nicht zusätzlich noch die Dauer der Maßnahmen selbst gesondert ausgewiesen werden, da in der Regel davon auszugehen ist, dass hier Dauer und Befristung der Anordnung gleich anzusetzen sind.

Der neue Absatz 3 Satz 2 regelt klarstellend die Möglichkeit der Verlängerungen von strategischen Aufklärungsmaßnahmen. Verlängerungen können mit entsprechender Begründung mehrfach erfolgen, eine diesbezügliche Begrenzung ist ausdrücklich nicht vorgesehen. Auch einzelne Suchbegriffe, zu denen bislang keine Erfassungen vorliegen, können nach Prüfung im Rahmen einer verlängerten Anordnung mehrfach erneut gesteuert werden und unterliegen diesbezüglich keiner pauschalen Begrenzung, da der fehlenden Erfassung vielfältige Ursachen zugrunde liegen können. So können beispielsweise etwa die limitierten Erfassungsmöglichkeiten im Rahmen der strategischen Aufklärung oder auch ein besonders überwachungssensibles Verhalten des Betroffenen (z.B. ein längere Abschaltung einer SIM-Karte oder eine nur sporadische Nutzung zu bestimmten Zwecken oder Zeitpunkten) für die fehlende Erfassung ursächlich sein.

Zu Absatz 4

Absatz 4 nimmt die Regelung des bisherigen § 23 Absatz 5 auf und passt sie an die neue Systematik an. Geregelt werden die gesonderten Anordnungen, welche bei der Steuerung qualifiziert schützenswerter Suchbegriffe vorzuschalten sind.

Zu Absatz 5

Die Vorschrift entspricht dem bisherigen § 23 Absatz 6. Entsprechend der systematischen Veränderungen betrifft die Verwendung von Suchbegriffen dabei den zweiten Schritt der Datenerhebung durch strategische Aufklärungsmaßnahmen, also die Verwendung der Suchbegriffe im Rahmen der Einsichtnahme. Zur Möglichkeit der Verlängerung siehe die Ausführungen oben zu Absatz 3.

Zu Absatz 6

In Absatz 6 ist geregelt, dass der im Rahmen von Kooperationen zur Übermittlung unselektierter kommunikationsbezogener Metadaten erforderliche „qualifizierte Aufklärungsbedarf“ ebenfalls der Anordnung in Form einer Feststellung bedarf.

Zu Absatz 7

Satz 1 entspricht dem bisherigen § 23 Absatz 8. Schon aufgrund des fehlenden Schriftformerfordernisses der Anordnung ist diese zu dokumentieren. Die Dokumentation der „Durchführung“ der Anordnung soll dabei nur sicherstellen, dass nachvollzogen werden kann, ob und wann die Maßnahme tatsächlich zur Durchführung gelangt ist. Siehe ergänzend die Begründung zu § 46 Absatz 6.

Zu § 48 (Anordnung sonstiger besonderer Befugnisse der technischen Aufklärung)

Die Vorschrift regelt die Anordnungen für sonstige technische Aufklärungsmittel, also der Telekommunikationsüberwachung und sog. CNE-Maßnahmen.

Zu Absatz 1

In Absatz 1 ist zunächst – wie auch im Rahmen der übrigen Anordnungsvorschriften – geregelt, dass die Anordnung der im Einzelnen genannten Maßnahmen der technischen Aufklärung durch die Behördenleitung des Bundesnachrichtendienstes oder einer von ihr bestimmten Vertretung zu erfolgen hat. Auf die obigen Ausführungen zu § 46 Absatz 1 wird insoweit verwiesen.

Zu Absatz 2

In Absatz 2 sind sodann die erforderlichen Angaben benannt, welche eine – abermals nicht notwendigerweise schriftliche – Anordnung einer der genannten Maßnahmen enthalten muss. Im Übrigen kann eine Anordnung (dies sei lediglich klarstellend erwähnt) auch mehrere Maßnahmen zugleich anordnen und miteinander „kombinieren“, das heißt, dass in einer Anordnung mehrere Maßnahmen der „sonstigen“ technischen Aufklärung indes – falls erforderlich – auch andere nachrichtendienstliche Mittel (§§ 46 bis 48) angeordnet werden können.

Inhaltliche Voraussetzungen von Anordnungen sind vornehmlich diejenigen Angaben, welche dem Unabhängigen Kontrollrat ermöglichen, die Rechtmäßigkeit der jeweiligen Maßnahme beurteilen zu können.

Hierbei ist die Person oder Personengruppe – denkbarerweise auch in der Ausgestaltung eines „Netzwerkes“, dessen Teilnehmern gemein ist, dass sie gerade (noch) nicht bekannt sind - zu konkretisieren. Die Anordnung darf sich dabei aber auch auf - noch unbekannte -

Personen beziehen, soweit sie beispielweise über ihre Funktion oder Aufgabe in einem Unternehmen oder einer staatlichen Stelle bestimmbar sind. Zugleich ist anzuführen, ob sich die Maßnahme gegen einen Deutschen, einer sich im Bundesgebiet aufhaltenden Person oder eine inländische juristische Person richtet (Nummer 1). Die Anordnung muss ferner Angaben zur Befristung (Nummer 2 in Verbindung mit Absatz 3) der Maßnahme enthalten. Auch hier muss anders als in § 46 bei strategischen Aufklärungsmaßnahmen im Übrigen nicht zusätzlich noch die Dauer der Maßnahme selbst gesondert ausgewiesen werden. Handelt es sich um einen Anschluss, welcher von der (eigentlich) verantwortlichen Person genutzt wird, aber einer anderen Person zuzuordnen ist (§ 35 Absatz 4 Nummer 3 Buchstabe b), so ist die Rufnummer oder Kennung des zu überwachenden Anschlusses oder Endgerätes aufzuführen (Nummer 3). Bei den Eingriffen in informationstechnische Systeme ist darüber hinaus eine Beschreibung desjenigen informationstechnischen Systems anzugeben, in welches eingriffen werden soll (Nummer 4 und 5), die es ermöglicht, die Maßnahme rechtlich einzuordnen. Die Bezeichnung des informationstechnischen Systems muss (nur) so genau erfolgen, wie es möglich ist. Dies bedeutet nicht die konkrete Nennung von technischen Parametern o.ä., sondern verlangt lediglich eine Beschreibung des Ziels, die eine Vorstellung dazu vermitteln soll, um welche Art Zielsystem es sich handelt und ggf. welche Art von Daten sich voraussichtlich darauf befinden. Die Anordnung ist zu begründen (Nummer 6).

Nicht Teil der Anordnung sind Angaben dazu, auf welche „Weise“ die jeweilige Maßnahme durchgeführt werden soll. So ist insbesondere auch im Rahmen der Telekommunikationsüberwachung nicht anzugeben, in welcher Form (vgl. § 35 Absatz 3) die Telekommunikationsüberwachung erfolgen soll. Hierbei handelt es sich vielmehr um bloße Durchführungsmodalitäten, welche grundsätzlich keine besondere Grundrechtsrelevanz aufweisen. Die verschiedenen Durchführungsarten dienen letztlich dem gleichen Ziel und sind, da sie allesamt auf eine rechtmäßig angeordnete Überwachung der Telekommunikation abzielen, von vergleichbarem Eingriffsgewicht (wobei die Durchführungsform der „strategischen Aufklärung“ faktisch in der Regel hinter dem Eingriffsgewicht der beiden anderen Eingriffsformen zurückbleiben wird).

Ferner ist die beabsichtigte Durchführungsform für den Bundesnachrichtendienst in aller Regel im Vorfeld nicht abschätzbar ist: So knüpfen die verschiedenen Möglichkeiten letztlich an technische Parameter an (etwa die Verschlüsselung der Kommunikation durch den Betroffenen oder die Möglichkeit einen Zugriff auf sein Endgerät zu erhalten), welche sich bei Anordnung noch nicht verlässlich einschätzen lassen.

Zu Absatz 3

Die Anordnung einer Maßnahme der technischen Aufklärung ist – mit Ausnahme der besonders eingriffsintensiven Maßnahme nach § 37 Absatz 3 (Online-Durchsuchung gegenüber einer Person mit deutscher Staatsangehörigkeit oder einer sich im Bundesgebiet aufhaltenden Person), die nur für einen Zeitraum von maximal sechs Monaten angeordnet werden kann – auf höchstens ein Jahr zu befristen, wobei die Frist verlängert werden kann, wenn die jeweiligen Voraussetzungen der Anordnung fortbestehen. Dass die Maßnahme nach § 37 Absatz 3 insoweit trotz ihres Eingriffsgewichts vergleichsweise lang angeordnet werden kann (vgl. etwa den Zeitraum einer Wohnraumüberwachung), ist dem Umstand geschuldet, dass aufgrund technischer Notwendigkeiten regelmäßig ein längerer Zeitraum für eine erfolgreiche Maßnahmendurchführung erforderlich ist.

Zu Absatz 4

Absatz 4 enthält die (neue) Möglichkeit, dass Anordnungen einen (gesondert zu begründenden und zu prüfenden) Zusatz enthalten, nach dem die Maßnahme auch gegen andere Personen gerichtet werden kann. Nach Satz 2 ist dies bei einer Maßnahme der Telekommunikationsüberwachung erweitert auch hinsichtlich von Anschlüssen und

Telekommunikationsmerkmalen möglich und nicht nur bezüglich Personen. Ergänzend wird auf die Ausführungen zu § 17 Absatz 4 verwiesen.

Zu Absatz 5

Absatz 5 statuiert eine Ausnahme von dem Anordnungserfordernis bei Eingriffen in informationstechnische Systeme und ermöglicht es dem Bundesnachrichtendienst so, den Zugang zu einem informationstechnischen System zu sichern. Maßnahmen der Zugangssicherung ermöglichen eine sofortige Handlungsfähigkeit, wenn nur eine zeitlich eng begrenzte Realisierungsmöglichkeit zur Verfügung steht. Mitunter vergehen wenige Stunden zwischen dem Bekanntwerden bzw. der Kenntniserlangung einer Realisierungsmöglichkeit und etwaigen Maßnahmen zur Behebung z.B. von Schwachstellen in Programmen eines informationstechnischen Systems.

Die Zugangssicherung sichert daher in denjenigen Fällen, bei denen zum Zeitpunkt der möglichen Zugangsgewinnung bislang keine Anordnung zum Eingriff in informationstechnische Systeme erwirkt wurde, etwa wegen der bis dahin technisch-operativ nicht möglichen Umsetzbarkeit, eine Zugriffsmöglichkeit auf die im informationstechnischen System gespeicherten personenbezogenen Daten, ohne die auf dem Zielsystem enthaltenen personenbezogenen Daten zunächst zu erheben oder weiterzuverarbeiten.

Selbst eine Anordnung im Eilverfahren kann hier im Einzelfall schon zu lange dauern. Insofern besteht große Eile beim Herstellen der Zugangsmöglichkeit und es wird dem Bundesnachrichtendienst mit dieser Befugnis ermöglicht, dies schnellstmöglich durchzuführen. Soweit es sich um ein Zielsystem handelt, für das gesetzliche Vorgaben betreffend die Anordnung vorgegeben sind, wird dem Anordnungserfordernis insofern Rechnung getragen, als dass bis zur Anordnung und deren Bestätigung durch den Unabhängigen Kontrollrat keine über die Zugangsschaffung hinausgehende Datenverarbeitung stattfinden darf.

Die technische Vorbereitung der Zugangssicherung schließt die dafür notwendige Datenverarbeitung mit ein, die Datenerhebung und -weiterverarbeitung bleibt durch ihren Zweck eng begrenzt. Die Besonderheit des hier geregelten Sachverhalts besteht im Eingriff in die Integrität des informationstechnischen Systems. Ansonsten sind bloße – auch technische - Vorbereitungsmaßnahmen auch ohne spezielle Regelungen bereits vor der Anordnung der besonderen Befugnis zulässig.

Zu Absatz 6

Schon aufgrund des fehlenden Schriftformerfordernisses der Anordnung ist sie zu dokumentieren. Die Dokumentation der „Durchführung“ der Anordnung soll dabei nur sicherstellen, dass nachvollzogen werden kann, ob und wann die Maßnahme tatsächlich zur Durchführung gelangt ist. Siehe ergänzend die Begründung zu § 46.

Zu Abschnitt 4 (Erweiterte nachrichtendienstliche Maßnahmen)

Die Primäraufgabe des Bundesnachrichtendienstes ist die Sammlung und Auswertung von Informationen, um die Bundesregierung mit Entscheidungsgrundlagen zur Sicherung ihrer außen- oder sicherheitspolitischen Handlungsfähigkeit zu versorgen (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 128). Erkennt der Bundesnachrichtendienst im Rahmen seiner aufklärenden Tätigkeit (etwa durch Erkenntnisse aus dem Einsatz nachrichtendienstlicher Mittel oder durch Informationen ausländischer Nachrichtendienste), dass von einer bestimmten fremden Macht eine spezifische und besonders qualifizierte Gefährdung für besonders gewichtige Kollektivrechtsgüter ausgeht, so wird er durch die in Abschnitt 4 geregelten „Einwirkungsbefugnisse“ erstmals befähigt, in diesen Sondersituationen dieser Gefährdung entgegenzutreten, d.h. sie abzuwenden oder wenigstens einzuschränken. Diese Befugnisse schaffen den Rechtsrahmen für „erweiterte nachrichtendienstliche Maßnahmen“, die über die bloße Informationsbeschaffung hinausreichen. Die Bundesregierung nimmt die Bedrohung durch von fremden Mächten ausgehenden Gefährdungen ernst und

schafft hier Rechtsgrundlagen, mit deren Hilfe die Bundesrepublik Deutschland – unter Beachtung des Verhältnismäßigkeitsgrundsatzes – auch im Ausland reagieren kann. Damit wird ein angemessenes und flexibles sicherheitspolitisches Mittel zur Bewältigung spezifischer Herausforderungen geschaffen. Im Kontext internationaler Bündnisverpflichtungen können auch intensivierte auslandsnachrichtendienstliche Tätigkeiten der Bundesrepublik Deutschland geboten sein.

Der Bundesnachrichtendienst ist in diesen Fällen schon aufgrund seines Tätigkeitsschwerpunktes regelmäßig die einzige Behörde, welche einer entsprechenden Gefährdung wirksam begegnen kann. Entsprechend bedarf es auch korrelierender begrenzter Einwirkungsbefugnisse, um eine anderenfalls bestehende Schutzlücke zu schließen und damit den staatlichen Schutzpflichten zu entsprechen. Dies ändert nichts daran, dass dem Bundesnachrichtendienst „grundsätzlich“ (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 149) keine operativen Befugnisse zukommen: einerseits aufgrund des (tatbestandlich verankerten) Ausnahmecharakters der Regelungen und andererseits deshalb, weil es sich hierbei regelmäßig nicht um „Anschlussmaßnahmen“ im Sinne der Rechtsprechung des Bundesverfassungsgerichts handelt, da der Bundesnachrichtendienst gerade nicht durch verwaltungsrechtliche Mittel im Allgemeinen oder polizeilichen Zwang im Konkreten agiert, sondern im Ausland außerhalb des regulären Rahmens hoheitlicher „Anschlussbefugnisse“ operiert.

Zu § 49 (Spezifische Gefährdungslage)

Zu Absatz 1

Die Vorschrift enthält die situativ begrenzte Erweiterung der Aufgabe des Bundesnachrichtendienstes um das „aktive Einwirken zur Abwendung oder Einschränkung einer spezifischen Gefährdungslage“. Dabei ist zugleich klargestellt, dass diese Aufgabe als Addendum zu der (Primär-)Aufgabe der nachrichtendienstlichen Auslandsaufklärung hinzutritt, auf dieser also faktisch „aufsetzt“. Die Feststellung der spezifischen Gefährdungslage setzt dabei voraus, dass ein über das bloße Erkennen hinausgehender (schriftlicher) Feststellungsprozess erfolgt. Wie dieser behördenseitig ausgestaltet wird, ist dabei dem Bundesnachrichtendienst vorbehalten. Eine Zuständigkeit für entsprechende Maßnahmen der aktiven Einwirkung besteht im Ausland umfassend. Im Inland ist sie demgegenüber subsidiär ausgestaltet und tritt grundsätzlich hinter entsprechende (hinreichende) Zuständigkeiten der Gefahrenabwehrbehörden zurück. Dabei ist indes in gewissen Sachverhalten eine Zuständigkeit des Bundesnachrichtendienstes auch im Inland geboten und vonnöten. Auch ist bei Maßnahmen im Cyberraum die entsprechende Besonderheit zu beachten, dass der Belegenheitsort eines informationstechnischen Systems für die Qualifikation einer Maßnahme als „Inlandsmaßnahme“ unerheblich ist, maßgeblich kommt es vielmehr darauf an, wer Ziel und damit Hauptbetroffener der Maßnahme ist.

Dies betrifft die in Satz 2 (insbesondere) genannten Beispiele, bei denen eine originäre Zuständigkeit des Bundesnachrichtendienstes besteht, weil nur ihm eine wirksame Durchführung aus tatsächlichen oder rechtlichen Gründen möglich ist: Beispielhaft ist es im Rahmen der internationalen Zusammenarbeit von Nachrichtendiensten die Regel, dass Informationen nur unter der Maßgabe geteilt werden, dass diese nicht an andere Stellen weitergegeben werden dürfen. Wenn der Bundesnachrichtendienst entsprechende Informationen erhält, welche aktive Maßnahmen bedingen, so kann er diese Informationen nicht an andere Stellen weitergeben, sondern muss „selbst“ handeln. Vergleichbares gilt, wenn nur der Bundesnachrichtendienst aufgrund seiner (nachrichtendienstlichen oder technischen) Fähigkeiten in der Lage ist, die Maßnahmen durchzuführen.

Zu Absatz 2

Erweiterte nachrichtendienstliche Maßnahmen knüpfen an eine „spezifische Gefährdungslage“ an. Diese wird in Absatz 2 tatbestandlich konturiert, wobei – der allgemeinen

nachrichtendienstlichen Logik entsprechend – tatsächliche Anhaltspunkte bestehen müssen, dass die im Folgenden ausgeführten besonderes hohen Schwellen erreicht werden.

Erforderlich ist zunächst, dass die zugrundeliegende Gefährdung gegen die besonders gewichtigen Kollektivrechtsgüter gerichtet ist, die in § 2 Absatz 2 Nummer 1 bis 5 geregelt sind. Damit ist die Gefährdungslage nur gegeben, wenn z.B. der Bestand oder die Sicherheit des Staates oder die freiheitlich demokratische Grundordnung gefährdet wird.

Die Gefährdung muss zumindest mittelbar von einer bestimmten fremden Macht ausgehen (Nummer 1). Dies bedeutet einerseits, dass nur hoheitliche oder quasi-hoheitliche (vgl. hierzu § 6 Absatz 3) Gefährdungen erfasst werden und nicht z.B. das Handeln von kriminellen Gruppierungen ohne jedweden konkreten Bezug zu einer fremden Macht. Andererseits soll das Merkmal, dass es sich um eine „bestimmte“ fremde Macht handeln muss, verdeutlichen, dass die spezifische Gefährdungslage bereits in ihrer tatbestandlichen Reichweite auf einen konkreten Ursprung begrenzt bleibt und eine besondere Ausnahmesituation darstellt. Eine eindeutige Attribuierung von gefährdenden Tätigkeiten zu einer fremden Macht ist nicht erforderlich; tatsächliche Anhaltspunkte sind vielmehr auch insoweit hinreichend.

Es müssen zudem auch tatsächliche Anhaltspunkte dafür bestehen, dass die Gefährdung „anhaltend und planvoll“ (Nummer 2) erfolgt. Sie darf also nicht nur vorübergehender Natur sein und gleichsam zufällig auftreten. Für den Ausschluss der vorübergehenden Natur ist gleichwohl nicht erforderlich, dass die Gefährdung schon eine längere Zeit andauert. Entscheidend ist vielmehr, ob die Gefährdung als einmaliger und dann auch beendeter Vorgang auftritt oder die Rechtsgüter gerade anhaltend gefährdet werden sollen.

Zuletzt erfolgt eine qualifizierende Steigerung dadurch, dass die Gefährdung „in besonderem Maße“ vorliegen muss (Nummer 3). Dies stellt sicher, dass nicht „jede“ Art von Gefährdung für die genannten besonders gewichtigen Rechtsgüter für eine spezifische Gefährdungslage hinreichend ist. Eine solche qualifizierte Gefährdung kann etwa vorliegen, wenn die besonders gewichtigen Rechtsgüter durch eine große Vielzahl niedrigschwelliger einzelner Tätigkeiten „in der Summe“ oder durch einzelne oder wenige besonders schwerwiegende Aktivitäten gefährdet werden.

Zu Absatz 3

Durch die in Absatz 3 statuierte regelmäßige Pflicht, den Fortbestand einer spezifischen Gefährdungslage zu (über-)prüfen, wird sichergestellt, dass der Ausnahmecharakter auch in zeitlicher Hinsicht erhalten bleibt. Ein schematischer Zeitraum ist nicht vorgesehen, es kommt insoweit auf die jeweiligen Umstände des Einzelfalles an. Zugleich ist nicht ausgeschlossen, dass – etwa aufgrund eines Regimewechsels und der damit verbundenen Einstellung von gefährdenden Tätigkeiten durch eine fremde Macht – eine spezifische Gefährdungslage auch plötzlich und unvermittelt enden kann.

Zu § 50 (Grundanordnung)

In der Vorschrift finden sich – der allgemeinen Systematik des Gesetzes folgend – die Maßgaben für die Grundanordnung. Die Grundanordnung ist dem Unabhängigen Kontrollrat zur Vorabkontrolle vorzulegen. Sie schafft damit einerseits den Rahmen der erweiterten nachrichtendienstlichen Maßnahmen und zugleich den Kontrollgegenstand, welcher durch die erforderliche unabhängige Vorabkontrolle sicherstellt, dass rechtsstaatliche Vorgaben eingehalten werden.

Zu Absatz 1 und Absatz 2

Rechtssystematisch ist entsprechend vorgesehen, dass die Durchführung konkreter erweiterter nachrichtendienstlicher Maßnahmen den Erlass einer Grundanordnung voraussetzt, welche die Maßnahmen inhaltlich eingrenzt (Absatz 1). Diese Grundanordnung, welche

durch die Behördenleitung oder ihre Vertretung (also nicht einer, wie bei den übrigen Anordnungen regelmäßig möglichen, gewillkürten Vertretung) erfolgt (Absatz 2), schafft somit die Grundlage und den Rahmen für individuelle erweiterte nachrichtendienstliche Maßnahmen. Inwieweit die einzelnen Maßnahmen auch weiterer Entscheidungen durch die Behördenleitung (oder einer politischen Freigabe) bedürfen, kann untergesetzlich oder durch entsprechende Weisungen der Dienst-/Fachaufsicht geregelt werden.

Zu Absatz 3

In Absatz 3 finden sich die konkreten Inhalte der Grundanordnung. Dabei sind neben der spezifischen Gefährdungslage, die abgewendet oder eingeschränkt werden soll (Nummer 1) und der Befristung (Nummer 3) insbesondere die Art und der Umfang, in denen erweiterte nachrichtendienstliche Maßnahmen erfolgen sollen (Nummer 2) anzugeben. Hierbei ist keine konkrete Benennung einzelner Maßnahmentypen erforderlich, wohl aber eine gewisse abstrakte Eingrenzung angelegt. Denkbar wäre es z.B. beim „Umfang“ der erweiterten nachrichtendienstlichen Maßnahmen Tätigkeitsfelder zu benennen, in denen einer spezifischen Gefährdungslage entgegengewirkt werden kann und soll (etwa der Kommunikations- oder Informationsraum, Warenlieferungen, der Rüstungsproduktion oder staatlichen Wirtschaftsstrukturen). Die „Art“ von Maßnahmen kann auch abstrakt (etwa als Manipulation oder Unterbindung) beschrieben werden, soweit die Situation es erfordert, die notwendige Flexibilität zu erhalten. Ferner ist die Grundanordnung zu begründen (Nummer 4). Dies betrifft zum einen das Vorliegen der spezifischen Gefährdungslage. Die Begründungspflicht erstreckt sich aber auch auf die Befristung und die Art und den Umfang, in denen erweiterte nachrichtendienstliche Maßnahmen erfolgen sollen. In diesem Zusammenhang ist es notwendig, dass speziell die Erforderlichkeit der unter Nummer 2 beschriebenen Maßnahmen für die Abwendung bzw. Einschränkung der Gefährdung dargelegt wird. Zugleich stellt die Notwendigkeit einer Begründung sicher, dass die Grundanordnung einen hinreichenden Grad der Konkretisierung aufweist. Dabei verschließt sich der notwendige Detailierungsgrad einer Grundanordnung aufgrund der unvorhersehbaren möglichen Konstellationen von spezifischen Gefährdungslagen einer schematisch abschließenden Betrachtung. Vielmehr wird es im Zusammenspiel mit dem Unabhängigen Kontrollrat darauf ankommen, eine hinreichend spezifische Begründung für die jeweils in Rede stehende Grundanordnung zu finden und mögliche übergreifende Erfahrungswerte zu definieren. Denkbarerweise lässt sich hierbei durch die Schilderung konkreter Beispiele für die realweltliche Gefährdung ein größeres Konkretisierungsniveau erreichen, da diese Beispiele zugleich für Art und Umfang der erweiterten nachrichtendienstlichen Maßnahmen leitend sein können.

Zu Absatz 4

In Absatz 4 ist geregelt, dass Grundanordnung grundsätzlich auf zwölf Monate zu befristen sind, aber auch verlängert werden können. Zugleich ist klargestellt, dass die Grundanordnung auch vor der Frist aufzuheben ist, wenn die zugrundeliegende spezifischen Gefährdungslage endet

Zu Absatz 5

In Absatz 5 findet sich die (allgemeine) Dokumentationspflicht in Bezug auf die jeweilige Grundanordnung.

Zu § 51 (Befugnis für erweiterte nachrichtendienstliche Maßnahmen)

Die Vorschrift enthält die (eigentliche) Befugnisnorm für die Durchführung von erweiterten nachrichtendienstlichen Maßnahmen. Die Befugnis zur Durchführung von Maßnahmen umfasst alle denkbaren Durchführungsformen, also neben physischem Wirken und Handeln im Informationsraum auch Maßnahmen wie Auskunftsersuchen o.Ä. Greift der Bundesnachrichtendienst zur Durchführung erweitert nachrichtendienstlicher Maßnahmen auf nachrichtendienstliche Verbindungen zurück, so ist auch dies möglich – ohne dass § 23

Anwendung findet – und das Handeln insoweit von der Befugnisnorm gedeckt und gerechtfertigt. Die Vorschriften des Abschnittes 3 bleiben bei vorbereitenden Maßnahmen, die auf die Informationsgewinnung beschränkt sind, unberührt.

Zu Absatz 1

In Absatz 1 ist geregelt, dass der Bundesnachrichtendienst die jeweiligen Maßnahmen durchführen darf, wenn diese zur Abwendung oder Einschränkung der konkreten spezifischen Gefährdungslage im Einzelfall erforderlich sind. Die Maßnahmen werden in ihrer inhaltlichen Reichweite durch die Grundanordnung begrenzt, können aber grundsätzlich jede denkbare Durchführungsart annehmen, welche zur Abwendung oder Einschränkung in Betracht kommt (etwa informationstechnische wie realtweltliche Durchführungsformen, dinglicher wie informationeller Art– insbesondere ist z.B. auch das Übermitteln von personenbezogenen Daten ohne Anwendung der Vorgaben von Abschnitt 6 erfasst, wenn dieses zur Abwendung oder Einschränkung der Gefährdung erforderlich ist). Dabei ist erforderlich – aber auch hinreichend – dass dem Bundesnachrichtendienst tatsächliche Anhaltspunkte dafür vorliegen, dass eine Gefährdung einer bestimmten fremden Macht zuzuordnen ist. Dies ist bereits eine (hinreichende) Voraussetzung für die Begründung einer spezifischen Gefährdungslage und ist insoweit gleichermaßen geeignet, auch ein aktives Handeln des Bundesnachrichtendienstes zu bedingen. Auch in Bezug auf die erweiterten nachrichtendienstlichen Maßnahmen gelten die Ausführungen zur Rechtfertigung, vgl. Begründung zu § 6 Absatz 1. Die öffentlich-rechtliche Befugnis stellt auch hier zugleich einen umfassenden Rechtfertigungstatbestand dar und ist insbesondere bei der Kollision mit ordnungsrechtlichen Vorschriften ebenso wie für das Strafrecht bedeutsam. Soweit der Bundesnachrichtendienst sowie die an der Erfüllung des gesetzlichen Auftrags des Bundesnachrichtendienstes beteiligten Personen im Rahmen ihrer gesetzlichen Befugnisse tätig werden, handeln sie nicht rechtswidrig.

Zu Absatz 2

In Absatz 2 ist in Satz 1 zunächst der Grundsatz statuiert, dass erweiterte nachrichtendienstliche Maßnahmen grundsätzlich im Ausland durchgeführt werden. Dies spiegelt letztlich den Umstand wieder, dass es gerade die mit Blick auf das Ausland bestehende „Schutzlücke“ ist, welche die Notwendigkeit eines aktiven Einwirkens des Bundesnachrichtendienstes zum Rechtsgüterschutz erforderlich machen kann. Der Bundesnachrichtendienst handelt mit Ziel- und Wirkrichtung Ausland. Der Ort der Durchführung ist dabei – grundsätzlich – derjenige Ort, an dem die jeweilige Maßnahme ihre Wirkung entfaltet. Insbesondere bei Operationen im Cyber-Raum kann insoweit auch die jeweilige Handlung im Inland erfolgen, solange die Wirkung der Maßnahme im Ausland eintritt. Dem allgemeinen Grundsatz folgend ist dabei auch hier der Belegenheitsort eines informationstechnischen Systems unerheblich; maßgeblich kommt es darauf an, wer das Ziel und damit Hauptbetroffener der Maßnahme ist.

Da eine strikte räumliche Begrenzung auf das Ausland weder sinnvoll noch aufgrund praktischer Abgrenzungsschwierigkeiten möglich ist, ist in Satz 2 die Ausnahme geregelt, dass der Bundesnachrichtendienst auch im Inland erweiterte nachrichtendienstliche Maßnahmen ausführen darf. Das Handeln auch im Inland kann im Einzelfall erforderlich sein, um der Gefährdung wirksam zu begegnen, wenn eine Vornahme im Ausland aus Effektivitätsgesichtspunkten weniger zielführend wäre.

Zu Absatz 3

In Absatz 3 findet sich die Zielrichtung von erweiterten nachrichtendienstlichen Maßnahmen: Diese sind nach Satz 1 gegen diejenige fremde Macht zu richten, welche für die spezifische Gefährdungslage verantwortlich ist. Dabei kommt es nicht maßgebend darauf an, dass z.B. nur „staatliches Eigentum“ beeinträchtigt werden kann. Vielmehr ist eine funktionale Abgrenzung vorzunehmen und sicherzustellen, dass sich Maßnahmen nicht gezielt

gegen unbeteiligte Privatpersonen in dieser Eigenschaft richten. Ebenso können die Maßnahmen auch gegen Ziele gerichtet werden, welche unmittelbar staatliche Aufgaben wahrnehmen oder von fremden Mächten für die (quasi-)staatliche Aufgabenwahrnehmung beauftragt wurden oder gesteuert werden. In Satz 2 ist eine weitere Begrenzung dahingehend vorgesehen, dass sich erweiterte nachrichtendienstliche Maßnahmen nicht gezielt gegen Leib und Leben von Personen richten dürfen, also gezielte Verletzungen oder Tötungen ausgeschlossen sind.

Zu Absatz 4

Durch Absatz 4 wird sichergestellt, dass sich erweiterte nachrichtendienstliche Maßnahmen immer im Rahmen der Verhältnismäßigkeit bewegen und dabei Nutzen und Schaden streng abgewogen werden müssen.

Zu Absatz 5

In Absatz 5 ist die Möglichkeit enthalten, um ergänzende Unterstützungshandlungen durch öffentliche und nichtöffentliche Stellen zur Durchführung erweiterter nachrichtendienstlicher Maßnahmen zu ersuchen.

Zu Absatz 6

Absatz 6 regelt, dass neben der Grundordnung (§ 50 Absatz 5) jeweils auch die auf ihrer Grundlage durchgeführten erweiterten nachrichtendienstlichen Maßnahmen zu dokumentieren sind.

Zu Abschnitt 5 (Weiterverarbeitung personenbezogener Daten)

Zu Unterabschnitt 1 (Allgemeine Weiterverarbeitungsvorschriften)

Die Weiterverarbeitung von personenbezogenen Daten durch den Bundesnachrichtendienst wurde grundlegend neugestaltet. Dabei wurde – neben der Lösung vom BVerfSchG – auch nicht länger an dem antiquierten „Datei“-begriff festgehalten. Die Vorschriften werden zudem an das veränderte System der Datenerhebung angepasst.

Das Gesetz unterscheidet nunmehr einzig zwischen personenbezogenen Daten insgesamt und solchen sach- oder personenbezogenen Vorgängen, welche in „Akten“ gesammelt werden. Dabei gilt für Akten der Grundsatz der Aktenvollständigkeit, sodass (nur) insoweit eine Ausnahme von den strengen Löschpflichten besteht.

Zu § 52 (Allgemeine Befugnis zur Weiterverarbeitung)

In § 52 wird – anlehnend an den bisherigen § 6 Absatz 1 und insoweit die Verweise auf § 10 BVerfSchG auflösend – die grundsätzliche Befugnis des Bundesnachrichtendienstes zur Weiterverarbeitung erhobener personenbezogener Daten geregelt. Das Gesetz verwendet nunmehr – der allgemeinen datenschutzrechtlichen Terminologie im Sicherheitsrecht (vgl. BVerfG, Urteil vom 1. Oktober 2024, 1 BvR 1160/19, Rn. 120) entsprechend – den Begriff der „Weiterverarbeitung“ für all diejenigen Verarbeitungsschritte, die zwischen Erhebung von Daten auf der einen Seite (wobei zu der Erhebung der Daten auch die notwendigen Schritte der Vorprozessierung zählen, innerhalb derer die – insbesondere im Rahmen der technischen Aufklärung – Vielzahl von erhobenen Daten gefiltert, aufbereitet und mit Bestandsdaten abgeglichen werden, um irrelevante Treffer auszufiltern) und der Übermittlung der personenbezogenen Daten auf der anderen Seite liegen. Abermals sei insoweit auch auf die besondere, zweistufige Systematik der strategischen Aufklärung hingewiesen, bei der die Einsichtnahme ausnahmsweise als Bestandteil der „Erhebung“ im weiteren Sinne geregelt ist.

Zu Absatz 1

Nach Absatz 1 ist der Bundesnachrichtendienst zunächst befugt, von ihm erhobene Daten über die erstmalige Speicherung hinaus weiterzuverarbeiten, soweit dies zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist und keine abweichenden gesetzlichen Bestimmungen bestehen. Solche abweichenden Bestimmungen gelten für personenbezogene Daten, bei denen die Weiterverarbeitung (etwa aufgrund besonderer Schutzpflichten, vgl. etwa § 21 oder § 22 oder aufgrund der bereichsspezifischen Ausweitung der Einsichtnahmemöglichkeiten zur Eignungsprüfung) eingeschränkt ist.

Die „erstmalige Speicherung“ ist dabei diejenige Speicherung, welche „erstmalig“ nach Abschluss des Erhebungsprozesses in einem System des Bundesnachrichtendienstes erfolgt, welches der manuellen Auswertung dient und dem Zugriff der Mitarbeiter des Bundesnachrichtendienstes, die mit der Auswertung erhobener Daten beauftragt sind, offensteht. Insoweit ist es nicht ausgeschlossen, dass im Rahmen der Erhebung bereits mehrere Zwischenspeicherungen erfolgen, weil dies im Rahmen technischer Verarbeitungsschritte unabdingbar oder zweckmäßig ist. Ebenso soll so die Möglichkeit offenbleiben, dass durch automatisierte Prozesse auf Erhebungsebene bereits Daten ausgefiltert werden, was bereits eingriffsmildernd wirkt, oder mit anderen Daten abgeglichen oder „verschnitten“ werden. Entscheidendes Kriterium für die „erstmalige Speicherung“ ist, dass die Daten hier dergestalt in den Datenbestand des Bundesnachrichtendienstes übergehen, dass sie für Mitarbeiterinnen und Mitarbeiter zur Kenntnisnahme und Weiterverarbeitung im Rahmen der Datenauswertung zur Auftragserfüllung des Bundesnachrichtendienstes zur Verfügung stehen.

Dabei trägt die normative Anknüpfung an die Weiterverarbeitung nach erstmaliger Speicherung dem Umstand Rechnung, dass es dem Bundesnachrichtendienst faktisch und schlechterdings unmöglich ist, Daten auf ihre Relevanz zu prüfen oder sonst zu verwenden, bevor er sie in dem für die Auswertung der Daten vorgesehenen System gespeichert hat. Zudem handelte sich bei einer vorherigen Prüfung auf die nachrichtendienstliche Relevanz (also einer Relevanz für die o.g. Aufgabenerfüllung) regelmäßig um eine bloße Förmlichkeit: Liegen im Moment der Datenerhebung tatsächliche Anhaltspunkte dafür vor, dass die Daten für die Aufgabenerfüllung des Bundesnachrichtendienstes erforderlich sind, so tragen diese tatsächlichen Anhaltspunkte faktisch über den (logischen) Moment der Datenerhebung hinaus und begründen zugleich tatsächliche Anhaltspunkte dafür, dass auch die Speicherung der Daten zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist. Dies ist allenfalls bei solchen Erhebungsarten (etwa der strategischen Aufklärung oder der Telekommunikationsüberwachung) anders, in denen eine größere „Streubreite“ der Datenerhebung vorliegen kann, also bewusst und unvermeidlich auch eine bestimmte Anzahl an Daten erhoben werden, die keine Relevanz für die Aufgaben des Bundesnachrichtendienstes haben. Entsprechend ist für diese Erhebungsformen eine gesonderte Prüfpflicht vorgesehen. Bei dieser Speicherung handelt es sich – der Terminologie des Verfassungsgerichts folgend – um eine „vorsorgende“ Speicherung, da die Speicherung einen „Datenbestand schafft, der nicht aus sich heraus auf konkrete Zwecke beschränkt ist, dabei aber Möglichkeiten der Verknüpfung von Daten eröffnet und personenbezogen auf potentiell sicherheitsrelevante Bezüge hinweisen kann“ (BVerfG, Urteil vom 1. Oktober 2024, 1 BvR 1160/19, Rn. 162).

Tatsächliche Anhaltspunkte für die nachrichtendienstliche Erforderlichkeit personenbezogener Daten ergeben sich grundsätzlich aus der vor der Datenerhebung geprüften und festgestellten nachrichtendienstlichen Relevanz des Ziels als Ganzem. Einzelne (mit-)erhobene personenbezogene Daten, die bei einer weiteren Bearbeitung des konkreten Datums als nicht nachrichtendienstlich relevant festgestellt werden, unterfallen grundsätzlich dem Löschgebot. Die Prüfung der einzelnen Daten erfolgt dementsprechend im Anschluss an die erstmalige Speicherung sukzessive im Rahmen der Weiterverarbeitung der erhobenen Daten. Um dem Umstand Rechnung zu tragen, dass bestimmte Erhebungsarten des Bundesnachrichtendienstes eine große Menge an Daten liefern, werden für die Weiterverarbeitung von Daten die aus Maßnahmen der strategischen Aufklärung und der

Telekommunikationsüberwachung besondere Vorgaben getroffen. Hintergrund ist, dass bestimmte erhobene Daten – etwa aufgrund ihres Volumens oder der Notwendigkeit vorheriger umfangreicher Analysen – inhaltlich nicht ausgewertet und auf ihre nachrichtendienstliche Erforderlichkeit geprüft werden können. Um dies zu berücksichtigen, findet sich in Absatz 2 eine Ausnahme von dem o.g. Grundsatz und den in Abschnitt 3 Unterabschnitt 3 vorgesehen Prüf- und Löschvorgaben. Diesen Maßnahmen ist zudem gemein, dass auch Daten miterhoben werden, welche für sich genommen keine nachrichtendienstliche Relevanz aufweisen. Um diesen Umstand zu kompensieren, enthalten die Vorschriften zur technischen Aufklärung (vgl. Abschnitt 3 Unterabschnitt 3) gesonderte Vorgaben für die Prüfung und Löschung von (bestimmten) personenbezogenen Daten, die mittels dieser Maßnahmen erhoben wurden.

Der Hintergrund dieser Regelung, die eine Weiterverarbeitung grundsätzlich ohne erweiternde Voraussetzungen und insbesondere – mit Ausnahme des Satzes 2 – ohne Rückgriff auf den Grundsatz der hypothetischen Datenneuerhebung gestattet, ist, dass der Bundesnachrichtendienst im Rahmen seiner Auftragstätigkeit insgesamt ausschließlich zum Schutz besonders gewichtiger Rechtsgüter tätig wird (zu dem insoweit maßgeblichen Aspekt der „Rechtsgutsäquivalenz“ vgl. instruktiv: Unterreitmeier in JZ 2021, S. 175ff.). Es handelt sich damit bei der Weiteverarbeitung durch den Bundesnachrichtendienst faktisch immer um einen Fall der sogenannten „zweckwahrenden Weiterverarbeitung“ (vgl. BVerfG, Urteil vom 1. Oktober 2024, 1 BvR 1160/19, Rn. 120), für die § 52 Absatz 1 die erforderliche Rechtsgrundlage bildet.

Hieraus folgt, dass die gesamte Aufklärungstätigkeit des Bundesnachrichtendienstes die Erfüllung einer „einheitlichen Aufgabe“ dient (die Sammlung von Informationen von außen- oder sicherheitspolitischer Bedeutung zum Schutz der qualitativ auf einer Stufe stehenden Rechtsgüter im Sinne des § 3 Absatz 1 vor Bedrohungen (vgl. auch die Ausführungen zu § 3 Absatz 1)). Der Bundesnachrichtendienst nutzt die mittels seiner Aufklärungstätigkeit erlangten Daten im Rahmen dieser einheitlichen nachrichtendienstlichen Aufgabe für den Schutz derselben Rechtsgüter (vgl. BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 279; wortgleich auch in BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19 u.a., Rn. 57: „Eine Weiternutzung kommt damit nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz der derselben Rechtsgüter in Betracht. Ist die Datenerhebung nur zum Schutz bestimmter Rechtsgüter (oder zur Verhütung bestimmter Straftaten) erlaubt, so begrenzt dies deren unmittelbare sowie weitere Verwendung auch in derselben Behörde, soweit keine gesetzliche Grundlage für eine Zweckänderung eine weitergehende Nutzung erlaubt.“) Und weiter: „Für die Wahrung der Zweckbindung kommt es demnach darauf an, dass die erhebungsberechtigte Behörde die Daten im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutzt, wie es die jeweilige Datenerhebungsvorschrift erlaubt. Diese Anforderungen sind erforderlich, aber grundsätzlich auch ausreichend, um eine weitere Nutzung der Daten im Rahmen der Zweckbindung zu legitimieren“ (BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19 u.a., Rn. 58).

Es können insbesondere auch die Daten von „Dritten“, also von Personen, die nicht unmittelbar für eine Bedrohung verantwortlich sind, diese unterstützen oder in einem Zusammenhang zu ihr stehen, gespeichert werden, wenn und solange dies für die nachrichtendienstliche Auslandsaufklärung erforderlich ist. Eine Notwendigkeit zur Speicherung der Erforderlichkeit eines personenbezogenen Datums kann sich somit auch daraus ergeben, dass das für sich genommen nicht nachrichtendienstlich relevante personenbezogene Datum in einem Kontext verarbeitet wird, welches im Aufklärungsinteresse des Bundesnachrichtendienstes steht. Beispielhaft hierfür sind Desinformationskampagnen, in deren Rahmen auch personenbezogene Daten nicht nachrichtendienstlich relevanter Personen (z.B. Prominente aus Sport, Kunst und Kultur) durch die Akteure solcher Kampagnen thematisiert werden. Für den vormaligen § 10 Absatz 2 des Bundesverfassungsschutzgesetzes besteht insoweit schon keine Regelungsnotwendigkeit mehr.

Absatz 1 Satz 2 enthält besondere Vorgaben für die Weiterverarbeitung von Daten aus einer Wohnraumüberwachung im Inland (§ 29 Absatz 2) und der nachrichtendienstlichen Maßnahme, die der sogenannten Online-Durchsuchung (§ 37 Absatz 3) gleichkommt (vgl. BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 283).

Zu Absatz 2

Absatz 2 regelt die allgemeine Zulässigkeit der Weiterverarbeitung gewisser personenbezogener Daten jenseits der Voraussetzungen des Absatzes 1.

Dies gilt zum einen für die in Nummer 1 genannten personenbezogene Daten, die aus allgemein zugänglichen Quellen erlangt werden (z.B. die Speicherung von Presseveröffentlichungen oder angekaufte Daten). Dass die Weiterverarbeitung „abweichend von den Absätzen 1 und 2“ zulässig ist, bringt zum Ausdruck, dass es insoweit keiner gesonderten Eingriffsschwellen bedarf; d.h. auch nicht, wenn ein Zugriff auf Daten aus allgemein zugänglichen Quellen erfolgt, die mittels einer automatisierten Auswertung zusammengeführt und zum Zweck der Datenanalyse weiterverarbeitet wurden. Möglich bleibt auch insoweit die automatisierte Weiterverarbeitung. Für die Aufgabenerfüllung des Bundesnachrichtendienstes spielen insbesondere Daten aus sozialen Medien eine wesentliche Rolle. Soziale Medien bieten ausländischen Akteuren ein breites Spektrum an Möglichkeiten, z.B. zur hybriden Einflussnahme. Vor allem mit Blick auf die gezielte Verbreitung von Desinformation sind soziale Medien von besonderer Relevanz. Für eine umfassende Auswertung der Ursprünge, Inhalte und Hintergründe von Desinformationskampagnen und in authentischen Netzwerken ist die Einbeziehung und Analyse offen verfügbarer Daten unerlässlich. Hierbei ist unter Umständen auch eine Weiterverarbeitung erforderlich, obwohl (noch) nicht absehbar ist, ob die erhobenen Daten im Einzelnen für die nachrichtendienstliche Auslandsaufklärung relevant sind. Dies betrifft dabei insbesondere Fälle, in denen der Bundesnachrichtendienst eine große Menge von Daten erhebt (etwa durch Ankauf), die einzelnen Daten aber nicht oder nicht unmittelbar darauf prüfen kann, ob sie für die nachrichtendienstliche Auslandsaufklärung relevant sind.

Für den Fall der Erhebung von personenbezogenen Daten aus allgemein zugänglichen Quellen nach § 2 Absatz 1 finden die Regelungen zur Beauskunftung nach § 102 keine Anwendung. Eine Prüfung der erhobenen personenbezogenen Daten aus allgemein zugänglichen Quellen zur Beantwortung von Auskunftsersuchen nach § 102 würde einen erstmaligen Grundrechtseingriff begründen, da die erhobenen Daten bestimmten Personen zugeordnet werden müssten. Ein solcher Grundrechtseingriff zur Beauskunftung würde datenschutzrechtliche Grundprämissen konterkarieren.

Nach Nummer 2 ist darüber hinaus auch die voraussetzungslose Weiterverarbeitung von personenbezogenen Daten zulässig, wenn die betroffene Person eingewilligt hat.

Zu Absatz 3

In Absatz 3 ist die Befugnis des Bundesnachrichtendienstes geregelt, personenbezogene Daten erstens in Personendatensätzen und Personendatensätze zweitens in Personendatenbanken zu speichern. Satz 2 enthält sodann die Legaldefinition von Personendatensätzen und Satz 3 die Legaldefinition von Personendatenbanken. Die Speicherung eines Personendatensatzes in einer Personendatenbank des Bundesnachrichtendienstes geht mit einer besonderen Grundrechtsintensität einher (und ist deshalb gesondert regelungsbedürftig), da der Bundesnachrichtendienst bei externen Anfragen etwa im Rahmen eines Visaverfahrens regelmäßig einen Abgleich mit seinen Personendatenbanken durchführt.

Entscheidend ist, dass personenbezogene Daten anhand „bestimmter Merkmale“ gespeichert werden. Bei diesen kann es sich z.B. um Staatsangehörigkeit, biometrische Merkmale, Namen etc. handeln. Für die Personendatenbanken tritt ergänzend hinzu, dass die Merkmale vom Bundesnachrichtendienst selbst (vor-)ausgewählt sein müssen. Dies bedeutet, dass eine an den Bundesnachrichtendienst übermittelte Personendatenbank – da

hier nicht der Bundesnachrichtendienst die Merkmale definiert hat – nicht von dem Begriff umfasst wird. Anderenfalls müsste der Bundesnachrichtendienst zu jeder umfangreichen, personenzentrierten Excel-Datei, welche ihm übermittelt wird, eine Errichtungsanordnung nach § 61 treffen.

Zu Absatz 4

Auch die automatisierte Auswertung von Daten ist auf Grundlage des Absatzes 4 grundsätzlich möglich. Dies betrifft etwa diejenigen Weiterverarbeitungsschritte, die nicht zu gesteigerten Grundrechtseingriffen führen, wie etwa eine automatisierte Organisation, Speicherung, Kennzeichnung, Übersetzung, etc. sowie den Abgleich von Daten. Erfasst ist jedoch auch die automatisierte Auswertung von Daten zur Generierung neuer persönlichkeitsrelevanter Informationen, solange hieraus keine spezifisch regelungsbedürftigen Grundrechtseingriffe erwachsen, welche über das „normale“ Maß einer Weiterverarbeitung unter Berücksichtigung der nachrichtendienstlichen Tätigkeit der Informationsauswertung hinausgehen. Durch die automatisierte Auswertung sollen dabei in den ausgewerteten Daten angelegte verborgene Erkenntnisse erschlossen werden oder Verknüpfungen über Personen hergestellt werden, welche nur durch den Einsatz automatisierter Verfahren erkennbar sind. Der Einsatz solcher automatisierten Auswertungen ist im Rahmen der Weiterverarbeitung möglich. Die für die „Regelverarbeitung“ der personenbezogenen Daten geltende materielle Schwelle darf dabei nicht höher liegen als jene für die Datenerhebung selbst. Andernfalls liefe die Erhebungsbefugnis ins Leere, da die gewonnenen Daten mangels Verarbeitungsmöglichkeit nicht zweckentsprechend verarbeitet werden könnten. Die Verwendung spezifischer Auswertungsprodukte, deren Eingriffsgewicht über das einer regulären Weiterverarbeitung hinausgeht, ist unter den in § 53 geregelten Voraussetzungen zulässig.

Die automatisierte Weiterverarbeitung kann dabei grundsätzlich auch – dies regelt Satz 2 – unter Verwendung von Anwendungen erfolgen, welche für ihre Funktion selbstlernende Systeme verwenden und anpassungsfähig auf einen autonomen Betrieb ausgelegt sind und hier als „KI-Anwendungen“ legaldefiniert werden. Die Begrifflichkeiten dieser Definition sind dabei weit zu verstehen – die automatisierte Weiterverarbeitung soll umfassend ermöglicht werden und keine Anwendungen sollen in technischer Hinsicht ausgeschlossen werden. Grenzen ergeben sich insoweit lediglich aus Absatz 4 Satz 3 und Absatz 5. Dabei ist die Grenze des Absatzes 4 Satz 3 – das Verbot der Herausbildung oder Verwendung diskriminierender Algorithmen – klarstellend, da der Bundesnachrichtendienst bereits kein Interesse an solchen Algorithmen hat oder haben kann. In Satz 4 und 5 finden sich besondere, verfahrenssichernde Maßgaben für den Einsatz von KI-Anwendungen: Diese sind in erhöhtem Maße zu kontrollieren, um ihr ordnungsgemäßes Funktionieren sicherzustellen. Entsprechend hat der Bundesnachrichtendienst stichprobenartige Kontrollen unter Aufsicht eines Volljuristen (die dann wiederum der Kontrolle durch das administrative Kontrollorgan des Unabhängigen Kontrollrates unterliegen) durchzuführen, ob die Weiterverarbeitungs- oder Entscheidungsprozesse, welche mittels KI-Anwendungen angeleitet sind bzw. getroffen werden, zu zutreffenden Ergebnissen führen. Da es oftmals nicht möglich ist, den genauen Entscheidungsprozess einer KI-Anwendung nachzuvollziehen, ist insoweit regelmäßig sicherzustellen, dass die Entscheidung zur Weiterverarbeitung/Maßnahmenveranlassung auch von einem Menschen aufgrund der vorliegenden Informationen getroffen worden wäre.

Zu Absatz 5

In Absatz 5 findet sich eine – mit der Vorschrift im Rahmen der Befugnis für die Erhebung mittels biometrischem Abgleich vergleichbare – Regelung der „Anschaffungssubsidiarität“. Hierdurch ist bezweckt, dass der Bundesnachrichtendienst nur auf Produkte von Anbietern aus Drittstaaten ausweichen darf, wenn kein gleich geeignetes Produkt in Deutschland oder Europa (oder aus der Eigenentwicklung) verfügbar ist. Hierdurch sollen auch die Souveränität und Unabhängigkeit gestärkt werden. Die Subsidiaritätsregelung greift nur vor einer Anschaffung, sobald diese einmal getätigt wurde, darf die Anwendung auch (beliebig lange)

verwendet werden. Erforderlich ist auch nicht, dass der Bundesnachrichtendienst vor jeder Anschaffung eine umfangreiche Marktprüfung und -analyse durchführt. Es ist hinreichend, dass in periodischen Abständen (z.B. alle 3-5 Jahre) überprüft, welche kommerziell verfügbaren Anwendungen für seine Tätigkeit von Relevanz sein könnten und ob es für diese Anwendungen europäische/deutsche Anbieter gibt.

Nicht erfasst sind Produkte, deren Quellcode öffentlich verfügbar ist (sog. „open source“), da es sich hierbei gewissermaßen um „globale“ Community-betriebene Projekte handelt.

Zu § 53 (Besondere Befugnis zum Abruf von Auswertungsprodukten mit qualifiziertem Eingriffsgewicht)

Die Vorschrift schafft die Befugnis des Bundesnachrichtendienstes zu Abruf von Auswertungsprodukten, welche mittels (der in der Praxis schon zum jetzigen Zeitpunkt immens wichtigen) automatisierten Auswertungen von Daten erstellt wurden. Geregelt wird dabei nicht die Erschaffung von solchen Datenanalysen – diese ist von der allgemeinen Weiterverarbeitungsvorschrift des § 52 erfasst –, sondern ihr Abruf.

Die Differenzierung ist erforderlich, um den gebotenen Ausgleich zwischen dem Grundrechtsschutz Betroffener – für die die automatisierte Datenverarbeitung einen eigenen Eingriff zu begründen vermag – und der Aufgabenerfüllung des Bundesnachrichtendienstes, für die ein Rückgriff auf fortgeschrittene Auswertungswerkzeuge von existenzieller Bedeutung ist, zu wahren.

Die hier verfolgte Systematik orientiert sich dabei an dem zweistufigen Aufbau: Das Eingriffsgewicht wird nicht pauschal beurteilt, sondern präzise bestimmt: Wie bei der Erhebung von Daten im Rahmen der strategischen Aufklärung ist auch bei dem Abruf von Auswertungsprodukten (mit eigenem, „qualifizierten Eingriffsgewicht“) von einem Grundrechtseingriff auszugehen. Dieser bedarf einer Rechtfertigung. Gleichwohl bleibt der Eingriff jeweils in seinem Gewicht reduziert, weil die erhobenen Daten bzw. – für den hier geregelten Fall – die erstellten Auswertungsprodukte gerade noch nicht verwendet werden, sondern zunächst „nur“ in den Dateisystemen des Bundesnachrichtendienstes gespeichert werden. Diesem verminderten Grundrechtseingriff wird durch die Voraussetzungen des § 52 hinreichend entsprochen. Die im zweiten Schritt erfolgende Verwendung begründet demgegenüber einen tiefergehenden Grundrechtseingriff, weil sie gerade erst die inhaltliche Kenntnisnahme durch den auswertenden Bereich ermöglicht und die potentiell nachteiligen Folgen (bis hin zu einer Übermittlung der gewonnenen Erkenntnisse) ermöglicht. Entsprechend sieht § 53 weitergehende Voraussetzungen (erst) für die Verwendung eingriffsintensiver Auswertungsprodukte vor.

Maßgeblich für die hier getroffenen Regelungen sind zudem substantielle Abweichungen in den Verhältnismäßigkeitserwägungen gegenüber vergleichbaren Befugnissen im polizei- und gefahrenabwehrrechtlichen Aufgabenkreis (wie sie insbesondere im Urteil zum Hessischen Gesetz über die öffentliche Sicherheit und Ordnung des BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19 angelegt ist): Diese folgen insbesondere aus dem Umstand, dass der Bundesnachrichtendienst bereits im Vorfeld konkreter (oder auch konkretisierter) Gefahren tätig wird und stattdessen schon mit der Früherkennung von Bedrohungen beauftragt ist. In diesem Stadium der Vorfeldaufklärung ist es von überragender Wichtigkeit, dass der Bundesnachrichtendienst die verfügbaren technischen Möglichkeiten ausschöpft: Einerseits, um zumindest einen Gleichlauf mit Staaten zu erreichen, die die Bundesrepublik Deutschland aufklären und den von diesen ausgehenden Bedrohungen wirksam begegnen zu können. Andererseits, weil im Gefahrenvorfeld im Bereich der Datenerhebung abgesenkte Erfordernisse für kompensative Eingriffsschwellen gelten (insoweit unstrittig, vgl. BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17 mwN) und gleiches auch auf der für die Erkennung von Bedrohungszusammenhängen so bedeutsamen Ebene der anschließenden Weiterverarbeitung gelten muss.

Die in § 53 (in Verbindung mit § 52) angelegte Gesetzessystematik greift diese Wertungsunterschiede in zweierlei Hinsicht auf: Zunächst differenziert die gesetzliche Systematik zwischen der Erstellung von eingriffsintensiven Auswertungsprodukten (die mangels gesonderter Regelung von § 52 erfasst ist) und ihrem Abruf. Der Abruf in diesem Sinne ist der an eine inhaltliche Prüfung anschließende Verarbeitungsschritt, welcher das Auswertungsprodukt für die weitere Verwendung zugänglich macht, es für die anschließenden Weiterverarbeitungsschritte zugänglich macht und es z.B. durch Nutzung in Produkten des Bundesnachrichtendienstes zum Gegenstand der Berichterstattung macht. Mit einem nach Eingriffsintensität gestuften Modell wird zudem dem Verhältnismäßigkeitsgrundsatz differenziert Rechnung getragen. Zwar liegt auch in der Erstellung bereits ein Grundrechtseingriff. Dieser bleibt jedoch in seinem Gewicht begrenzt und bedarf daher keiner über die Regelung des § 52 hinausgehende spezifische Grundlage.

Dies liegt zum einen daran, dass die Auswertungsprodukte gerade automatisiert, also ohne konkrete menschliche Kenntnisnahme erstellt werden. Zu diesem Zeitpunkt ist eine Prüfung etwaiger „Beobachtungsbedürftigkeiten“ schlechterdings noch nicht möglich. Die automatisierte Auswertung muss indes aus technischen Gründen bereits im Hintergrund stattfinden können: Es genügt gerade nicht, eine Befugnis zu schaffen, nach der eine Mitarbeiterin oder ein Mitarbeiter im Bundesnachrichtendienst anlassbezogen einen spezifischen Auswertungsvorgang startet und dort eine konkrete Erstellung eines eingriffsintensiven Auswertungsproduktes zu einem ihm bekannten Bedrohungssachverhalt initiiert. Vielmehr müssen die erforderlichen Datenverknüpfungen auch ohne individuellen Anlass schon im „informationstechnischen Hintergrund“ möglich sein. Nur so lassen sich etwa Muster in verdächtigen Schiffs- oder Flugbewegungen finden, ohne dass eine menschliche Vorfilterung der Daten stattfindet. Zudem lassen sich umfangreiche Auswertungen nur auf diese Weise anfertigen, bevor personelle Verbindungen auch nur im Vagen bekannt sind. Des Weiteren lassen sich ausschließlich dadurch verdächtige Verkehre im Cyberraum identifizieren und aufbereiten, bevor sichere Kenntnis von einem bevorstehenden oder begonnenen Angriff besteht. Zum anderen ist der von einer Erstellung eingriffsintensiver Auswertungsprodukte ausgehende Grundrechtseingriff bereits von § 52 erfasst, weil das Gewicht dieses Eingriffs durch die in § 53 enthaltenen Einschränkungen durch Verwendungsvoraussetzungen rechtssystematisch begrenzt bleibt. Drohen dem Betroffenen aber aufgrund dieser spezifischen Verwendungsvoraussetzungen durch den in der Erstellung liegenden Eingriff allein keinerlei über die Auswertung hinausgehenden Folgemaßnahmen, so bleibt auch das Eingriffsgewicht begrenzt. Dies gilt umso mehr für diejenigen automatisierten Verarbeitungsschritte, die als „Vorprozessierung“ bereits als Teil der Datenerhebung zu betrachten sind, weil zu diesem Zeitpunkt bereits ein Zugriff auswertender nachrichtendienstlicher Mitarbeiterinnen und Mitarbeiter ausgeschlossen bleibt. Die automatisierte Auswertung dient darüber hinaus in vielen Fällen der grundrechtsschonenden Weiterverarbeitung erhobener personenbezogener Daten, indem nicht nachrichtendienstlich-relevante Informationen durch die automatisierte Auswertung bereits verworfen werden können, so dass die menschliche Kenntnisnahme von personenbezogenen Daten von Nichtbetroffenen nicht mehr erfolgen muss.

Neben dieser Differenzierung zwischen Erstellung und Verwendung findet außerdem keine normative Differenzierung zwischen den für die automatisierte Auswertung herangezogenen Datenarten, -mengen, -typen, -herkunft etc. statt. All diese Daten (mit Ausnahme der in § 52 genannten Daten aus Maßnahmen der Wohnraumüberwachung und Online-Durchsuchung) finden gegebenenfalls Eingang in eingriffsintensive Auswertungsprodukte. Dies ist auch zwingend erforderlich, weil die Vorselektion von Daten durch einen Mitarbeiter des Bundesnachrichtendienstes ineffizient und ineffektiv wäre. Zusammenhänge bspw. im Bereich der Proliferations- und Terrornetzwerke oder bei Cyberangriffen ergeben sich regelmäßig erst bei der Gesamtschau der vorliegenden Daten. Aufgrund der Datenmenge ist es für Menschen nicht möglich, vorab potentielle Muster zu erkennen und so die auszuwertenden Quellen vorab zu benennen und zu sortieren. Eine hierüber hinausgehende Daten-Differenzierung würde derart umfangreiche Kennzeichnungserfordernisse und Datenabschottungen bedingen, dass eine technische Umsetzung faktisch unmöglich wäre. Zudem

würde dies dem Ansatz des Bundesnachrichtendienstes, aus den von ihm erlangten Erkenntnissen gerade in umfangreicher strategischer Analyse Muster und Bedrohungen zu erkennen, diametral entgegenlaufen.

Zu Absatz 1

Absatz 1 regelt in Satz 1 zunächst die allgemeine Einschränkung für den Abruf von eingriffsintensiven Auswertungsprodukten. Dieser darf nur erfolgen, wenn eine qualifizierte und der von dem Auswertungsprodukt jeweils ausgehenden Eingriffsintensität kompensierende materielle Schwelle erreicht ist (Nummer 1) oder wenn die Verwendung der Auswertungsprodukte zugunsten von Betroffenen (z.B. zur Feststellung fehlender nachrichtendienstlicher Relevanz) erfolgt (Nummer 2).

Durch den in Nummer 1 angelten Verweis auf die Absätze 2 bis 4 wird – wie im Rahmen der Erhebung – auch insoweit zwischen drei Stufen unterschieden. Die Verwendung von Auswertungsprodukten mit einem eigenen „qualifizierten Eingriffsgewicht“ (dies entspricht der im Rahmen der Erhebung angelegten „Grundstufe“ der „Erforderlichkeit zur nachrichtendienstlichen Auslandsaufklärung“), sowie mit erheblichem (erste Qualifikationsstufe) und herausgehobenem (zweite Qualifikationsstufe) Eingriffsgewicht.

Zu Absatz 2

Absatz 2 regelt, was von Auswertungsprodukten mit qualifiziertem Eingriffsgewicht inhaltlich im Einzelnen umfasst ist.

Es handelt sich um Auswertungsprodukte, die mittels einer automatisierten Auswertung erstellt wurden (Nummer 1), wobei dieser Begriff in technischer Hinsicht sehr weit zu verstehen ist. Inbegriffen sind insbesondere alle denkbaren Arten der Verarbeitungsprogramme, die auf „künstlicher Intelligenz“ bzw. selbstlernender Systeme beruhen.

Erfasst sind einzig solche Prozesse nicht, welche auf einen einfachen Datenabgleich beschränkt bleiben (Nummer 2). Nicht unter den Anwendungsbereich der Norm fallen somit „manuelle“ Auswertungsprodukte oder solche, die von geringer technischer Komplexität sind und sich in einfachen Datenabgleichen erschöpfen. Bei einem einfachen Datenabgleich „erfolgt die Suche nach einem vorhandenen Datenbestand etwa über eine Person, indem im jeweiligen System die eingegebenen Daten des Betroffenen an den gespeicherten Daten vorbeigeführt werden; als automatisches Datenverarbeitungsverfahren führt der Dateienabgleich insoweit regelmäßig Datenbestände zusammen, um Übereinstimmungen der Daten festzustellen oder Daten des einen Bestands in den anderen zu überführen. Der einfache Abgleich ist also ein suchender Vergleich von Daten zur Feststellung von Übereinstimmungen“ (BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19 u.a., Rn. 91f.).

Ab welchem Moment die Eingriffsintensität auch bei einem „einfachen Datenabgleich“ dergestalt erhöht wird, dass durch die Komplexität des suchenden Vergleichs abermals ein eigenes Eingriffsgewicht entsteht, lässt sich nicht pauschal bestimmen. Die von dem Bundesverfassungsgericht genannte „höhere Zahl an Abgleichschritten und Verknüpfungen“ ist dahingehend auszulegen, dass nicht der Abgleich eines Datums (z.B. eines Namens) mit einem vorhandenen Datenbestand (auch über mehrere Datenbanken hinweg) gemeint ist, sondern die „wertende Verknüpfung“, d.h. die inhaltliche Zusammenführung zur Herstellung von Beziehungen, zu wiederum neuen Suchparametern (etwa der Telefonnummer und der Anschrift), die wiederum vollautomatisiert für eigene Abgleiche genutzt werden. Dies wird in Nummer 3 normativ abgebildet. Maßgebend ist insoweit die verfassungsgerichtliche Rechtsprechung, nach der es auf die Generierung neuer, persönlichkeitsrelevanter Informationen ankommt (BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19 u.a., Rn. 69). Diese „neuen Informationen“ zu einer Person, die zwar in den vorhandenen Daten bereits angelegt waren, nicht aber auf herkömmlichen Wege richtig miteinander verknüpft und nur durch den Einsatz automatisierter Verfahren erkennbar und zugänglich gemacht werden können, stellen das besondere eigene Eingriffsgewicht der Verwendung dar.

Ausgenommen werden dabei Auswertungsprodukte, die ausschließlich auf offen verfügbaren Daten beruhen; dies zeichnet die für diese Daten gleichermaßen herabgesenkte Erhebungsschwelle nach.

Gegenstand von Auswertungsprodukten mit qualifiziertem Eingriffsgewicht sind dabei nur inländische Personen und Deutsche. Dies folgt daraus, dass der von der Weiterverarbeitung aufgehende Eingriff in das Recht auf informationelle Selbstbestimmung, welches als Abwehrrecht gerade geschaffen wurde, um das Verhältnis des Bürgers zum Staat zu konturieren und sicherzustellen, dass eine umfassende Teilhabe am gesellschaftlichen Leben ohne Furcht, dass das hoheitliche Gegenüber eine umfassende Datensammlung über jeden Einzelnen anlegt, möglich bleibt, hier ein spezifisches Eingriffsgewicht entfaltet.

Zu Absatz 3

In Absatz 3 ist der Abruf solcher eingriffsintensiver Auswertungsprodukte geregelt, deren Eingriffsgewicht noch nicht die besondere Qualifikation der in Absatz 3 und 4 genannten Beispiele erreicht hat. Gleichwohl gebietet auch hier das von der Datenverarbeitung ausgehende eigene Eingriffsgewicht eine Befugnisnorm und eine spezifische Verwendungsschwelle. Letzteres wird – der allgemeinen Gesetzessystematik entsprechend – durch die Erforderlichkeit im Einzelfall für die nachrichtendienstliche Auslandsaufklärung abgebildet.

Zu Absatz 4

In Absatz 4 wird die Verwendung von Auswertungsprodukten mit erheblichem Eingriffsgewicht geregelt. Diese Auswertungsprodukte sind in Satz 2 abschließend genannt. Ihre Verwendung erfordert – der allgemeinen Systematik entsprechend – die Erforderlichkeit der Verwendung für erhebliche Bedrohungen, wobei hier nicht auf die Erlangung von Informationen zu erheblichen Bedrohungen abgestellt wird, sondern auf die Erforderlichkeit der Verwendung aufgrund einer solchen Bedrohung.

Zu Nummer 1

Bewegungsprofile vermögen weitreichende Informationen zur Lebensführung einer Person zu ermitteln (vgl. hierzu auch BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19 u.a., Rn. 70, 73). Sie stellen deshalb – abhängig von den im Rahmen der Erhebung bestimmten Zeiträumen und vorausgesetzt, sie werden im Rahmen einer automatisierten Auswertung erstellt – denkbarerweise Auswertungsprodukte mit erheblichem Eingriffsgewicht dar. Die durch ein solches Profil entstehende besondere Persönlichkeitsrelevanz stellt – der Wertung des § 26 Absatz 2 entsprechend – unter Umständen (konkret: Einsatz im Inland oder gegenüber Deutschen und bei entsprechendem zeitlichen Umfang) einen erheblichen Eingriff dar und bedarf einer erhöhten Verwendungsschwelle. Entscheidend ist dabei, dass nur solche „nachträglichen Bewegungsprofile“ normativ erfasst sind, die in ihrer jeweiligen Eingriffsintensität denjenigen entsprechen, die durch „klassische“ Methoden (etwa durch GPS-Tracker) angefertigt werden. Somit kommt es also insbesondere auch auf die Genauigkeit der jeweiligen Daten und ihre zeitliche „Taktung“ an – vgl. hierzu § 26 Absatz 3.

Zugleich sind gerade Bewegungsprofile ein Beispiel dafür, dass nicht bereits die Erstellung des Auswertungsproduktes an hohe Schwellen geknüpft werden kann: Die Erstellung von Bewegungsprofilen auf Grundlage von im Rahmen der technischen Aufklärung erhobenen Daten erfolgt gerade nicht nur anlassbezogen, sondern muss bereits Teil der automatisierten Datenverarbeitungsprozesse sein. Erst die Sichtbarmachung, Bewertung und anschließende Verwendung des Bewegungsprofils zusammen ist an eine erhöhte Schwelle geknüpft.

Zu Nummer 2

In Abgrenzung zu konkreten Persönlichkeitsprofilen werden in Nummer 2 solche Auswertungsprodukte geregelt, die nicht zu einer konkreten, bereits im Vorfeld individualisierten

Person erstellt werden, sondern aus einer Vielzahl von Daten eine Person, die im Vorfeld noch nicht als nachrichtendienstlich relevant identifiziert war, herausfiltert, aufbereitet und mit einer Verdachtsprognose versieht. Diese Produkte, die im polizeilichen Bereich als „predictive policing“ bekannt sind, begründen eine besondere Eingriffsintensität, weil sie eine vormals unerkannte Person gerade erst zum Gegenstand nachrichtendienstliches Interesse machen. Diese Fallgruppe ist auch in der Rechtsprechung des Bundesverfassungsgerichtes angelegt (vgl. BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19 u.a., Rn. 98). Dem Regelungsbereich unterfallen dabei (nur) Produkte, welche explizit zu dem Ziel erstellt werden, bislang unbekannte Personen zu identifizieren. Etwaige „Nebenerkenntnisse“ bei anderweitigen Auswertungsprodukten werden hingegen nicht erfasst. Darüber hinaus sind nur solche Produkte erfasst, die der Aufklärung von Verdachtspersonen zu einer erheblichen Bedrohung dienen.

Zu Nummer 3

Persönlichkeitsprofile, welche Aussagen zum individuellen Bedrohungspotenzial einer Person enthalten, bilden die dritte Fallgruppe von Auswertungsprodukten mit erheblichem Eingriffsgewicht. Es handelt sich hierbei um ein Auswertungsprodukt, welches nicht nur eine konkret individualisierte Person zum Gegenstand hat, sondern für diese Person aufgrund der Zielrichtung des Produktes (Bedrohungspotenzial) auch in besonderem Maße mit nachteiligen Folgen verknüpft sein kann. Das Bedrohungspotenzial ist es nämlich, welches gerade weitergehende (auch nachrichtendienstliche) Maßnahmen gegen die betroffene Person wahrscheinlich macht.

Zu Nummer 4

Geregelt sind personenbezogene Vorhersagen und Empfehlungen. Dies schließt etwa ein, dass ein Auskunftsersuchen aufgrund eines Risikoprofils einer bislang unbekannten Person empfohlen wird oder eine Vorhersage zu einer Person aufgrund ihres bisherigen Verhaltens getroffen wird.

Zu Absatz 5

Absatz 5 regelt – wieder der allgemeinen Systematik entsprechend – den Abruf von Auswertungsprodukten mit herausgehobenem Eingriffsgewicht. Abweichend zu Absatz 5 (siehe die dortige Begründung) ist hier eine Bedrohung von herausgehobener Bedeutung materielle Voraussetzung für den Abruf.

Zu Nummer 1

Die in Nummer 1 enthaltenen Persönlichkeitsprofile sind solche, die bei „regulärer Erstellung“ die Voraussetzung einer herausgehobenen Bedeutung haben (vgl. § 26 Absatz 2 Nummer 2). Entsprechendes muss auch bei der nachträglichen Verwendung solcher Profile anhand bereits vorhandener Daten gelten, um Wertungswidersprüche zu vermeiden. Im Einzelnen wird auf die Begründung zu Bewegungsprofilen mit erheblichem Eingriffsgewicht verwiesen.

Zu Nummer 2

In Nummer 2 werden als abschließende Fallkonstellation solche Persönlichkeitsprofile zur Bewertung eines individuellen Bedrohungspotenzials einer Person erfasst, die zur Gewinnung (neuer) höchstprivater Erkenntnisse über eine Person erstellt werden. Der Abruf solcher Erkenntnisse begründet einen besonders schwerwiegenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung, welcher einer besonderen Rechtfertigung bedarf. Dem wird mit dem Erfordernis der zweiten Qualifikationsstufe entsprochen.

Zu Absatz 6

Durch Absatz 6 ist sichergestellt, dass bei Auswertungsprodukten „gegen“ eine Person – die also gezielt zur Auswertung der zu einer konkreten Person vorliegenden Erkenntnisse genutzt werden – die Voraussetzungen des § 20 vorliegen.

Zu Absatz 7

Absatz 7 enthält spezielle Vorgaben für den Fall, dass ein Auswertungsprodukt mit qualifiziertem Eingriffsgewicht den Ausgangspunkt einer autonomen, maschinengestützten Entscheidung mit Folgewirkungen bildet. Dem Grund nach stellt Satz 1 dabei klar, dass die Veranlassung einer Maßnahme (dies meint nur das maßnahmenauslösende Moment, nicht etwa das automatisierte Nachsteuern von Suchbegriffen in der strategischen Aufklärung oder andere, rein maßnahmenbegleitende Elemente) auf Grundlage eines Auswertungsproduktes mit qualifiziertem Eingriffsgewicht nur in Betracht kommt, wenn es sich bei der Maßnahme um ein Auskunftsersuchen gegenüber öffentlichen Stellen handelt. Demgegenüber dürfen Maßnahmen auf Grundlage von Auswertungsprodukten mit qualifiziertem Eingriffsgewicht grundsätzlich nicht für die automatisierte und autonome Veranlassung von Auskunftsersuchen gegenüber nichtöffentlichen Stellen oder nachrichtendienstlichen Maßnahmen genutzt werden. Die erweiterten nachrichtendienstlichen Maßnahmen bilden insoweit einen nicht-regelungsbedürftigen Sonderfall, da diese bereits tatbestandlich nur mit der Zielrichtung einer „fremden Macht“ erfolgen dürfen.

In Satz 2 findet sich eine Ausnahme von dem soeben dargestellten Grundsatz, welche das Themenfeld der „Cyber-Angriffe“ betrifft. Hier ist (schon aufgrund technischer Notwendigkeiten) erforderlich, dass zur Abwehr solcher Angriffe durch Datenlöschung oder Umleitung von Datenströmen in Fällen, in denen eine anderweitige Abwehr nicht zielführend wäre, auch ein autonomes Handeln der automatisierten Systeme zulässig sein muss. Dabei ist denknotwendigerweise auch die Entscheidung, ob ein solcher Angriff vorliegt, welche Maßnahme am geeignetsten ist und ob (nur) eine automatische Veranlassung erfolgsversprechend ist, dem autonomen System vorbehalten.

Zu Absatz 8

Um die datenschutzrechtliche Kontrolle zu ermöglichen (vgl. Absatz 9) ist der Abruf eines Auswertungsproduktes mit qualifiziertem Eingriffsgewicht (also die Entscheidung des Bearbeiters, dieses Produkt für die weitere Auswertung/Weiterverarbeitung zu nutzen und die entsprechenden technischen Schritte eines „Exports“ des Produktes) zu protokollieren.

Zu Absatz 9

Die Verwendung eines Auswertungsproduktes stellt einen Grundrechtseingriff dar, welcher einerseits durch materielle Schwellen, andererseits aber auch durch verfahrenssichernde Vorgaben gerechtfertigt werden muss. Diese Vorgaben trifft Absatz 9, der – angelehnt an § 10 Absatz 2 Antiterrordatei-Gesetz) eine gesonderte und regelmäßige Datenschutzkontrolle durch das administrative Kontrollorgan des Unabhängigen Kontrollrates bei der Verwendung eingriffsintensiver Auswertungsprodukte vorsieht.

Stellt der Unabhängige Kontrollrat im Rahmen der periodischen Prüfung fest, dass es typisierte Auswertungsproduktarten gibt, welche mit den in den Absatz 4 und 5 enthaltenen Fallgruppen vergleichbar sind, so sind diese Produktarten durch den Bundesnachrichtendienst in der Folge auch nur unter den dort genannten Voraussetzungen abrufbar. Die Vorschrift gibt dabei konkrete Vorgaben, welche Faktoren bei der Beurteilung der Vergleichbarkeit zu berücksichtigen sind: Dies sind einerseits die Folgen der Auswertung und andererseits die gewonnene Persönlichkeitserkenntnis, wobei maßgebend darauf abzustellen ist, welche Persönlichkeitsrelevanz konkret besteht. So ist – dies wird beispielhaft genannt – bei Verhalten, welches der jeweiligen Bedrohung dient, keine besondere Persönlichkeitsrelevanz gegeben.

Zu § 54 (Weiterverarbeitung von personenbezogenen Daten aus informationstechnischen Speichern)

§ 54 regelt das Auslesen von personenbezogenen Daten aus elektronischen Speichermedien. Die informationstechnischen Speicher befinden sich dabei im Besitz des Bundesnachrichtendienstes, entsprechend handelt es sich um eine Weiterverarbeitungsvorschrift. Unerheblich ist, ob es sich bei dem Speicher um eine vom informationstechnischen System losgelöste Komponente handelt oder dieser noch in einem Gerät verbaut ist. Ferner ist unerheblich, ob etwaige Zugriffssicherungen überwunden werden müssen. Die Befugnis zur Auswertung umfasst auch das Erstellen von Abbildern des Speichermediums durch den Bundesnachrichtendienst.

Anders als bei einem Zugriff auf informationstechnische Systeme im Sinne der §§ 36 bis 38 handelt es sich bei den dieser Regelung unterfallenden Sachverhalten nicht um eine begleitend zur Nutzung durch den Berechtigten heimlich und typischerweise auch wiederholt unter Zugriff auf sich fortentwickelnde Datenbestände durchgeführte Überwachungsmaßnahme, sondern um das Auslesen eines Speichers, der sich nicht mehr im Besitz seines Nutzers befindet und damit von diesem nicht mehr aktiv genutzt und regelmäßig auch nicht fortgeschrieben wird (insofern ähnlich der Beschlagnahme eines informationstechnischen Systems oder Speichermediums im strafprozessualen Kontext).

Die Regelung berücksichtigt, dass bei elektronischen Speichermedien einerseits eine große Menge an personenbezogenen Daten betroffen sein kann, andererseits vor dem Auslesen dieser Daten in der Regel ungewiss ist, was im Näheren gespeichert ist. Der gesetzliche Tatbestand greift dies in differenzierten Rechtsfolgen auf.

Absatz 2 berücksichtigt eine mögliche besondere Eingriffstiefe der Maßnahme gegenüber der Nutzerin oder dem Nutzer des Speichers sowie das spezifische Eingriffsgewicht der Tätigkeit gegenüber deutschen Staatsangehörigen oder Inländerinnen und Inländern.

Die Regelung wird damit den verfassungsrechtlichen Anforderungen zum Schutz personenbezogener Daten gerecht, die zum Schutz großer und dadurch typischerweise oft mit Blick auf die Persönlichkeit eines Menschen besonders aussagekräftiger Datenbestände erhöhte Befugnisvoraussetzungen fordern.

Zu Absatz 1

Die Befugnis regelt die Informationsgewinnung aus mit dem Einsatz nachrichtendienstlicher Mittel beschafften elektronischer Speichermedien. Nicht unter die Regelung fällt, wenn etwa eine nachrichtendienstliche Verbindung gesammelte Informationen auf einem von ihr dazu genutzten Speichermedium kompiliert und übergibt. Ferner sind auch informationstechnische Speicher, die nicht mit nachrichtendienstlichen Mitteln beschafft wurden und auch nicht von einem ausländischen Nachrichtendienst stammen, nicht von dieser Regelung erfasst; einschlägig sind insofern die allgemeinen Regelungen der § 52ff. Dies betrifft etwa die Asservatenauswertung von durch Innenbehörden beschlagnahmte Speichermedien.

Zu Absatz 2

Absatz 2 trägt dem Umstand Rechnung, dass das Eingriffsgewicht beim Weiterverarbeiten von Datensammlungen aus informationstechnischen Speichern unterschiedlich zu bewerten sein kann. Informationstechnische Speicher können auch sehr große Speicher- oder Verarbeitungskapazitäten besitzen. Absatz 2 regelt daher besondere Verfahren und Verwendungsbeschränkungen zu Sachverhalten gesteigerten Eingriffsgewichts.

Insofern ist also zu berücksichtigen, ob der Speicher eine Datensammlung enthält, die dem eines privat genutzten informationstechnischen Systems entspricht und so tiefe Einblicke in verschiedene Lebensbereiche und damit in die persönliche Lebensführung des Nutzers zulässt (vgl. dazu die Ausführungen in der Begründung zu § 37). Liegt ein solcher

Qualifikationssachverhalt vor, gelten erhöhte Voraussetzungen für die Weiterverarbeitung. Ein solcher Qualifikationssachverhalt ergibt sich jedoch nicht bereits durch das Vorliegen punktueller personenbezogener Daten mitbetroffener Dritter.

Dieser hier in Absatz 2 beschriebene Qualifikationssachverhalt, kann sich einerseits bereits aus den Umständen der Erlangung, die möglicherweise bereits verdeutlichen, dass es sich um ein in einem privat genutzten mobilen Endgerät beschriebenen Speicher handelt, ergeben. Andererseits sind auch Fallkonstellationen denkbar, in denen diese Information nicht vorliegt wie etwa bei einer weitgehend unkommentierten Übergabe durch einen ausländischen Nachrichtendienst. In solchen Fällen wird der Qualifikationssachverhalt für den Bundesnachrichtendienst in der Regel erst im Rahmen der Weiterverarbeitung erkennbar (vgl. hierzu die Ausführungen in der Begründung zu § 37 Absatz 4). Absatz 2 deckt daher beide Konstellationen ab.

Die Ausgestaltung der gesetzlichen Befugnis in Absatz 2 Nummern 1 und 2 trägt auch dem Umstand Rechnung, dass die nachrichtendienstliche Maßnahme gegenüber einer Ausländerin oder einem Ausländer im Ausland ein geringeres Eingriffsgewicht aufweist. Diese Personengruppe unterliegt typischerweise nicht dem Zugriff deutscher Behörden und ist damit in deutlich verringertem Ausmaß Folgemaßnahmen ausgesetzt, vgl. BVerfG Urteil vom 19. Mai 2020, 1 BvR 2835/17 (154, 152), Rn. 186. Für die rechtliche Einordnung der Weiterverarbeitung ist damit maßgeblich, wer das Speichermedium als eigenes privat nutzte – vgl. hierzu die die Ausführungen in der Gesetzesbegründung zu § 37 (privat genutztes informationstechnisches System).

Zu Absatz 3

Soweit die informationstechnischen Speicher mit nachrichtendienstlichen Mitteln in den Besitz des Bundesnachrichtendienstes gelangt sind, findet § 21 unmittelbare Anwendung. Insoweit ist Absatz 3 Satz 1 klarstellend. Die in § 21 enthaltenen Vorgaben zum Kernbereichsschutz gelten indes auch dann, wenn die informationstechnischen Speicher nicht mit nachrichtendienstlichen Mitteln beschafft wurden (etwa durch Übergabe durch einen ausländischen Nachrichtendienst). Diesbezüglich regelt Absatz 3 Satz 2, dass auch in diesen Fällen die Vorgaben für den Kernbereichsschutz zu beachten sind.

Zu § 55 (Datensätze zu minderjährigen Personen)

Die vorgesehen Regelung für die Behandlung von Datensätzen minderjähriger Personen bewahrt einen besonderen Schutz für solche Personen, vereinfacht aber die Rechtsanwendung. Dabei ist der Anwendungsbereich der Norm nur eröffnet, wenn ein Datensatz in Rede steht, also eine Sammlung personenbezogener Daten, die anhand bestimmter Merkmale, die zu den jeweiligen Personen hinterlegt werden, in einer Personendatenbank automatisiert ausgewertet werden können. Nicht erfasst sind damit solche personenbezogenen Daten einer minderjährigen Person, welche nicht gezielt und systematisiert zu einer Person gespeichert sind (oder im Personendatensatz einer anderen Person enthalten sind). Unbenommen bleibt die Möglichkeit, mit Volljährigkeit einer Person einen (neuen) Personendatensatz anzulegen.

Zu Absatz 1

Nach Absatz 1 hat der Bundesnachrichtendienst einen Datensatz einer minderjährigen Person nach einem bestimmten Fristablauf zu löschen. Dieser beträgt bei Personen, die zwischen 16 und 18 Jahre alt sind fünf Jahre, im Übrigen zwei Jahre.

Zu Absatz 2

Absatz 2 stellt klar, dass es bei der Fristenberechnung des Absatzes 1 immer auf denjenigen Zeitpunkt ankommt, zu dem die letzte nachrichtendienstlich relevante Information in den Datensatz aufgenommen wurde.

Zu § 56 (Prüf- und Löschpflichten)

In § 56 sind allgemeine Vorgaben für die Prüfung und Löschung von personenbezogenen Daten vorgesehen, die vom Bundesnachrichtendienst gespeichert wurden.

Zu Absatz 1

In Absatz 1 ist zunächst (klarstellend) geregelt, dass unzulässig gespeicherte Daten unverzüglich zu löschen sind (Nummer 1).

Gleiches gilt, wenn es sich um Daten handelt, die nicht aus allgemein zugänglichen Quellen stammen und die zwar zulässigerweise erhoben und/oder gespeichert wurden, deren nachrichtendienstliche Erforderlichkeit aber nicht oder nicht länger besteht (Nummer 2). Hierbei ist, das wird durch den in Buchstabe a) ausgeführten Zusatz der Notwendigkeit der Daten „alleine oder in ihrer Gesamtheit“ geregelt, nicht erforderlich, dass jedes Datum auf seine individuelle Relevanz geprüft wird. Vielmehr kann sich die Erforderlichkeit für die nachrichtendienstliche Auslandsaufklärung auch aus der „Gesamtheit“ der Daten selbst oder den Umständen ihrer Speicherung, Verwahrung, etc. ergeben. Dies kann regelmäßig etwa der Fall sein, wenn eine große Menge von Daten erhoben wird (etwa nach Maßgabe der §§ 36 bis 38), die erst und gerade in ihrer Gesamtschau eine besondere Bedeutung und Relevanz für die Tätigkeit des Bundesnachrichtendienstes haben, oder wenn z.B. das Zielgerät der Datenerhebung bereits auf die nachrichtendienstliche Relevanz hinweist.

Zu Absatz 2

Absatz 2 löst den bisherigen § 7 Absatz 1 i.V.m. § 12 Absatz 2 Satz 1 und Absatz 3 des Bundesverfassungsschutzgesetzes sowie § 7 Absatz 2 i.V.m. § 13 Absatz 3 Satz 2 und Absatz 4 des Bundesverfassungsschutzgesetzes ab.

Dabei wird die Regelhöchstspeicherfrist auf 15 Jahre angehoben. Diese Anhebung ist insbesondere aufgrund der besonderen Aufgaben des Bundesnachrichtendienstes sachlich gerechtfertigt. Anders als das andere Behörden, die primär inländische Phänomenbereiche mit kürzeren Informationszyklen beobachten, befasst sich der Bundesnachrichtendienst mit der Auslandsaufklärung. Politische Prozesse, die Stabilität fremder Regime oder die Entwicklung transnationaler Bedrohungen vollziehen sich oft in Zyklen, die weit über zehn Jahre hinausgehen. Um historische Kausalitäten und personelle Kontinuitäten bei ausländischen Akteuren verlässlich bewerten zu können, ist eine längere Vorhaltung der Daten fachlich geboten.

Wird ein Datensatz nach zehn Jahren gelöscht und nicht durch einen Ausnahmetatbestand legitimiert, muss er bei bestehendem oder wieder auftretendem Bedarf erneut erhoben werden. Das führt zu zusätzlichem Aufwand, erhöht das Risiko von Lücken und Inkonsistenzen in Lagebildern und kann die Effektivität von Entscheidungsprozessen beeinträchtigen. Die Löschfrist von 15 Jahre stellt sicher, dass bereits aufgearbeitete Informationen über einen ausreichend langen Zeitraum verfügbar bleiben. Darüber hinaus stellt die Frist von 15 Jahren lediglich die äußerste Grenze für das systematische Prüfintervall dar. Die Pflicht, Daten unverzüglich zu löschen, wenn ihre Erforderlichkeit im Einzelfall entfällt, bleibt hiervon unberührt. Die Neuregelung dient somit der administrativen Entlastung und der Anpassung an die Realitäten der langfristigen Informationsgewinnung im Ausland, ohne den grundlegenden Löschungsanspruch bei Wegfall der Erforderlichkeit in Frage zu stellen oder gar aufzuheben.

Eine Speicherfrist von 15 Jahren bietet dem Bundesnachrichtendienst das zeitliche Fundament für den Aufbau langfristiger Personen und Netzwerkprofile. Einzelne, seltene Datensätze gewinnen erst in Kombination mit älteren Informationen an Aussagekraft. Viele sicherheitsrelevante Entwicklungen (z. B. militärische Doktrinen, Cyber Strategien, technologische Fortschritte) zeigen sich erst über Jahre hinweg. Nur ein langer Datenbestand ermöglicht die Identifikation von sukzessiven Änderungen und die Ableitung von Prognosen und

frühe Warnungen bei strategischen Verschiebungen (z. B. neuer Einsatz von KI gestützten Angriffstools). Viele Ereignisse lassen sich zudem häufig erst im Nachhinein vollständig beurteilen (z. B. verdeckte Operationen, “false flag”-Kampagnen). Ohne archiviertes Material kann die Analyse lückenhaft bleiben (z.B. Aufdeckung von verdeckten Aktivitäten (AND), die erst Jahre später klar werden; Bewertung der Wirksamkeit eigener Gegenmaßnahmen). Zuletzt werden auch politische und militärische Entscheidungen oft über ein Jahrzehnt hinweg getroffen. Ein Datenbestand über Jahrzehnte liefert die Basis für Szenario Modelle und Risikoanalysen (Erstellung von „What If“-Szenarien, die den Handlungsspielraum AND simulieren; Unterstützung der Bundesregierung bei langfristigen Sicherheitsstrategien).

Denkbar ist zudem, dass ein längerer Speicherungszeitraum die Beweiskraft von gesammelten Informationen für Gerichts- und parlamentarische Verfahren erhöhen kann. Zudem würden durch gesetzlich definierte Kontrollmechanismen die Maßnahme verhältnismäßig, transparent und rechenschaftspflichtig bleiben, während die strategische Wettbewerbsfähigkeit des Bundesnachrichtendienst gegenüber anderen Nachrichtendiensten nachhaltig gestärkt werden würde.

Die Höchstspeicherfrist gilt dabei nicht für Daten, die aus allgemein zugänglichen Quellen erhoben wurden (Nummer 1 Buchstabe a). Eine anderweitige Regelung wäre insoweit schon nicht praktikabel, da ein Abgleich zwischen den im Bundesnachrichtendienst vorliegenden Daten und den allgemein zugänglichen Daten stattfinden müsste. Zudem werden Social-Media Inhalte oftmals als Gesamtheit zu einer Person/Thema abgezogen. Dabei tragen nicht alle Daten in einem Abzug das gleiche Datum, was zu einer praktisch nicht zu bewerkstelligen Teillöschung führen würde.

Die Höchstspeicherfrist gilt ferner nicht für solche Daten, die zu sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten für einen fremden Staat erhoben wurden (Nummer 1 Buchstabe b). Eine Lösung von der starren Prüfpflicht ist notwendig und gerechtfertigt: Geheimdienste fremder Staaten arbeiten in geheimdienstlichen Operationen regelmäßig langfristig über mehrere Jahre mit klandestinen Strukturen und mit teils tief abgedeckten Legenden. So ist es auch gängige Praxis, dass offiziell „ausgeschiedene/pensionierte“ Mitarbeiter von Geheimdiensten, die mittlerweile für z.B. Wirtschaftsunternehmen tätig sind, hauptamtlich (mit Firmenabdeckung) oder in Zweitfunktion (z.B. unter Legende ohne Wissen der Firmenmitarbeiter) noch immer im Auftrag der jeweiligen Nachrichtendienste operieren. Eine Identifikation derartiger Fälle kann nur durch ausgedehnte Aufbewahrung von personenbezogenen Daten erfolgen. Gleiches gilt für Fälle, in denen Proxy-Koordinatoren (zum Teil nicht hauptamtliche Mitarbeiter, jedoch im engen Austausch mit diesen stehend) über lange Zeit mehrere Netzwerke führen und somit immer wieder in den Fokus der Bearbeitung des Bundesnachrichtendienstes gelangen. Über längere Zeit kann es vorkommen, dass keine Erkenntnisse zu den entsprechenden Akteuren vorliegen. Gerade in diesem sensitiven Bereich und vor dem Hintergrund der veränderten Sicherheitslage gebietet diese Fallkonstellation, dass keine personellen Kapazitäten in bürokratische Formalismen fließen und stattdessen für die tatsächliche und zwingend erforderliche Fallbearbeitung zur Verfügung stehen.

Zu Absatz 3

Absatz 3 entspricht dem bisherigen § 7 i.V.m. § 12 Absatz 2 Satz 2 und 3 BVerfSchG.

Zu Absatz 4

Absatz 4 wird neu eingefügt. Dieser Absatz berücksichtigt, dass beispielsweise die auszuwertenden Daten aus informationstechnischen Speichern oftmals in speziellen forensischen Dateiformaten vorliegen, die zum Schutz der Integrität von forensischen Untersuchungen keine Manipulation oder Löschung von Einzeldaten zulassen. Ebenso lassen sich aber auch personenbezogene Daten unbeteiligter Dritter, die durch Video- oder

Bildaufnahmen erhoben wurden, nur mit einem erheblichen Aufwand von den Daten der eigentlich relevanten nachrichtendienstlichen Erkenntnis oder Person trennen. Auch in diesem Fall soll der Bundesnachrichtendienst nicht dazu verpflichtet sein, die Bilder der mitbetroffenen Dritten beispielsweise unkenntlich zu machen.

Zu Absatz 5

Die bislang in § 27 Absatz 2, § 59 Absatz 2 geregelten Ausnahmen von der Löschpflicht sind nun einheitlich aufgeführt. Mit der Erweiterung der Kontrolle durch den Unabhängigen Kontrollrat auf weitere nachrichtendienstliche Maßnahmen und der Schaffung einer entkoppelten Regelung zur Löschung von Daten im Rahmen dieser Novellierung des BND-Gesetzes wird mit Absatz 5 eine zentrale Regelung geschaffen. Es ist auch klargestellt, wann die Daten in diesen Fällen zu löschen sind.

Zu Absatz 6

Eine Ausnahme von der Löschpflicht besteht ferner dann, wenn es sich um „Produkte“ des Bundesnachrichtendienstes handelt. Produkte sind Dokumente oder sonstige Informationsträger, die der Bundesnachrichtendienst zur Erfüllung seines Auftrages als Ergebnis der Auswertung zuvor erhobener Erkenntnisse erstellt. Hierunter fallen insbesondere die Berichterstattung, Lagebilder, ~~oder~~ Meldungen an andere Stellen, mit welchen der Bundesnachrichtendienst die durch ihn ausgewerteten Erkenntnisse teilt, Operationspläne, Dokumente zu Zielpersonen oder sonstige Unterlagen im Rahmen der Auftragserfüllung. Diese Produkte unterfallen keiner Löschfrist. Von der Ausnahme unberührt bleiben die personenbezogenen Daten und Erkenntnisse, die dem Produkt zugrunde liegen. Für sie gelten die in diesem Gesetz festgelegten Lösch- und Löschwiedervorlagefristen. Als Auslandsnachrichtendienst sieht sich der Bundesnachrichtendienst strategischen und damit typischerweise langfristig ausgerichteten Fragestellungen gegenüber. Um beispielsweise politische Entwicklungen im Ausland fundiert beurteilen zu können, müssen die Produkte des Bundesnachrichtendienstes mit personenbezogenen Daten zu relevanten Akteuren regelmäßig über einen langen Zeitraum hinweg als Hintergrund- und Detailwissen verfügbar sein. In der Regel weisen die Produkte keine personenbezogene Ausrichtung auf, da im Bundesnachrichtendienst eine themen- und sachbezogene Arbeitsweise dominiert, beispielsweise zum Thema Proliferation, Waffenhandel oder zu bestimmten Regionen. Die Produkte des Bundesnachrichtendienstes stellen dessen institutionelles Gedächtnis dar. Sie geben Auskunft darüber, wie der Bundesnachrichtendienst bestimmte Lagen zu vergangenen Zeiten aus welchen Gründen eingeschätzt hat und wie er politische Entscheidungsträger beraten hat. Sie können somit eine zeitgeschichtliche Bedeutung aufweisen. Ferner ist es für den Bundesnachrichtendienst erforderlich Auskunft zu Produkten geben zu können, die er in vergangenen Zeiten mit Partnern geteilt hat, deren Rechtsordnung keine Löschverpflichtung vorsehen.

Die Grundrechtsrelevanz der Produkte wird dadurch abgemildert, dass die Daten und Erkenntnisse, auf die der Bundesnachrichtendienst seine Einschätzungen in den Produkten stützt, weiterhin einer Löschpflicht oder Löschwiedervorlageprüfung unterliegen. So kann sich die in einem Produkt getroffene Einschätzung ausweislich ihrer Quellenangabe beispielsweise auf eine Information beziehen, die mit nachrichtendienstlichen Mitteln erhoben wurde. Obgleich die Einschätzung noch Jahre später eingesehen werden kann, kann die Quellinformation bereits gelöscht und durch den Bundesnachrichtendienst nicht mehr nachvollziehbar sein. Die Quellinformation wiederum steht in einem engeren Zusammenhang zur natürlichen Person, zu der die Information erhoben wurde. Produkte weisen damit im Vergleich zur Quellinformation eine deutliche Abstrahierung auf.

Für Produkte sowie (für Unterlagen allgemein) des Bundesnachrichtendienstes gilt insofern, dass sie in der Regel nur dann gelöscht werden, wenn sie vom Bundesarchiv mangels Archivwürdigkeit abgelehnt wurden (Satz 2). Eine vorherige Löschung bleibt dem Bundesnachrichtendienst unbenommen.

Zu § 57 (Protokolldaten)

Die Vorschrift schafft eine allgemeine Vorgabe für die Behandlung von Protokolldaten. Dabei entspricht der Regelungsgehalt den bereits bislang – indes verstreut – enthaltenen Regelungen in BND-Gesetz und Artikel 10-Gesetz.

Zu Absatz 1

In Absatz 1 findet sich die allgemeine Vorgabe, zu welchen Zwecken die angefertigten Protokolldaten verwendet werden dürfen. Dies sind neben den naheliegenden Zwecken des Datenschutzes, der Datensicherung und der funktionierenden Datenverarbeitungsprozesse insbesondere auch die in Nummer 2 genannten Eigensicherungszwecke. Die Notwendigkeit dieser Verwendung ist evident; der Bundesnachrichtendienst muss anhand der vorhandenen Protokolldaten z.B. nachvollziehen können, welcher Mitarbeitende zu welchem Zeitpunkt einen Zugriff auf welche Daten genommen hat, wenn ein Informationsabfluss im Raum steht. In Satz 2 ist klargestellt, dass auch eine Verwendung für Löschaufforderungen weiter möglich ist (vgl. § 32 Absatz 6 des bisherigen Rechts).

Zu Absatz 2

In Absatz 2 ist geregelt, dass Protokolldaten grundsätzlich bis zum Ablauf des zweiten Kalenderjahres, das auf die Protokollierung folgt, aufzubewahren sind und nach Ablauf dieser Aufbewahrungsfrist unverzüglich zu löschen sind. Mögliche („kann“) Ausnahmen hiervon sind in Satz 2 enthalten; einerseits – dies entspricht den allgemeinen Grundsätzen -, wenn die Daten nicht von erforderlichen Daten getrennt werden können (Nummer 1), und andererseits, wenn es sich um solche Protokolldaten handelt, welche vorgenommene Übermittlungen dokumentieren (Nummer 2). Letzteres dient dabei dem Datenschutz und soll sicherstellen, dass nachvollzogen werden kann, wie oft der Bundesnachrichtendienst an welche Stellen Daten übermittelt.

Zu Absatz 3

In Absatz 3 ist eine deutlich längere maximale Speicherfrist für diejenigen (einheitlich nach Absatz 1 zu erstellenden) Protokolldaten vorgesehen, die zu Zwecken der Eigensicherung vorgehalten werden können. Für die zuverlässige Aufklärung sicherheitsgefährdender und geheimdienstlicher Aktivitäten ist es erforderlich, Protokolldaten über längere Zeiträume auswerten zu können. So sind etwa Sachverhalte pressebekannt, bei denen Innentäter über lange Zeiträume in Nachrichtendiensten aktiv waren bzw. bei denen die sicherheitsgefährden-den und geheimdienstlichen Aktivitäten erst nach langer Zeit entdeckt werden. Es ist hier erforderlich, den zeitlichen und inhaltlichen Umfang derartiger Aktivitäten aufzuklären, um insbesondere feststellen zu können, welche Folgen sich aus den genannten Aktivitäten für den Bundesnachrichtendienst ergeben können. Dies wäre bei Geltung des Absatzes 1 nur sehr eingeschränkt möglich; wenn sich die Aktivitäten auf einen länger zurück liegenden Zeitraum beschränken, wäre eine Aufklärung ohne die Speicherfrist des Absatz 4 womöglich ausgeschlossen.

Für diese Protokolldaten gilt nach Satz 2 eine Zweckbindung; sie dürfen nur für Zwecke der Eigensicherung genutzt werden.

Zu § 58 (Verwendungseinschränkung personenbezogener Daten)

Zu Absatz 1

In Absatz 1 ist nunmehr – unabhängig von der elektronischen Speicherung oder Speicherung in Akten – grundsätzlich festgelegt, dass der Bundesnachrichtendienst bei einer gesetzlich angeordneten Einschränkung der Verwendung (also sowohl der Weiterverarbeitung als auch der Übermittlung) die personenbezogenen Daten entsprechend zu kennzeichnen hat. Die Art der Kennzeichnung kann der Bundesnachrichtendienst selbst

festlegen. Darüber hinaus hat der Bundesnachrichtendienst durch geeignete technische und organisatorische Maßnahmen dafür Sorge zu tragen, dass die personenbezogenen Daten entsprechend ihrer Verwendungsbeschränkung nicht weiterverarbeitet oder übermittelt werden.

Zu Absatz 2

In Absatz 2 Satz 1 ist geregelt, dass (dem bisherigen § 13 Absatz 2 Satz 3 BVerfSchG entsprechend) die gesetzlich angeordnete Verwendungseinschränkung entfällt, wenn die Voraussetzungen für diese Einschränkung nachträglich entfallen. In diesem Fall ist auch die entsprechende Kennzeichnung aufzuheben (Satz 2).

Zu § 59 (Berichtigungspflicht)

Der Bundesnachrichtendienst hat – dem bisherigen § 7 Absatz 1 in Verbindung mit § 12 BVerfSchG entsprechend – personenbezogene Daten zu berichtigen, wenn sie unrichtig sind. Diese Pflicht besteht (nur), wenn der Bundesnachrichtendienst datenverantwortliche Stelle ist und die Daten in seinen Personendatenbanken gespeichert sind. Durch die Einschränkung auf Unrichtigkeiten in Personendatenbänken ist sichergestellt, dass der Bundesnachrichtendienst nicht seinen gesamten Datenbestand nach etwaig unrichtigen Daten durchsuchen muss, sondern sich auf die Datenbanken beschränken kann; einerseits weil diese eine deutlich leichtere Suche ermöglichen, aber andererseits und zuvorderst, weil für betroffene Personen gerade die Speicherung in Personendatenbanken ein besonderes Eingriffsgewicht hat. Zudem greift die Pflicht nur dann, wenn der Bundesnachrichtendienst positive Kenntnis über die Unrichtigkeit hat. Eine Pflicht zur aktiven und ständigen Überprüfung der gespeicherten Daten besteht nicht.

Für Akten ist eine gesonderte Vorschrift in § 62 Absatz 2 enthalten.

Zu § 60 (Weiterverarbeitung zu Forschungs- oder Entwicklungszwecken)

Die Norm sieht eine eigene Weiterverarbeitungsbefugnis für Forschungs- oder Entwicklungszwecke vor. Die Begriffe sind dabei weit zu verstehen und schließen technische Weiterentwicklungen ebenso ein wie die anwendungsorientierte Forschung, Entwicklung und Grundlagenforschung. Diese Vorhaben dienen der Entwicklung neuer nachrichtendienstlicher Fähigkeiten z.B. in der Erfassung und Verarbeitung von Daten, den Plattformen und Systemen dazu oder der Entwicklung neuer Methoden zur Absicherung und Unterstützung der Mitarbeitenden bei der Auftragserfüllung, sowie der Steigerung der Resilienz des Bundesnachrichtendienstes. Weiterhin dient die Forschung und Entwicklung der Aufrechterhaltung bestehender nachrichtendienstlicher Fähigkeiten vor dem Hintergrund des sich rapide verändernden technologischen Umfeldes.

Zu Absatz 1

Forschung und Entwicklung im Bundesnachrichtendienst zielen u.a. darauf ab, neue Technologien für den künftigen nachrichtendienstlichen Einsatz zu erforschen, Prototypen zu entwickeln und zu testen oder Bestandssysteme weiterzuentwickeln. Mit diesen Tätigkeiten sollen einerseits die Effizienz und Effektivität bestehender Systeme gestärkt, aber auch neue Fähigkeiten perspektivisch in den Bundesnachrichtendienst integriert werden. Weltweit besteht derzeit ein Wettbewerb von privaten und öffentlichen Stellen bei der Entwicklung neuer Systeme – insbesondere im Bereich der Künstlichen Intelligenz. Um hier auch nur ansatzweise mithalten zu können, ist es erforderlich, dass der Bundesnachrichtendienst im Rahmen der Verhältnismäßigkeit auch personenbezogene Daten verwendet. Nur durch die Entwicklung eigener Systeme kann der Bundesnachrichtendienst unabhängig von kommerziellen Anbietern anderer Staaten seinen Auftrag im digitalen Zeitalter im Sinne der Sicherheit der Bundesrepublik Deutschland erfüllen.

Im Grundsatz sind bei der Weiterverarbeitung zu Forschungs- und Entwicklungszwecken anonymisierte, d.h. unkenntlich gemachte Daten zu verwenden. Die Unkenntlichmachung darf auch so erfolgen, dass die Eindeutigkeit der Daten erhalten bleibt. Die Unkenntlichmachung soll eine rückwirkende Identifizierung der betroffenen Person unmöglich, jedenfalls aber nur mit unvertretbar hohem Aufwand möglich machen. Die Erhaltung der Eindeutigkeit ist nach der Regelung möglich, jedoch nicht gesetzlich gefordert, wobei eine Eindeutigkeit im Sinne der Vorschrift auch dann erreicht sein kann, wenn die Wahrscheinlichkeit so hoch ist, dass ernsthafte Zweifel nicht mehr bestehen. Bestimmte Anforderungen an das Verfahren zur Unkenntlichmachung werden durch den Gesetzgeber nicht vorgegeben, die Wahl des Verfahrens zur Unkenntlichmachung der Daten bleibt dem Bundenachrichtendienst überlassen.

Satz 2 sieht eine Ausnahme von dem Grundsatz vor, dass unkenntlich gemachte Daten zu verwenden sind. Ein Grund hierfür ist, dass ein entwickelter Prototyp zunächst auf seine Funktionalität und die Validität seiner Ergebnisse getestet werden muss, bevor er in die internen Systeme überführt werden kann. Dafür kann es teilweise erforderlich sein, mit „Realdaten“ (also nicht unkenntlich gemachten Daten) zu arbeiten, die dann auch personenbezogene Daten enthalten. Auf Grund der Tatsache, dass nicht sämtliche Fallkonstellationen von Realdaten mit synthetischen Testdaten nachgestellt werden können, kann auf den Einsatz von Realdaten nicht in jedem Fall verzichtet werden. Gleiches gilt für den Fall, dass eine Unkenntlichmachung nur mit unverhältnismäßigem Aufwand möglich wäre.

Zur Unkenntlichmachung siehe die Ausführungen zu § 32 Absatz 3 Nummer 4.

Zu Absatz 2

In Absatz 2 ist geregelt, dass ausnahmsweise auch eine Einsichtnahme (und anschließende Weiterverarbeitung) in die im Wege der strategischen Aufklärung erhobenen Daten zu Forschungs- oder Entwicklungszwecken möglich ist. Diese Möglichkeit der Einsichtnahme tritt dabei zu den bestehenden Möglichkeiten der §§ 33 und 34 hinzu.

Zu Absatz 3

In Absatz 3 ist geregelt, dass einerseits auf die Entwicklung und das Training von „KI-Anwendungen“ von § 60 umfasst ist. Andererseits werden besondere Vorgaben hierfür getroffen, die in ihren Begrifflichkeiten im Wesentlichen der Verordnung (EU) 2024/1689 des Europäischen Parlaments (so. KI-Verordnung) entlehnt sind. Die Entlehnung bedeutet dabei nicht, dass die Begriffe im Sinne der o.g. Regelungen auszulegen sind. Vielmehr sind die Begriffe nachrichtendienstlich auszulegen. Insbesondere das „angemessene“ Niveau im tatbestandlichen Sinne ist individuell und mit Blick auf die Spezifika des Bundesnachrichtendienstes zu bewerten.

Zu Absatz 4

Die Löschfrist von 15 Jahren begründet sich damit, dass Forschung und Entwicklung in der Regel geraume Zeit benötigen, um valide Ergebnisse zu erhalten. In manchen Forschungsvorhaben wird es zudem nötig sein, längerfristige Trends zu beobachten, bevor diese ausgewertet werden können. Schließlich besteht bei Weiterentwicklungen die Möglichkeit, ausgehend von einem verarbeiteten Grundlagendatensatz zu vergleichen, wie neue Methoden und Ansätze die nachrichtendienstlichen Ergebnisse verbessern. Dafür muss zu einem späteren Zeitpunkt idealiter auf die gleichen Datensätze zurückgegriffen werden können. Eine Verlängerung im Einzelfall ist möglich, falls die Daten weiterhin erforderlich sind.

Zu Absatz 5

In der Regel dürfen Daten, die zum Zweck der Forschung und Entwicklung erhoben wurden, nur zu diesem Zweck verwendet werden. Gleiches gilt für Daten, die zu anderen Zwecken erhoben und sodann zu Forschungs- und Entwicklungszwecken weiterverarbeitet wurden.

Insoweit ist dabei eine Weiterverarbeitung einmal erhobener Daten auch zu verschiedenen Zwecken möglich. So ist es beispielsweise zulässig, erhobene Daten sowohl zur Primäraufgabe der nachrichtendienstlichen Aufklärung (d.h. nach Maßgabe der regulären Weiterverarbeitungsvorschriften) und gleichzeitig auch zu Forschungs- und Entwicklungszwecken weiterzuverarbeiten. Die in Absatz 5 statuierte Zweckbindung gilt insoweit (nur) für den „Forschungs- und Entwicklungszeit“ der Weiterverarbeitung der Daten. Diejenige „Kopie“, welche für die Auftragserfüllung genutzt wird, unterfällt der Zweckbeschränkung nicht.

Bei tatsächlichen Anhaltspunkten einer unmittelbar bevorstehenden Gefahr für ein besonders gewichtiges Rechtsgut muss zudem auch eine Verwendung der zweckgebundenen Daten im Einzelfall möglich sein. Für Daten aus der technischen Aufklärung und gespeicherten Daten aus informationstechnischen Systemen (Asservate), die im dortigen Kontext – ggf. auch parallel zur Verarbeitung zu Forschungszwecken nach Absatz 1 - verschlüsselt verarbeitet werden, gilt § 66 Absatz 2.

Zu § 61 (Errichtungsanordnungen für Personendatenbanken)

Zu Absatz 1

Errichtungsanordnungen sollen beim Umgang mit personenbezogenen Daten für deren grundrechtliche Bedeutung sensibilisieren und für einen entsprechend verantwortungsvollen Umgang bei der datenverarbeitenden Person führen. Die Grundrechtsintensität der Weiterverarbeitung personenbezogener Daten ist deutlich erhöht, wenn eine Person aufgrund von einzelnen Merkmalen automatisiert im Datenbestand des Bundesnachrichtendienstes aufgefunden werden kann. Eine Personendatenbank gewährleistet die Auffindbarkeit einer Person. Vor dem Hintergrund dieser erhöhten Eingriffsintensität, die mit einer Speicherung in einer Personendatenbank einhergeht, ist eine Errichtungsanordnung für Personendatenbanken erforderlich.

Der Unabhängige Kontrollrat hat für Errichtungsanordnungen ein Anhörungsrecht. Dieses ist zentral bei den Zuständigkeiten des Unabhängigen Kontrollrat geregelt, § 97 Absatz 4. Eine Kontrolllücke entsteht durch diese Veränderung nicht, der Unabhängige Kontrollrat kann die Datenhaltung des Bundesnachrichtendienstes im Rahmen der administrativen Kontrolle laufend kontrollieren.

Zu Absatz 2

Absatz 2 regelt die Anforderungen an eine Errichtungsanordnung nach Absatz 1 und entspricht § 14 Absatz 1 BVerfSchG des bisherigen Rechts. Dabei wurden die in Nummer 3 enthaltenen Klammerzusätze (betroffener Personenkreis, Arten der Daten) aus rechtsförmlichen Gründen entfernt, ohne dass hiermit eine Rechtsänderung intendiert ist.

Zu Absatz 3

Absatz 3 regelt wie bislang die Zuständigkeit des Bundeskanzleramtes für die Zustimmung zu den Errichtungsanordnungen. Aus Gründen der Rechtsklarheit und besseren Lesbarkeit in einem gesonderten Absatz.

Zu Absatz 4

Die Dringlichkeitsregelung wurde unverändert aus dem bisherigen § 14 Absatz 3 des Bundesverfassungsschutzgesetzes übernommen, lediglich die Zuständigkeit für das nachzuholende Errichtungsanordnungsverfahren geht von der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit auf den Unabhängigen Kontrollrat über. Dies hat wiederum das Ziel einer einheitlichen Kontrolle aus einer Hand beim Unabhängigen Kontrollrat.

Zu Absatz 5

Die Praxis hat gezeigt, dass mit dieser Neuregelung eine Klarstellung dahingehend erwirkt wird, dass eine Heilung der fehlenden Formalvoraussetzung eines Dateianhörungsverfahrens möglich ist, indem diese bei Erkennen ihres Fehlens unverzüglich nachgeholt wird.

Zu § 62 (Akten)

Die Regelung entspricht in ihrem Regelungsziel dem bisherigen § 13 Absatz 4 des Bundesverfassungsschutzgesetzes, welcher über einen Verweis im bisherigen § 7 Absatz 2 auch auf den Bundesnachrichtendienst anwendbar gewesen ist (BT-Drs. 18/4654, S. 30 f. und S. 37).

Zu Absatz 1

Absatz 1 macht dabei deutlich, dass der Bundesnachrichtendienst personenbezogene Daten auch weiterhin in Akten speichern darf. Wie bislang wird es ihm dabei erlaubt, Personen- und Sachakten zu führen. Das Führen von Sachakten stellt dabei die Regel dar, da es im Bundesnachrichtendienst regelmäßig an einer personenbezogenen Ausrichtung fehlt. Akten im Bundesnachrichtendienst weisen eine stärker themen- und sachbezogene Arbeitsweise aus, beispielsweise zum Thema Proliferation, Waffenhandel oder zu bestimmten Regionen (BT-Drs. 18/4654, S. 37). Personenakten haben für den Bundesnachrichtendienst eine untergeordnete Relevanz. Sie bieten sich an für Personen, die aufgrund ihrer Schutzwürdigkeit gerade nicht zentral in einer Personendatenbank auffindbar sein sollen, deren Informationen aber weiterhin vorgehalten werden müssen, bspw. aus Gründen einer operativen Nachsorge. Häufig enthalten diese Daten auch personenbezogene Daten Dritter, bspw. von Familienangehörigen.

Die Neufassung der Vorschrift vereinheitlich die automatisierte Auswertung der elektronischen Akte mit der Auswertbarkeit von Personendatenbanken. Ein Abgleich ist dabei nicht mehr beschränkt auf Akten eng umgrenzter Anwendungsgebiete (bisheriger § 13 Absatz 4 Satz 4 des Bundesverfassungsschutzgesetzes), da dafür kein Sachgrund ersichtlich ist und sich der Klärungsbedarf bei der Suche vorhandener Informationen zu einer bestimmten Person nicht auf „eng umgrenzte Anwendungsbereiche“ – eine zudem kaum bestimmte Vorgabe – beschränkt. Die Protokollierungsvorgaben entsprechen dem bisherigen § 13 Absatz 4 Sätze 5 bis 7 des Bundesverfassungsschutzgesetzes, wobei die einzelnen zu protokollierenden Daten hier nicht länger normativ bezeichnet werden. Für eine ordnungsgemäße Protokollierung werden dabei indes weiterhin der Zeitpunkt, die Angaben, die die Feststellung der abgefragten Daten ermöglichen, sowie Angaben zur Feststellung des Abfragenden zu protokollieren sein.

Zu Absatz 2

Der Absatz entspricht dem bisherigen § 13 Absatz 2 des Bundesverfassungsschutzgesetzes.

Zu Absatz 3

Absatz 3 gibt im Wesentlichen die Rechtslage des bisherigen § 13 Absatz 3 des Bundesverfassungsschutzgesetzes wieder. Aufgrund des weniger stark ausgeprägten Personenbezugs elektronischer Akten wurde auf eine starre Löschwidervorlagefrist verzichtet. Stattdessen sind Akten zu vernichten, wenn sie für die Aufgabenerfüllung des Bundesnachrichtendienstes nicht mehr erforderlich sind und das Bundesarchiv die Übernehme der Akten mangels Archivwürdigkeit abgelehnt hat (BT-Drs. 18/4654, S. 37).

Zu § 63 (Gemeinsame automatisierte Auswertung mit inländischen öffentlichen Stellen)

Zu Absatz 1

Die Regelung schafft über die bisherigen Regelungen zu gemeinsamen Dateien hinausgehend die Option einer gemeinsamen Weiterverarbeitung. Schon die bisherige Regelung bezweckte keine Verantwortungsdiffundierung zu eingegebenen Daten, sondern den fortbestehenden Datenbesitz der eingebenden Stelle, die damit allein befugt blieb, ihren Datensatz zu ändern oder zu löschen. In der Sache geht es danach darum, dass die beteiligten Behörden nach demselben Datenmodell strukturierte Dateisysteme führen und sich dazu automatisierten Abrufzugriff einräumen. Die Bezeichnung als „gemeinsame Datei“ ist für einen solchen Abrufverbund logisch getrennter Dateisysteme, die die beteiligten Stellen jeweils in eigener Zuständigkeit und Verantwortung führen, eher fehlleitend.

Grundsätzlich sind automatisierte Abrufverfahren bereits nach den allgemeinen Vorschriften zur Durchführung von Ersuchens- und Übermittlungsregelungen möglich. Der Mehrwert des § 63 besteht in einer einheitlichen Befugnisgrundlage aller beteiligten Stellen durch Absatz 2. Dazu ist der Anwendungsbereich mit Absatz 1 auf einen Bereich informationeller Zusammenarbeit bezogen, bei dem ohne Ansehung der beteiligten Stellen eine einheitliche Übermittlungsregelung angemessen gestaltbar ist. Dies ist der Fall, wenn die Aufgabe der nachrichtendienstlichen Auslandsaufklärung wahrgenommen wird und operative Anschlussmaßnahmen grundsätzlich ausgeschlossen sind.

Die in Absatz 1 geregelte Einrichtungsaufgabe umfasst die vorlaufende Koordination der beteiligten Stellen, mündend auch in die Vereinbarung nach Satz 2, sowie unter Umständen technische Services für die Durchführung der Auswertung, wie etwa die Bereitstellung der eigenen Auswertungsanwendung auch für die weiteren beteiligten Stellen. Übernimmt der Bundesnachrichtendienst auch das Hosting der Dateisysteme auf einer von ihm betriebenen technischen Plattform, gilt dafür Absatz 3.

Zu Absatz 2

Satz 1 und 2 synchronisieren die Datenbereitstellung zur gemeinsamen Auswertung mit den jeweils für die innerbehördliche Auswertung getroffenen Regelungen. Im Zusammenwirken mit den Voraussetzungen nach Absatz 1 Satz 1 werden dadurch angemessene Weiterverarbeitungsgrundlagen für die gemeinsame Auswertung geregelt. Dies kann aber nicht für Daten gelten, die nach besonderen Übermittlungsverboten nicht bereitgestellt werden dürfen (Satz 3). Für den Bundesnachrichtendienst betrifft dies insbesondere die Zweckbindungen bei Maßnahmen der Wohnraumüberwachung und der sog. Online-Durchsuchung, sofern die gemeinsame Auswertung nicht den danach geltenden Anforderungen genügt.

Sätze 4 und 5 regeln - komplementär zum Aufgabenrahmen nach Absatz 1 – ein grundsätzliches Verbot operativer Anschlussmaßnahmen. Beispielsweise kommt in Betracht, dass primärer Zweck der Auswertung die Erforschung und Bewertung von Bedrohungen ist (etwa auf Grund gemeinsam erstellter Lagebilder oder der Auswertung nach Vorgehensmustern von Aufklärungsobjekten), dabei aber Erkenntnisse gewonnen werden, die auch zur einschreitenden Gefahrenabwehr oder Strafverfolgung benötigt werden. Eine solche Sekundärnutzung wird dann nach Maßgabe der einschlägigen Übermittlungsvorschriften des BND-Gesetzes geöffnet. Da in solchem Fall sogar die operative Anschlussnutzung nachrichtendienstlich ersterhobener Daten eröffnet ist, kann die Angemessenheit solcher Regelung für einbezogene Daten anderen beteiligter Stellen erstrecht angenommen werden.

Zu Absatz 3

Für die technische Gestaltung der gemeinsamen Auswertbarkeit sind unterschiedliche Varianten denkbar. Dass die verschiedenen Dateisysteme dazu physisch auf einem Server

geführt werden, ist nicht notwendig, möglicherweise aber zweckmäßig. Übernimmt dies der Bundesnachrichtendienst, ist es nach Absatz 3 auch zu den insoweit gebotenen Maßnahmen für die Sicherheit der Datenverarbeitung verpflichtet.

Zu Unterabschnitt 2 (Besondere Weiterverarbeitungsvorschriften für Daten aus der technischen Aufklärung)

In Unterabschnitt 3 finden sich besondere Vorschriften, welche für die Weiterverarbeitung personenbezogener Daten gelten, die der Bundesnachrichtendienst mittels besonderer Befugnisse der technischen Aufklärung erhoben hat. Dabei regeln die nachfolgenden Vorschriften nicht alle Schritte der Weiterverarbeitung von Daten, die im Wege der technischen Aufklärung erhoben wurden, sondern sie verdrängen die allgemeinen Weiterverarbeitungsvorschriften nur partiell. Insbesondere finden die nachfolgenden Vorschriften keine Anwendung auf solche Daten, die zwar dem Schutzbereich des Grundrechtes aus Artikel 10 Absatz 1 des Grundgesetzes unterfallen, aber weder Inhalts- noch Metadaten sind. Bei diesen „anderen mithilfe von Telekommunikationstechniken über Distanz transportierten Daten“ (vgl. BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Rn. 91) ist zwar der Schutzbereich des Fernmeldegeheimnisses ebenfalls betroffen. Gleichwohl rechtfertigt hier die – im Vergleich zu Daten der interpersonellen Kommunikation – herabgesetzte Persönlichkeitsrelevanz und Vertraulichkeitserwartung eine Behandlung der erhobenen Daten nach den (auch für die anderen nachrichtendienstlichen Mittel des Bundesnachrichtendienstes geltenden) allgemeinen Weiterverarbeitungsvorschriften.

Zu § 64 (Besondere Kennzeichnungspflichten für Daten aus der technischen Aufklärung)

Die Regelung konsolidiert die vormals im BND-Gesetz und Artikel 10-Gesetz in den jeweiligen Eingriffsbefugnissen wiederholt geregelten Kennzeichnungspflichten nunmehr für den gesamten Bereich der technischen Aufklärung durch den Bundesnachrichtendienst im Rahmen der Weiterverarbeitungsvorschriften.

Zu Absatz 1

In Absatz 1 finden sich die Kennzeichnungspflichten für personenbezogene Daten, die durch qualifizierte Eingriffe in die Integrität informationstechnischer Systeme erfolgt sind. Dabei ist bei Maßnahmen der „Onlinedurchsuchung“ nach § 37 Absatz 3 eine Angabe zum Mittel der Datenerhebung notwendig. Diese Kennzeichnungspflicht ist schon deshalb notwendig, weil die so erhobenen Daten engen Grenzen verfassungsrechtlichen Grenzen bei der Weiterverarbeitung und Übermittlung unterliegen.

Zu Absatz 2

Da nach Auflösung des Artikel 10-Gesetzes nunmehr ein einheitliches Regime für die strategische Fernmeldeaufklärung geschaffen wurde (siehe hierzu schon oben), kommt der in Absatz 2 Nummer 1 enthaltenen und dem bisherigen § 19 Absatz 7 Satz 2 entsprechenden Verpflichtung des Bundesnachrichtendienstes, den etwaigen qualifizierten Inlandsbezug von personenbezogenen Kommunikationsdaten durch automatisierte Filter, die nach Satz 2 stetig weiterzuentwickeln sind, soweit dies technisch möglich festzustellen, faktisch eine besondere Bedeutung zu. Die Kennzeichnung erfolgt dabei grundsätzlich unmittelbar nach Erhebung.

Die Rechtsprechung des Bundesverfassungsgerichts umsetzend, erstreckt sich diese Verpflichtung (Nummer 2) auch auf das Feststellen einer rein innerdeutschen Übertragung (BVerfG, Beschluss vom 8. Oktober 2024, 1 BvR 1743/16, Rn. 204ff.). Hiervon ausgenommen ist nur die Fallgruppe, in denen der Personenbezug der Daten entfernt wurde (§ 32 Absatz 3 Satz 1 Nummer 4), da es sich insoweit schon nicht mehr um personenbezogene Daten handelt.

Die Kennzeichnungen nach den Nummern 1 und 2 können in einheitlicher Weise umgesetzt werden. Die Vorgabe, die vorhandenen Verfahren kontinuierlich weiterzuentwickeln, schließt alle technischen Möglichkeiten des Bundesnachrichtendienstes ein. Erfordert die Weiterentwicklung der Verfahren eine Weiterverarbeitung der Daten, so ist dies zulässig, solange die Daten nur für diesen Zweck verwendet werden. Bestehen Anhaltspunkte dafür, dass eine automatisierte Auswertung und Analyse der Daten erforderlich sind, um die Verfahren weiterzuentwickeln, so ist auch dies zulässig, um Sorge zu tragen, dass die Kommunikationsdaten mit qualifiziertem Inlandsbezug zuverlässig gefunden werden und damit die Eingriffe in die Grundrechte der betroffenen Personen so gering wie möglich bleiben.

Sollte demgegenüber erst im Rahmen einer späteren Einsichtnahme festgestellt werden, dass ein nach Erhebung nicht automatisiert erkannter qualifizierten Inlandsbezug vorlag, so ist sicherzustellen, dass der qualifizierte Inlandsbezug (regelmäßig durch entsprechende Vormerkung des jeweiligen Telekommunikationsmerkmals) im Rahmen der weiteren Einsichtnahme in andere Kommunikationsdaten entsprechende Berücksichtigung findet; also im Rahmen einer etwaigen Einsichtnahme aus anderen Verkehren des jeweiligen Telekommunikationsmerkmals bei Meldungserstellung eine Kennzeichnung des qualifizierten Inlandsbezugs automatisiert erfolgt. Darüber hinaus können auch durch Maßnahmen nach §§ 37 und 38 kommunikationsbezogene Inhaltsdaten mit qualifiziertem Inlandsbezug erhoben werden. Insoweit ist bei solchen Maßnahmen, bei denen derartige kommunikationsbezogene Inhaltsdaten tatsächlich erhoben werden, dass die entsprechenden Daten auch dahingehend gekennzeichnet werden, um die gesetzlichen Voraussetzungen an die Prüfung- und Löschpflichten zu gewährleisten. Abhängig von der konkreten Fallgestaltung werden nicht bei allen Maßnahmen mittels des Zugriffs auf informationstechnische Systeme (§ 36ff.) laufende Telekommunikation im Sinne des Artikel 10 Absatz 1 des Grundgesetzes erhoben. Da bei Erhebung der Daten aufgrund der regelmäßig sehr großen Datenmengen eine Prüfung dahingehend, ob es sich um kommunikationsbezogene Inhaltsdaten mit qualifiziertem Inlandsbezug handelt, nicht schon bei Erhebung kurzfristig möglich ist (vgl. hierzu § 66 Absatz 4 Satz 1 Nummer 2), erfolgt auch diesbezüglich wie bei dem nachträglichen Erkennen eines qualifizierten Inlandsbezugs die Kennzeichnung (erst) im Rahmen der ersten Weiterverarbeitung nach der erstmaligen Speicherung. Die Kennzeichnung nach Nummer 1 und Nummer 2 darf in identischer Art und Weise vorgenommen werden, das heißt, es werden keine unterschiedlichen Kennzeichnungen für diese Anwendungsfälle benötigt.

Zu Absatz 3

Personenbezogene Daten, die der Bundesnachrichtendienst im Wege der technischen Aufklärung aus einer Vertraulichkeitsbeziehung erhebt, bedürfen – auch wenn die Erhebung nach Maßgabe des § 22 rechtmäßig war – vor ihrer etwaigen Übermittlung einer besonderen Prüfung (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 240). Um dies zu ermöglichen, sind die Daten von Bundesnachrichtendienst entsprechend zu kennzeichnen, sobald er erkennt, dass sie aus einer Vertraulichkeitsbeziehung entstammen.

Zu Absatz 4

Absatz 4 Satz 1 regelt, dass die Kennzeichnung der Daten entfällt, wenn die personenbezogenen Daten an externe Stellen übermittelt werden, und wenn die enthaltenen personenbezogenen Daten vor Übermittlung entfernt wurden (Beispiel: Erhebung einer relevanten Information zu einem Proliferations-Sachverhalt in einer E-Mail zwischen zwei natürlichen Personen; Reduktion auf die reine Sachinformation zum Proliferations-Sachverhalt ohne Bezugnahme auf Personen, da auch die reinen Geräte- und/oder Materialbezeichnungen von großer nachrichtendienstlicher Relevanz sein können).

Die Unkenntlichmachung darf auch so erfolgen, dass die Eindeutigkeit der Daten erhalten bleibt. Die Unkenntlichmachung soll eine rückwirkende Identifizierung der betroffenen Person unmöglich, jedenfalls aber nur mit unvertretbar hohem Aufwand möglich machen. Die Erhaltung der Eindeutigkeit ist nach der Regelung möglich, jedoch nicht gesetzlich

gefordert, wobei eine Eindeutigkeit im Sinne der Vorschrift auch dann erreicht sein kann, wenn die Wahrscheinlichkeit so hoch ist, dass ernsthafte Zweifel nicht mehr bestehen. Gleiches gilt auch für den Begriff der Unmöglichkeit. Bestimmte Anforderungen an das Verfahren zur Unkenntlichmachung werden durch den Gesetzgeber nicht vorgegeben, die Wahl des Verfahrens zur Unkenntlichmachung der Daten bleibt dem Bundenachrichtendienst überlassen.

Ausgenommen von der allgemeinen Regelung zur Kennzeichnungsentfernung bei Übermittlung (Satz 1 Nummer 1) bleiben Daten aus der sog. „Online-Durchsuchung“, deren Kennzeichnung sich nach Absatz 1 richtet. Diese Kennzeichnung ist auch bei Übermittlungen aufrecht zu erhalten (nicht aber bei Entfernung des Personenbezugs). Eine Ausnahme ist hiervon dann vorgesehen, wenn ein Verzicht auf die Kennzeichnung im Einzelfall erforderlich ist und der Unabhängigen Kontrollrat zuvor (oder bei Gefahr im Verzug nachträglich) zustimmt.

Zu § 65 (Besondere Prüfpflichten für Daten aus der technischen Aufklärung)

Der Prüfung von mittels technischen Aufklärungsmaßnahmen verarbeiteten personenbezogenen Daten auf ihren nachrichtendienstlichen Gehalt kommt weiterhin eine besondere Bedeutung zu. Dies folgt daraus, dass durch Mittel der technischen Aufklärung häufig eine Vielzahl von personenbezogenen Daten erfasst werden (können), deren Inhalt zum Zeitpunkt der Erfassung denknotwendigerweise noch nicht bekannt ist. In besonderem Maße trifft dies zu auf die strategische Aufklärung bzw. diesen nachgelagerten strategischen Aufklärungsmaßnahmen – da insoweit gerade eine Ergiebigkeit im Vorfeld nicht voraussehbar ist, sondern zunächst unsystematisch eine Vielzahl von Daten erfasst werden – und auf Zugriffe auf informationstechnische Systeme, mit denen eine große Menge an gespeicherter Daten erhoben werden können, die im Vorfeld nicht inhaltlich gesichtet werden können.

Für personenbezogene Daten, die mit Mitteln der technischen Aufklärung erhoben wurden, zu denen hier keine besonderen Regelungen getroffen werden, gelten die allgemeinen Regelungen für die Weiterverarbeitung personenbezogener Daten. Für personenbezogene Daten, die mit Mitteln der technischen Aufklärung erhoben wurden und in im Rahmen der Auftragserfüllung erstellen Produkten des Bundesnachrichtendienstes enthalten sind, gilt § 56 Absatz 6.

Zu Absatz 1

Die im Wege der strategischen Aufklärung erhobenen personenbezogenen Inhaltsdaten, in die Einsicht genommen wurde, sind bereits im Rahmen der Einsichtnahme auf ihre nachrichtendienstliche Relevanz zu prüfen. Soweit eine Einsichtnahme (zumindest) eine Relevanz ergibt, werden die Daten weiterverarbeitet. Anschließend an diese Weiterverarbeitung hat eine wiederholte Prüfung nach (nunmehr) sechs Jahren daraufhin zu erfolgen, ob die Voraussetzungen der jeweiligen Weiterverarbeitung weiterhin vorliegen, d.h. ob die Daten allein oder zusammen mit bereits vorliegenden Daten zur nachrichtendienstlichen Auslandsaufklärung weiterhin erforderlich sind. Eine Erforderlichkeit ist auch und insbesondere dann gegeben, wenn das der Einsichtnahme zugrundeliegende Ziel der Aufklärung weiterhin nachrichtendienstlich relevant ist.

Die Frist des bisherigen § 27 wurde insoweit von sieben Jahren auf sechs Jahre verringert, was zu einer weiteren Verringerung der (durch die fortwährende Speicherung anhaltenden) Eingriffstiefe führt. Vgl. zur Begründung für die nunmehr nur noch einmal erfolgende Prüfung die Ausführungen zu Absatz 3.

Zu Absatz 2

Absatz 2 trifft besondere Regelungen für die personenbezogenen Daten, die im Wege der Telekommunikationsüberwachung erhoben wurden. Zunächst gilt, dass eine Prüfung der Daten auf ihre nachrichtendienstliche Wertigkeit unverzüglich nach Erhebung zu erfolgen

hat. Dabei ist der Begriff der „Unverzüglichkeit“ im allgemeinen Rechtssinne zu verstehen, setzt also voraus, dass kein „schuldhaftes Zögern“ vorliegt. Eine pauschale Regelung, wie weit dieser Zeitraum zu bemessen ist, verschließt sich dabei. Zur Bestimmung im Einzelfall sind eine ganze Reihe von Faktoren maßgeblich, etwa das Volumen der zu prüfenden Daten, die personelle und kapazitätsmäßige Ausstattung etc. Eine weitere Erforderlichkeit der erhobenen Daten ist auch und insbesondere dann gegeben, wenn das der Datenerhebung zugrundeliegende Ziel der Aufklärung weiterhin nachrichtendienstlich relevant ist. Im Anschluss an diese erstmalige Prüfung erfolgt nach Satz 2 eine (einmalige) weitere Prüfung wie in Absatz 1 nach (spätestens) sechs Jahren.

Zu Absatz 3

Zur Gewährleistung eines besonderen Schutzes der Kommunikation von deutschen Staatsangehörigen, sich im Bundesgebiet aufhaltenden Personen und inländischen juristischen Personen – ist in Absatz 3 festgeschrieben, dass eine erneute Überprüfung der Notwendigkeit der weiteren Datenspeicherung (die ihrerseits den Grundrechtseingriff perpetuiert) bei kommunikationsbezogenen Inhaltsdaten mit qualifiziertem Inlandsbezug nach zwei Jahren zu erfolgen hat. Dies gilt unabhängig von der Maßnahme, mittels derer die Daten erhoben wurden; auch wenn im Rahmen einer Maßnahme nach den §§ 37 und 38 ausnahmsweise ebenfalls kommunikationsbezogene Inhaltsdaten mit qualifiziertem Inlandsbezug erhoben wurden, gilt für diese ebenfalls die Prüffrist nach Absatz 3.

Die im Artikel 10-Gesetz angelegte Prüffrist von sechs Monaten wurde insoweit unter Erwägungen wirtschaftlicher Verwaltung auf zwei Jahre verlängert und auch nicht endlos periodisch fortgeschrieben, sondern erfolgt künftig (nur noch) einmalig. Angesichts der erfolgten Erstselektion ist eine wirksam gestaltete nochmalige Routineüberprüfung erst nach 2 Jahren sinnvoll, da laufende Erkenntnisse zur Erforderlichkeit ohnehin in die laufende Bearbeitung eingehen und speziell bei Abschluss einer Maßnahme danach eine generelle Überprüfung der Wertigkeit gewonnener Erkenntnisse erfolgt. Eine spätere Neubewertung, die nicht von einer neuen Information veranlasst ist, sondern im Rahmen neuerlicher Gesamtschau erfolgt, kommt ernstlich erst mit einem wesentlich verbreiterten Bild von Folgeerkenntnissen in Betracht. Das bisher sehr kurze Überprüfungsstakkato ist danach eine Bürokratieroutine ohne relevanten Effekt für den Grundrechtsschutz. Dies gilt ebenso für die dauerhafte Fortführung der Routinen. Bei bereits gesichert als erforderlich eingeschätzten Informationen kommt dem keine weitere Bedeutung zu. Deshalb werden die Sonderprüfungen zugleich nach 2 Jahren abgeschlossen. Dies führt nicht zu einem Wegfall von Prüfroutinen, sondern zur Einbettung in das allgemeine Verfahren der Weiterverarbeitungsvorschriften. Bei bereits gesichert als erforderlich eingeschätzten Informationen kommt dem keine weitere Bedeutung zu. Dies führt nicht zu einem Wegfall von Prüfroutinen, sondern zur Einbettung in das allgemeine Verfahren der Weiterverarbeitung. Der Reformansatz der operativen Stärkung soll gerade auch vermeiden, dass operativer Ressourcen für unzweckmäßige Bürokratieroutinen gebunden werden. Wenn sie durch solche Aufwände vom Einsatz zur Gefahrerforschung abgehalten werden, beeinträchtigt dies wirksamen Rechtsgüterschutz.

Zu Absatz 4

Zuletzt sind in Absatz 4 besondere Prüfpflichten für personenbezogene Daten, die im Rahmen des Auslesens technischer Spuren bei informationstechnischen Angriffen nach § 36 verarbeitet wurden, geregelt. Da die Verarbeitung insoweit bereits auf Erhebungsebene beschränkt ist, ist auch im Rahmen der weiteren Prüfung der Erforderlichkeit der Daten eine entsprechende Begrenzung angezeigt. Flankiert wird dies in Absatz 4 Satz 3 durch eine Begrenzung bei der Auswertung von dem Bundesnachrichtendienst gefertigten Datenkopien, bei denen unverzüglich zu prüfen ist, ob jenseits der in § 14 Absatz 1 Satz 2 Nummer 2 bezeichneten Informationen auch weitere personenbezogene Daten enthalten sind. In Bezug auf die Trennbarkeit von Daten findet § 56 Absatz 4 Anwendung.

Zu § 66 (Besondere Löschpflichten für Daten aus der technischen Aufklärung)

Die Vorschrift enthält besondere Löschpflichten für kommunikationsbezogene Daten aus der technischen Aufklärung. Für sonstige personenbezogene Daten, die mit Mitteln der technischen Aufklärung erhoben wurden, zu denen hier keine besonderen Regelungen getroffen werden, gelten die allgemeinen Regelungen für die Weiterverarbeitung personenbezogener Daten. Für personenbezogene Daten, die mit Mitteln der technischen Aufklärung erhoben wurden und in im Rahmen der Auftragserfüllung erstellen Produkten des Bundesnachrichtendienstes enthalten sind, gilt § 56 Absatz 6.

Zu Absatz 1

In Absatz 1 ist zunächst der Umgang mit den im Rahmen der strategischen Aufklärung erhobenen personenbezogenen Daten geregelt. Wie bereits ausgeführt steht darf der Bundesnachrichtendienst, in diese personenbezogenen Daten unmittelbar anschließend an ihre Erhebung im Rahmen einer strategischen Aufklärungsmaßnahme Einsicht nehmen. Dem Bundesnachrichtendienst ist es nunmehr nach Absatz 1 auch möglich, die personenbezogenen Daten zunächst für bis zu sechs Monate zu speichern und erst zu einem späteren Zeitpunkt (innerhalb dieser sechs Monate) im Wege der Einsichtnahme auf sie zuzugreifen. Die vergleichsweise kurze Speicherfrist ist geboten, da bereits die Erhebung der (u.a.) personenbezogenen Kommunikationsdaten im engeren Sinne einen Grundrechtseingriff darstellt (vgl. hierzu ausführlich oben), obschon eine inhaltliche Auswertung zu diesem Zeitpunkt noch nicht erfolgt und nicht erfolgen kann. Dieser Grundrechtseingriff ist nur zu rechtfertigen, wenn die Speicherdauer eng begrenzt bleibt. Während der sechsmonatigen Speicherdauer darf der Bundesnachrichtendienst auch die Suchbegriffe, die er im Rahmen der Eignungsprüfung erkannt hat, in eine laufende Aufklärungsmaßnahme überführen und die kommunikationsbezogenen Inhaltsdaten mit diesem Suchbegriff nutzen, um relevante Verkehre im Datenspeicher (einschließlich des Verkehrs, welcher zur Generierung des Suchbegriffes genutzt wurde) zu finden.

Führt die Einsichtnahme zu einer Weiterverarbeitung der Daten – weil sie für die nachrichtendienstliche Auslandsaufklärung erforderlich sind –, so finden grundsätzlich (mit Ausnahme der weiteren in diesem Unterabschnitt enthaltenen Bestimmungen) die allgemeinen Weiterverarbeitungsvorschriften des Unterabschnittes 1 Anwendung.

Zu Absatz 2

Erhebt der Bundesnachrichtendienst mit Befugnissen der technischen Aufklärung verschlüsselte Daten oder Daten, die aus anderen Gründen durch den Bundesnachrichtendienst nicht lesbar gemacht werden können (z.B. aufgrund unbekannter/neuartiger technischer Protokolle), so ist eine Speicherung von bis zu fünfzehn Jahren zulässig. Dies folgt daraus, dass die Verschlüsselung bzw. Nichtlesbarkeit eine Einsichtnahme und anschließende inhaltliche Nutzbarmachung verhindert, sodass sich auch das Eingriffsgewicht dieser Verarbeitungsschritte nicht manifestieren kann. Da es sich bei den Daten gleichwohl um nachrichtendienstlich relevante Daten handeln kann, soll der Bundesnachrichtendienst die Möglichkeit erhalten, diese Daten über die üblichen Zeiträume hinweg vorzuhalten. Nach Satz 2 kann in besonderen Ausnahmefällen auch eine Speicherung verschlüsselter Daten über den in Satz 1 genannten Zeitraum zulässig sein. Dies wird insbesondere bei solchen personenbezogenen Daten anzunehmen sein, bei denen der Bundesnachrichtendienst bereits Kenntnis von der Wertigkeit hat, indes lediglich aus technischen Gründen eine Entschlüsselung oder sonstige Lesbarmachung der Inhalte (weiterhin) nicht möglich ist. Die Befugnis zur Speicherung umfasst auch lesbare Daten, soweit diese nicht oder nur mit unverhältnismäßig hohem Aufwand von den nicht lesbaren Daten trennbar sind oder eine Trennung den Zweck der Speicherung gefährden würde. Letzteres betrifft dabei insbesondere auch den Fall von „lesbaren“ Metadaten bei „unlesbaren“ Inhaltsdaten. In Satz 3 ist geregelt, dass im Anschluss an eine Lesbarmachung das „reguläre“ Regime des Absatzes 1 gilt, also eine Einsichtnahme innerhalb von sechs Monaten erfolgen muss, soweit

es sich um Daten aus der strategischen Aufklärung handelt. Im Übrigen gelten im Anschluss die regulären Prüfpflichten.

Zu Absatz 3

Absatz 3 regelt ein unverzügliches Löschgebot für kommunikationsbezogene Inhaltsdaten mit qualifiziertem Inlandsbezug, bei denen es sich nicht um Metadaten handelt, wenn eine Einsichtnahme unter Missachtung der Vorgaben des § 34 Absatz 2 erfolgt ist (Nummer 1) oder – insoweit klarstellend – eine Prüfung der Relevanz der Daten deren fortbestehende Erforderlichkeit nicht bestätigt (Nummer 2). Im Rahmen der Löschpflicht der Nummer 1 erfolgt dabei nur eine Löschung derjenigen Datenkopien, welche im Rahmen der Weiterverarbeitung Verwendung gefunden haben. Dies bedeutet, dass die Daten aus der ursprünglichen Erhebung – solange der Zeitraum der Datenspeicherung noch nicht abgelaufen ist – weiter im Datenspeicher vorgehalten werden können.

Ausgenommen von der Löschpflicht sind solche Daten, die zur Prüfung der Rechtmäßigkeit der Datenverarbeitung, insbesondere für Kontrollzwecke des Unabhängigen Kontrollrats, oder zur Erfüllung von Mitteilungspflichten weiter benötigt werden. Dies gewährt keinesfalls eine allgemeine Vorhaltung sämtlicher Daten für etwaige künftige Kontrollen, erforderlich ist vielmehr ein konkreter Anlass, der eine fortgesetzte Speicherung rechtfertigt.

Zu Absatz 4

In Absatz 4 ist eine Sondervorschrift für Erhebungsarten mit hier gesondert geregelten Speicherbefugnissen. Dies geht darauf zurück, dass diese Erhebungsbefugnisse typischerweise zu einer solchen Vielzahl von Datenerhebungen folgen, dass eine inhaltliche Prüfung jedes Datums auf seine jeweilige Wertigkeit faktisch unmöglich wäre. Darüber hinaus ist den hier genannten Daten regelmäßig gemein, dass sie gerade nicht isoliert für sich genommen bereits von nachrichtendienstlicher Relevanz sind, sondern oft erst in ihrer Gesamtheit Rückschlüsse und Auswertungen zulassen.

Letzteres trifft dabei insbesondere auf die in Nummer 1 geregelten kommunikationsbezogenen Metadaten zu. Diese Daten sind von der (Vorab-)Prüfung auf ihre nachrichtendienstliche Wertigkeit nach Absatz 2 ausgenommen und unterliegen zudem einer weitergehenden Speicherfrist von bis zu fünfzehn Monaten. Die Vorschrift greift den bisherigen § 26 Absatz 5 auf, verlängert zugleich die dortige Speicherfrist und beinhaltet nunmehr auch die kommunikationsbezogenen Metadaten, die im Wege der Telekommunikationsüberwachung erhoben wurden. Bereits im bisherigen § 26 Absatz 5 ist die Möglichkeit der Verlängerung der Speicherfrist über die sechs Monate hinaus vorgesehen, wenn eine Speicherung für die Aufgabenerfüllung des Bundesnachrichtendienstes weiterhin erforderlich ist. Da dieser Fall in der Praxis sehr oft Anwendung vorkommt, wurde die Speicherfrist angepasst. Rein faktisch ist die Verlängerung der Frist erforderlich, da der Bundesnachrichtendienst insbesondere auch bei periodisch auftretenden Ereignissen (zum Beispiel bei sich jährlich wiederholenden militärischen Übungen) in die Lage versetzt werden muss, diese zielgerichtet und vergleichend anhand der erhobenen kommunikationsbezogenen Metadaten zu analysieren.

In Nummer 2 werden diejenigen personenbezogenen Daten, die mittels Maßnahmen der (begrenzten) Erhebung gespeicherter Daten aus informationstechnischen Systemen (§§ 37 und 38) erhoben wurden, einer Speichermöglichkeit von bis zu 36 Monaten belegt. Diese Daten werden durch die hier getroffene Vorschrift von den allgemeinen Speicherbefugnissen (von bis zu fünfzehn Jahren) ausgenommen. Stattdessen darf der Bundesnachrichtendienst diese Daten nur für einen deutlichen kürzeren Zeitraum von 36 Monaten – welcher in der Wertung dem bisherigen Recht entnommen wurde, vgl. § 4 Absatz 7 Satz 2 – speichern. Die leitende Erwägung ist hier, dass der Bundesnachrichtendienst mit den in Rede stehenden Maßnahmen eine Vielzahl von Daten erhebt, für die eine gewisse Speicherfrist notwendig ist, um eine sinnvolle Auswertung zu ermöglichen (so auch schon in

§ 34 Absatz 7). Zugleich darf wegen der potentiellen Persönlichkeitsrelevanz der erhobenen Daten die pauschale Speichermöglichkeit nicht überdehnt werden.

Die in Satz 2 enthaltene Möglichkeit einer über die spezifischen Speicherzeiträume hinausgehenden Speicherung entspricht dem bisherigen § 26 Absatz 5. Die dort enthaltende Regelung für „Metadaten“ wird nunmehr (auch) auf die übrigen Fallkonstellationen der vorsorgenden Speicherung bestimmter Datenarten aus der technischen Aufklärung (also insbesondere auch auf Daten aus Eingriffen in informationstechnische Systeme) erstreckt. Dies geschieht einerseits, um die Rechtslage zu vereinfachen und künftig nur noch ein einziges Verfahren für die längere Speicherung vorzusehen (anstelle wie bislang zwei Verfahren nach § 26 Absatz 5 und § 24 Absatz 7 Satz 2). Andererseits wird die Befassung des Unabhängigen Kontrollrates für die „Verlängerung“ (über die Unverzüglichkeit hinaus) der Speicherzeiträume aufgehoben. Letztere Regelung war dabei bereits im geltenden Recht unzureichend: Eine „unverzügliche“ Prüfung kann im Einzelfall durchaus auch länger als drei Jahre andauern; eben dann, wenn aufgrund großer Datenmengen insoweit kein „schuldhaftes Zögern“ vorlag. Durch die Verlagerung dieser Entscheidung zum Bundesnachrichtendienst – der im Rahmen der Verlaufskontrolle selbstverständlich gleichwohl vom Unabhängigen Kontrollrat kontrolliert wird – werden zudem unnötige Bürokratien abgebaut.

Zur Bejahung der Erforderlichkeit einer längeren Speicherung im Einzelfall ist es insoweit ausreichend, dass das der Datenhebung zugrundeliegende Ziel der Aufklärung weiterhin nachrichtendienstlich relevant ist; eine Prüfung jedes einzelnen erhobenen Datums ist mithin nicht erforderlich.

Zu Absatz 5

Soweit der Bundesnachrichtendienst im Rahmen der Verarbeitung von Daten aus Eingriffen in IT-Systeme feststellt wird, dass die vor der Datenerhebung getroffene Prognose hinsichtlich der Nutzung des IT-Systems nicht als „Eigenes für die private Lebensführung“ unzutreffend war, mithin erst im Nachhinein festgestellt wird, dass das IT-System ausschließlich oder weit überwiegend als eigenes für die private Lebensführung genutzt wird, ist neben dem Vorliegen der entsprechenden materiellen Voraussetzungen insbesondere auch die notwendige Anordnung der Behördenleitung zur Datenerhebung nebst Rechtsmäßigkeitsprüfung des Unabhängigen Kontrollrats unverzüglich nachzuholen. Gleiches gilt, wenn im Nachhinein festgestellt wird, dass sich die Maßnahme gegen eine Person mit deutscher Staatsangehörigkeit oder eine sich im Bundesgebiet aufhaltenden Person gerichtet hat. Bis zur Entscheidung durch den Unabhängigen Kontrollrat dürfen die erhobenen Daten nicht weiter ausgewertet werden. Wenn die Anordnung nicht erfolgt oder deren Rechtmäßigkeit nicht bestätigt wird, sind die erhobenen Daten zu löschen.

Damit ist denknotwendigerweise verbunden, dass eine Löschung der Daten unterbleibt, während eine Anordnung der Maßnahme, deren Erforderlichkeit erst nachträglich festgestellt wurde, eingeholt wird und vom Unabhängigen Kontrollrat geprüft wird.

Zu Absatz 6

In Absatz 6 ist eine Ausnahme von den in den Absätzen 3 bis 5 enthaltenen Löschpflichten für die eng begrenzten Fälle statuiert, in denen eine Weiterverarbeitung oder Übermittlung der personenbezogenen Daten zur Abwehr einer unmittelbar bevorstehenden Gefahr – also einer Sachlage, bei der das schädigende Ereignis bereits begonnen hat oder unmittelbar oder in allernächster Zeit mit an Sicherheit grenzender Wahrscheinlichkeit bevorsteht - für ein besonders gewichtiges Rechtsgut erforderlich ist. Dies greift die Rechtsprechung des Bundesverfassungsgerichts auf, dass in diesen Fällen ausdrücklich eine Ausnahme angenommen hat (vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 174).

Zu Absatz 7

Absatz 7 regelt, dass Löschungen nach dieser Norm unter Aufsicht eines Bediensteten mit Befähigung zum Richteramt zu erfolgen haben. Hiermit ist nicht gemeint, dass ein solcher Bediensteter der Löschung bzw. derjenigen oder demjenigen, die oder der die Löschung tatsächlich ausübt – sei es auf technische Art und Weise, sei es durch tatsächliche Vernichtung von Material – körperlich anwesend und in physischer Präsenz beizuwohnen hat; etwa dadurch, dass er sich in der selben Amtsstube aufhält, wie die Person, welche den Löschvorgang durch Tastendruck initiiert. Vielmehr meint eine „Aufsicht“ hier in lebens- und praxisnaher Auslegung, dass die Verantwortlichkeit für die ordnungsmäße Durchführung der Löschung durch eine Bedienstete oder einen Bediensteten mit Befähigung zum Richteramt durch geeignete organisatorische und aufsichtliche Maßnahmen sicherzustellen ist.

Zu § 67 (Besondere Protokollierungspflichten für Daten aus der technischen Aufklärung)

Die Pflicht in Nummer 1, eine Einsichtnahme und Löschung personenbezogener Kommunikationsdaten mit qualifiziertem Inlandsbezug zu protokollieren, greift die Regelung des § 5 Absatz 2 Satz 4 Artikel 10-Gesetz auf und verfolgt zwei Ziele: Zum einen wird dem besonderen Schutz der Daten mit qualifiziertem Inlandsbezug durch eine verfahrenssichernde Protokollierung bereits auf administrativer Seite entsprochen. Durch die Notwendigkeit einer Protokollierung wird so bereits der Bundesnachrichtendienst selbst gehalten, die besondere Schutzbedürftigkeit zu berücksichtigen. Darüber hinaus ist die Protokollierung entscheidend, um sicherzustellen, dass auch in den Fällen, in denen die personenbezogenen Daten selbst gelöscht wurden, eine wirksame Kontrolle möglich bleibt. Diese Kontrolle erstreckt sich dabei nach den allgemeinen Weiterverarbeitungsvorschriften insbesondere auch auf eine etwaige gerichtliche Nachprüfung und sieht eine Ausnahme von der Pflicht vor, die Protokolldaten am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen. Das Gesetz setzt insoweit die Rechtsprechung des Bundesverfassungsgerichts um (BVerfG, Beschluss vom 8. Oktober 2024, 1 BvR 1743/16, Rn. 204ff.).

Die Löschung von Daten nach § 66 Absatz 5 (vgl. die dortigen Ausführungen) ist ebenfalls zu protokolieren (Nummer 2).

Nummer 3 ist der entsprechenden Regelung aus dem Artikel 10-Gesetz (§ 11 Absatz 1a Satz 6) übernommen. Der Verweis auf die weitergehenden Protokollierungspflichten dieses Gesetzes erfolgt klarstellend.

Zu Abschnitt 6 (Übermittlung von personenbezogenen Daten)

Abschnitt 6 regelt die Übermittlung von personenbezogenen Daten durch den Bundesnachrichtendienst. Dabei sehen einige der hier geregelten, konkreten Übermittlungsbefugnisse vor, dass eine Übermittlung auch „automatisiert“ erfolgen kann. Damit ist gemeint, dass eine Übermittlung ohne vorherige Prüfung der nachrichtendienstlichen Relevanz der Daten erfolgen kann, also regelmäßig im sofortigen Anschluss an die Datenerhebung. Darüber hinaus kann eine Übermittlung von Daten, deren nachrichtendienstliche Relevanz bereits feststeht (sei es aufgrund einer Einzelfallprüfung, sei es aufgrund der Relevanz eines gesamten „Datenpakets“), ebenfalls auf automatischem Wege erfolgen. Dies schließt auch eine Übermittlung im unmittelbaren Anschluss an die Erhebung ein, wenn aufgrund der jeweiligen Spezifika feststeht, dass nur Daten bzw. „Datengesamtheiten“ von Relevanz erhoben wurden. Ein Beispiel hierfür wäre etwa die sofortige Übermittlung von Daten, die zu einem laufenden Cyberabwehr erhoben wurde, an inländische öffentliche Stellen. Hier findet keine „automatisierte“ Übermittlung im o.g. Sinne einer Rohdatenübermittlung statt, gleichwohl können die Daten, z.B. nach §§ 82 und 84, sofort automatisch an das Bundesamt für Sicherheit in der Informationstechnik übermittelt werden, da aufgrund der Einzelfallumstände regelmäßig von einer Relevanz der Daten auszugehen ist.

Zu Unterabschnitt 1 (Politische Unterrichtung und Information der Öffentlichkeit)

Zu § 68 (Politische Unterrichtung)

§ 68 ersetzt den bisherigen § 65 Absatz 1 und 2.

Die zuvor in einem gemeinsamen mit der Information der Öffentlichkeit in einem Paragraphen geregelte politische Unterrichtung wird nunmehr aus Gründen der Übersichtlichkeit und besseren Lesbarkeit in einem gesonderten Paragraphen geregelt. Ergänzt wird die Unterrichtungsmöglichkeit, auch an die den Landesregierungen nachgeordneten Stellen (Absatz 1 Satz 2).

Im Übrigen wurde der bisherige § 65 Absatz 1 Satz 3, der die Nichtanwendung der regulären Übermittlungsvorschriften statuiert hat, gestrichen, da sich diese Nichtanwendbarkeit nunmehr bereits aus der systematischen Verortung ergibt. Eine Ausnahme ist weiterhin in den gesetzlich gesondert aufgeführten Fällen (vormals nur § 11b Absatz 5) vorgesehen.

Zu § 69 (Information der Öffentlichkeit)

§ 69 entspricht im Wesentlichen dem bisherigen § 65 Absatz 3. Ausdrücklich aufgenommen ist nun, dass der Bundesnachrichtendienste auch Fachkreise über Erkenntnisse informieren kann. Im Unterschied zu der allgemeinen Öffentlichkeit kann hier eine Information an einen kleinen abgrenzbaren Personenkreis erfolgen, der gerade nicht für alle zugänglich ist. Dies ist zum Beispiel bei einer Information auf einem Fachforum, z.B. zum Thema Cybersicherheit oder Organisierte Kriminalität der Fall. Der Begriff der Historie wurde ersetzt durch den Begriff „Geschichte“, eine inhaltliche Änderung ist damit nicht intendiert.

Zu Unterabschnitt 2 (Vorgaben zur Übermittlung von personenbezogenen Daten durch den Bundesnachrichtendienst)

Die Regelungen dieses Unterabschnitts gelten für alle Übermittlungen der Unterabschnitte 3 und 4. Damit sind die allgemeinen Vorgaben dieses Unterabschnittes weder für die politischen Unterrichtungen nach § 68 noch die Information der Öffentlichkeit nach § 69 anzuwenden.

Zu § 70 (Zweckbindung der übermittelten personenbezogenen Daten)

Die Regelung entspricht dem bisherigen § 9a. Die Überschrift wurde aus redaktionellen Gründen angepasst.

Zu § 71 (Protokollierung der Übermittlung)

Die Regelung entspricht im Wesentlichen dem bisherigen § 9b Absatz 1. Die bisherigen § 9b Absatz 2 und 3 wurde in § 57 Absatz 2 Satz 1 und § 57 Absatz 2 Nummer 1 übernommen.

Zu § 72 (Verbundene personenbezogene Daten)

Die Regelung entspricht dem bisherigen § 9c.

Zu § 73 (Pflicht zur Übermittlung vervollständigter oder berichtigter Daten)

Die Regelung entspricht dem bisherigen § 9d.

Zu § 74 (Verbot der Übermittlung)

Die Regelung entspricht im Wesentlichen dem bisherigen § 9e. Im Interesse einer schlanken Gesetzgebung wurde Absatz 2 nicht übernommen da es in der Praxis keine

Anwendungsfälle gab und absehbar auch in Zukunft nicht geben wird. Die Streichung des Absatzes 2 ist gleichzeitig eine Angleichung an das MAD-Gesetz.

Zu § 75 (Schutz von minderjährigen Personen bei Übermittlungen)

Die Regelung greift den bisherigen § 9f und § 24 des Bundesverfassungsschutzgesetzes auf, gliedert deren Inhalt systematischer und harmonisiert auch die Formulierung systematisierend. Zudem erfolgt eine querschnittliche Regelung für Inlands- wie Auslandsübermittlungen.

Wird die Beobachtung eines vormals Minderjährigen als Erwachsener fortgesetzt, erfolgt zu den vorhandenen Daten bei Übermittlungen sachgerecht keine Differenzierung danach, ob sie noch zum Verhalten im Minderjährigenalter angefallen waren. Entscheidend ist hier, ob auch solche Daten für den Übermittlungszweck erforderlich sind.

Zu Absatz 1

Absatz 1 enthält die Vorgaben für Übermittlungen an inländische Stellen. Zunächst gilt im Grundsatz, dass eine Übermittlung erfolgen darf, wenn ausgeschlossen ist, dass eine Weiterverarbeitung zu negativen rechtlichen Folgen für die betroffene Person führen würde oder diese Person auf andere Weise erheblich beeinträchtigen würde (Nummer 1). Möglich ist eine Übermittlung darüber hinaus auch zur Gefahrenabwehr und Strafverfolgung, solange die minderjährige Person mindestens vierzehn Jahre alt ist (Nummer 2). Dies entspricht im Wesentlichen dem bisherigen § 9f Absatz 2. Ausnahmsweise ist auch eine Übermittlung von personenbezogenen Daten von minderjährigen Personen, welche noch nicht vierzehn Jahre alt sind, zulässig (Nummer 3). Dies ist (nur) dann der Fall, wenn eine konkretisierte Gefahr für eines der enumerativ genannten, besonders gewichtigen Rechtsgüter vorliegt und auf die Gefahrenabwehr beschränkt.

Zu Absatz 2

Absatz 2 enthält die Vorgaben für die Übermittlung von personenbezogenen Daten von minderjährigen Personen an ausländische öffentliche Stellen. Hierbei kann eine Übermittlung an EU-, NATO oder angrenzende Staaten grundsätzlich unter den gleichen Kautelen wie im Rahmen von Inlandsübermittlungen nach Absatz 1 erfolgen (Nummer 1).

An andere Staaten ist eine Übermittlung nur möglich, wenn ausnahmsweise ein besonderes nachrichtendienstliches Interesse an der minderjährigen Person – Ausländer im Ausland – besteht, etwa bei den Thronfolgern einer südostasiatischen Diktatur (Nummer 2 Buchstabe a). Eine Übermittlung ist ferner auch an ausländische Strafverfolgungsbehörden nach § 86, wobei hier ein dringender Tatverdacht Voraussetzung ist (Nummer 2 Buchstabe b), sowie nach § 82 zur Gefahrenabwehr, wobei hier abermals eine Verengung der Rechtsgüter im Falle einer Übermittlung der Daten von Personen unter 14 Jahren erfolgt, zulässig. Die in § 86 enthaltenen Vorgaben für die Übermittlung an ausländische Stellen sind jeweils zu berücksichtigen.

Zu § 76 (Übermittlung im Interesse der betroffenen Person)

Die Regelung greift den bisherigen § 9h auf, vereinfacht diesen aber. Dabei erfolgt künftig eine allein objektive Interessenbetrachtung (weiterhin beschränkt auf eine „Offensichtlichkeit“ der Interessenlage). Beispielsweise bei einer Mitteilung entlastender Erkenntnisse an Strafverfolgungsbehörden ist eine vorherige Einwilligung des Betroffenen nicht erforderlich. Bei einigen Sachverhalten kann nicht sachgerecht auf eine hypothetische Einwilligung abgestellt werden, etwa wenn der Betroffene sich aufgrund psychischer Probleme selbst gefährdet oder eine Gefährdung eines minderjährigen Betroffenen gerade vom Personensorgeberechtigten ausgeht. Die Änderung dient daher gleichermaßen der Effizienz als auch der Effektivität der Schutzmaßnahme für die tatsächliche betroffene Person.

Rechtssystematisch handelt es sich um eine eigene Übermittlungsvorschrift. Ergänzt wurde die Möglichkeit, in diesen Fällen auch automatisiert zu übermitteln.

Zu § 77 (Vorgaben für die Übermittlung von personenbezogenen Daten aus besonderen Erhebungsarten)

Die Vorschrift enthält die – konsolidierten – Sonderregelungen für die Übermittlungen von personenbezogenen Daten, welche mit besonderen Eingriffsbefugnissen erlangt wurden. Dies sind die Befugnisse zu Wohnraumüberwachungen (§§ 29 und 113) sowie zum Eingriff in eigengenutzte informationstechnische Systeme (§ 37 Absatz 3). Sollte ausnahmsweise ein Eingriff nach § 120 in ein eigengenutztes informationstechnisches System erfolgen, fallen auch die in diesem System erhobenen Daten in den Anwendungsbereich der Vorschrift; da § 120 indes nicht zwischen verschiedenen Gerätearten unterscheidet, ist eine Pauschalverweisung insoweit nicht möglich.

Die Vorschrift unterscheidet jeweils zwischen der Übermittlung an Strafverfolgungsbehörden (jeweils Buchstabe a) und an sonstige Stellen (jeweils Buchstabe b), und trägt dem Kriterium der hypothetischen Datenneuerhebung Rechnung, indem die Weiterverarbeitung zur Gefahrenabwehr den hierzu verfassungsrechtlich gebotenen Zweck- und Schwellenvoraussetzungen folgt und die Übermittlung zur Strafverfolgung an den Straftatenkatalog der strafprozessualen Ermittlungsbefugnis gebunden wird (§ 100c Absatz 1 Nummer 1 verweist auf § 100b Absatz 2 StPO). Unter die sonstigen Stellen fallen sowohl inländische wie ausländische, als auch öffentliche wie nicht öffentliche Stellen.

Dabei folgen die besonderen Vorgaben für die Übermittlungen von Daten aus Wohnraumüberwachung und dem Eingriff in komplexe informationstechnische Systeme unmittelbar der verfassungsgerichtlichen Rechtsprechung (BverfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 228, 388).

Zu § 78 (Einrichtung automatisierter Abrufverfahren)

§ 78 enthält – komplementär zu § 10 Absatz 2 Satz 3 – eine Regelung zur Einrichtung automatisierter Abrufverfahren. Zur Beurteilung, ob ein geeigneter Fall vorliegt, sind sowohl rechtliche Kriterien (speziell die Gewährleistung der Übermittlungsverbote nach § 73) wie auch fachliche Aspekte, die einerseits in technischen Bedingungen liegen und andererseits bei einem Nachrichtendienst im typischerweise gebotenen Geheimschutz, zu berücksichtigen. Ziel der Einrichtung eines automatisierten Abrufverfahrens ist, dass die Verantwortung der Datenweiterverarbeitung klar zugeordnet wird und nach demselben Datenmodel strukturierte Datensysteme geführt werden müssen, bei denen dann automatisierte Abrufzugriffe eingeräumt werden können. Praktische Anwendungsfällte kommen insbesondere in der Zusammenarbeit mit dem Bundesamt für den Verfassungsschutz oder dem Bundesamt für den Militärischen Abschirmdienst in Betracht.

Zu Unterabschnitt 3 (Übermittlung von personenbezogenen Daten durch den Bundesnachrichtendienst)

Zu § 79 (Übermittlung an inländische Nachrichtendienste)

Die Regelung entspricht dem bisherigen § 11, wobei in Nummer 1 die Begrifflichkeit angepasst wurde. Ergänzt wurde die Möglichkeit, Daten auch automatisiert an inländische Nachrichtendienste zu übermitteln.

Zu § 80 (Übermittlung an die Bundeswehr)

Die Regelung ist Ausdruck der besonderen Zusammenarbeit des Bundesnachrichtendienstes als einzigem Auslandsnachrichtendienst der Bundesrepublik Deutschland (vgl. § 1 Absatz 1) mit der Bundeswehr. Der Bundesnachrichtendienst ist damit auch mit der militärischen Aufklärung beauftragt. Dies setzt voraus, dass auch personenbezogene Daten,

die für die Aufgabenwahrnehmung der Bundeswehr erforderlich sind, unmittelbar und ohne Zeitverzug an die Bundeswehr übermittelt werden können. Der Bundesnachrichtendienst versorgt die Bundeswehr mit für die Aufgabenerledigung der Bundeswehr unverzichtbaren Informationen, insbesondere zur Landes- und Bündnisverteidigung sowie zu Einsätzen im Ausland, aber auch zu sonstigen Aufgabenwahrnehmungen der Bundeswehr. Nur durch die enge Zusammenarbeit des Bundesnachrichtendienstes mit der Bundeswehr kann die äußere Sicherheit der Bundesrepublik Deutschland uneingeschränkt wahrgenommen werden. Im Koalitionsvertrag der 21. Legislaturperiode (ab Rn. 3971) wurde dazu u.a. vereinbart: „Wir werden sämtliche Voraussetzungen schaffen, damit die Bundeswehr die Aufgabe der Landes- und Bündnisverteidigung uneingeschränkt erfüllen kann. Unser Ziel ist es, dass die Bundeswehr einen zentralen Beitrag zur Abschreckungs- und Verteidigungsfähigkeit der NATO leistet und zu einem Vorbild im Kreis unserer Verbündeten wird."

Für eine uneingeschränkte Aufgabenerfüllung der Bundeswehr sind die Informationen des Bundesnachrichtendienstes zentral. Aus diesem Grund sind die Übermittlungsbefugnisse des Bundesnachrichtendienstes an die Bundeswehr gesondert zu regeln.

Die Bundeswehr wird bei der Wahrnehmung ihrer Aufgaben, insbesondere zur Landes- oder Bündnisverteidigung sowie der Vorbereitung oder Durchführung von Auslandseinsätzen, in einem eng begrenzten Aufgabenbereich auf Grundlage verfassungsunmittelbarer Befugnisnormen sowie – je nach Einzelfall – von Bundestagsmandaten und/oder völkerrechtlichen Rechtsgrundlagen, die auch als nationales Recht gelten, tätig. Die Bundeswehr dient in allen ihren originären Tätigkeitsfeldern dem Schutz überragend wichtiger Rechtsgüter wie der Verteidigungs- und Bündnisfähigkeit der Bundesrepublik Deutschland, und damit letztlich auch zu Leib und Leben der Bevölkerung im Rahmen der Landes- oder Bündnisverteidigung sowie Leib und Leben von Soldatinnen und Soldaten im Auslandseinsatz.

Die Bundeswehr wird ggf. auf Grundlage der durch den Bundesnachrichtendienst übermittelten personenbezogenen auch mittels belastenden Folgemaßnahmen gegenüber Betroffenen tätig. Dabei handelt es sich jedoch nicht um die Ausübung „operativer Anschlussbefugnisse" im Sinne der verfassungsgerichtlichen Rechtsprechung zur Übermittlung personenbezogener Daten. In seiner bisherigen Spruchpraxis zu Überwachungsbefugnissen und Datenverarbeitung hat das Bundesverfassungsgericht daher konsequenterweise keine entsprechenden Vorgaben für die Bundeswehr entwickelt.

Hintergrund hierfür ist verfassungsrechtliche Sonderrolle der Bundeswehr, die im Wesentlichen durch drei Merkmale gekennzeichnet ist:

Zum einen wird die Bundeswehr im bewaffneten Konflikt tätig, für den die Maßgaben des Humanitären Völkerrechts gelten. Die vom Bundesverfassungsgericht zum Grundrechtsregime entwickelten Maßstäbe lassen sich darauf nicht übertragen. Weiterhin darf die Bundeswehr als „Parlamentsheer" in bewaffnete Unternehmungen ausschließlich aufgrund einer vorherigen Entscheidung des Bundestags im Einzelfall einbezogen werden. Dieser wehrverfassungsrechtliche Parlamentsvorbehalt (vgl. BVerfG, Urteil vom 12. Juli 1994, 2 BvE 3/92 u.a., Rn. 321ff.; Urteil vom 7. Mai 2008, 2 BvE 1/03, Rn. 58ff.; Urteil vom 23. September 2015, 2 BvE 6/11, Rn. 65ff.) bildet die Legitimationsbasis für das Handeln der Bundeswehr. Zuletzt bildet die Bundeswehr gemeinsam mit dem Bundesnachrichtendienst ein integriertes System der äußeren Sicherheit. Der Bundesnachrichtendienst ist neben seiner Funktion als ziviler Auslandsnachrichtendienst auch der mit der militärischen Auslandsaufklärung betraute Nachrichtendienst der Bundesrepublik Deutschland und ist arbeitet insofern technisch und personell äußerst eng mit der Bundeswehr zusammen.

Vor diesem Hintergrund ist es nicht erforderlich, die vom Bundesverfassungsgericht entwickelten Maßstäbe für Datenübermittlungen durch Nachrichtendienste an andere öffentliche Stellen mit operativen Anschlussbefugnissen, wie etwa Polizeien, auf das Verhältnis des Bundesnachrichtendienstes zur Bundeswehr anzuwenden.

§ 80 regelt insofern typisierend den Grundfall der Datenübermittlungen des Bundesnachrichtendienstes als ziviler und militärischer Auslandsnachrichtendienst an die Bundeswehr zur Stärkung der Verteidigungs- und Bündnisfähigkeit.

Nicht umfasst ist der atypische Ausnahmefall des Einsatzes der Bundeswehr im Bereich der Amtshilfe für die Polizei nach Artikel 35 Absatz 2 und 3 des Grundgesetzes sowie in einem inneren Notstand nach Artikel 87a Absatz 4 des Grundgesetzes. In diesen Fällen wird die Bundeswehr außerhalb ihrer originären Aufgaben quasi-polizeilich tätig. Um eine Umgehung der für die Polizeibehörden geltenden strengen Anforderungen zu verhindern, sind in diesen Fällen dieselben Übermittlungsvoraussetzungen wie für die Übermittlungen an Polizeien geboten.

Zu Absatz 1

Der Bundesnachrichtendienst übermittelt personenbezogene Daten an die Bundeswehr, wenn dies für die Einsatzbereitschaft und Sicherheit der Bundeswehr oder verbündeter Streitkräfte erforderlich ist (Nummer 1). Umfasst sind davon sowohl operativ-taktische wie auch strategische Informationen. So benötigt die Bundeswehr z.B. auch personenbezogene Daten zur Krisenfrüherkennung im Ausland. Informationen die für die Funktionsfähigkeit und Sicherheit der Bundeswehr erforderlich sind umfassen u.a. geplante Sabotageakten im Zusammenhang mit der Bundeswehr. Ohne die entsprechenden personenbezogenen Daten könnte die Bundeswehr keine kontinuierliche Bewertung der Sicherheitslage durchführen und die erforderlichen Maßnahmen ergreifen.

Die Übermittlung ist auch zulässig zur Landes- und Bündnisverteidigung (Nummer 2). Die Übermittlung findet insbesondere statt zum Erhalt der Handlungsfähigkeit der Bundesrepublik Deutschland, zum Schutz der Bevölkerung und Institutionen sowie zur Verteidigung seines Territoriums gegen Angriffe und Bedrohungen von außen, vgl. auch § 2 Absatz 2 Nummer 2 nebst Begründung. Der Begriff Landes- und Bündnisverteidigung ist weit zu verstehen und umfasst insbesondere sämtliche Vorfeldmaßnahmen, die vor dem Eintritt des Verteidigungsfalls oder Bündnisfalls getroffen werden, um verteidigungsfähig zu sein, umfasst. Dies setzt insbesondere auch die Krisenfrüherkennung und Erstellung informierter Lagebilder voraus.

Zur Vorbereitung und Durchführung von Auslandseinsätzen (Nummer 3) benötigt die Bundeswehr zwingend personenbezogene Daten. Sie sind Grundlage der Erarbeitung verschiedener Planungsprozesse auf strategischer, operativer und taktischer Ebene und zielen dabei regelmäßig unmittelbar auf belastende Folgemaßnahmen unter Einhaltung verfassungs- und völkerrechtlicher Normen gegenüber betroffenen Dritten ab. Bewaffneten Konflikten inhärent sind hohe Dynamiken und damit regelmäßig nicht vorhersehbaren Eskalationsgeschwindigkeiten. Kurze Reaktionsmöglichkeiten sind daher die Norm und nicht die Ausnahme. Zur konsequenten Wahrnehmung ihres verfassungsrechtlichen Auftrages auch zum Schutz überragend wichtiger Rechtsgüter ist die Nutzung von durch den Bundesnachrichtendienst übermittelten Daten bereits in der Vorbereitungs-/Planungsphase von Auslandseinsätzen unabdingbar. Der Begriff der Auslandseinsätze ist weit zu verstehen und beinhaltet insbesondere auch einsatzgleiche Verpflichtungen.

Zu Absatz 2

Essentiell ist die Möglichkeit der Datenübermittlung ohne Zeitverzug. Die Bundeswehr ist zur Erfüllung ihrer Aufgaben auf valide und schnelle Datenübermittlung angewiesen. Diese kann in vielen Fällen nur durch eine automatisierte Datenübermittlung ohne vorherige Prüfung der Datenrelevanz gewährleistet werden. Auch insoweit ist zu berücksichtigen, dass es sich hierbei nicht um einen regulären zwischenbehördlichen Austausch von Daten handelt, sondern die Bundeswehr mit dem Bundesnachrichtendienst als auch mit der militärischen Aufklärung betrauten Auslandsnachrichtendienst ein integriertes System des militärischen Handelns bildet. Das heißt, dass der Bundesnachrichtendienst Daten auch für die

Bundeswehr erhebt. Dies erfordert eine auch automatisierte, echtzeitnahe Datenübermittlung von Rohdaten.

Zu § 81 (Übermittlung an inländische öffentliche Stellen zur Strafverfolgung)

Die Regelung ersetzt den bisherigen § 11a. In Ansehung der fortgeführten Rechtsprechung des Bundesverfassungsgerichts und von Bedarfen der Strafrechtspflege werden die Vorgaben zur Übermittlung personenbezogener Daten zur Strafverfolgung hier neu gefasst.

Zu Absatz 1

Die Regelung entspricht dem bisherigen § 11a Absatz 1 Satz 1. Ersucht eine Strafverfolgungsbehörde den Bundesnachrichtendienst um Übermittlung von Daten, liegt die Verantwortung für die Zulässigkeit des Ersuchens bei ihr. Der Bundesnachrichtendienst prüft allerdings, ob von ihm anzuwendende besondere Übermittlungsregelungen entgegenstehen. Dies sind hier die Schranken der speziellen Übermittlungsbefugnis des § 74. Der Bundesnachrichtendienst muss danach prüfen, ob die Strafverfolgung wegen einer besonders schweren Straftat nach Absatz 2 erfolgt. Einer sphärenzugeordneten Verantwortungsverteilung entspricht dabei, dass die Dichte des Verdachtes, der das Ersuchen initiiert, nur von der ersuchenden Strafverfolgungsbehörde einzuschätzen ist. Der Bundesnachrichtendienst kann faktisch nicht nachvollziehen, ob dem Ersuchen bestimmte Tatsachen zugrunde liegen, die Daten zur Strafverfolgung erforderlich sind oder die Verdachtsannahme überhaupt berechtigt ist.

Zu Absatz 2

Der Absatz 2 definiert die besonders schweren Straftaten neu und trägt damit der Rechtsprechung des Bundesverfassungsgerichts Rechnung (vgl. BVerfG, Beschluss vom 17. Juli 2024, 1 BvR 2133/22). Die Qualifizierung einer Straftat als schwer oder besonders schwer muss nach diesem Beschluss in der Strafnorm selbst einen objektivierten Ausdruck finden (a.a.O., Rn. 206).

Dieser objektivierte Ausdruck bleibt dabei allerdings nicht auf den Strafrahmen reduziert, wenngleich dieser einen maßgebenden Anhaltspunkt für die Schwere einer Straftat liefert (a.a.O., Rn. 202). Vielmehr können auch andere Umstände, „tatbestandlich umschrieben, das besondere Gewicht der Straftat begründen“ (a.a.O., Rn. 205). „Maßgeblich für die Schwere des tatbestandlichen Unrechts sind der Rang des verletzten Rechtsguts und andere tatbestandlich umschriebene, gegebenenfalls auch in einem Qualifikationstatbestand enthaltene Begehungsmerkmale und weitere Tatfolgen“ (a.a.O., Rn. 202). Dem trägt die Nummer 2 Rechnung.

Der Umstand, dass eine Übermittlung nur im Falle einer besonders schweren Straftat möglich ist, schränkt dabei nicht das Legalitätsprinzip der Strafverfolgung ein. Übermittelt der Bundesnachrichtendienst einen Sachverhalt, so hat die Strafverfolgungsbehörde diesen unter allen in Betracht kommenden Gesichtspunkten zu würdigen. Ergeben sich aus dem übermittelten Sachverhalt andere Straftaten, die für sich genommen nicht schwer genug wiegen, dass sie eine Übermittlung rechtfertigen würden, so kann auch dieses Delikt selbstverständlich verfolgt werden, unabhängig davon, ob das Ausgangsdelikt der Übermittlung sich gerichtsverwertbar anklagereif verdichten lässt.

Übermittelt der Bundesnachrichtendienst beispielsweise wegen des Verdachts einer Mitwirkung an einem Organhandel (strafbar nach § 18 des Transplantationsgesetzes) und übermittelt dabei einen Sachverhalt, welcher zugleich eine Körperverletzung begründet, so darf die empfangende Behörde auch die Körperverletzung weiterverfolgen.

Zu Nummer 1

Der bisherige § 11a Absatz 1 Satz 2 Nummer 1 ist vom Bundesverfassungsgericht bestätigt worden (a.a.O. Rn. 203, 212) und wird hier übernommen.

Zu Nummer 2

Für die Qualifizierung einer Straftat als besonders schwer kann auch das geschützte Rechtsgut sowie dessen Bedeutung für die Rechtsgemeinschaft von Belang sein und daher ergänzend zum Strafrahmen berücksichtigt werden (a.a.O. Rn. 205). Für die Festlegung, welche Straftatbestände als besonders schwer gelten sollen, kann der Gesetzgeber neben dem Rückgriff auf bestehende Kataloge auch einen eigenen Katalog schaffen (a.a.O. Rn. 206). Die Anlage zu § 81 listet daher Delikte auf, die eine Höchststrafe von fünf Jahren Freiheitsstrafe vorsehen und tatbestandlich durch Tatbegehung oder -folgen zur besonders schweren Straftat qualifiziert sind.

Zu § 82 (Übermittlung an inländische öffentliche Stellen zur Gefahrenabwehr)

Die Trennung des bisherigen § 11b in drei gesonderte Vorschriften (§§ 82 bis 84) dient der Vereinheitlichung der Systematik der Gesetze der Nachrichtendienste des Bundes. Das BND-Gesetz wird dabei an die Systematik des Bundesverfassungsschutzgesetzes und des Gesetzes über den Militärischen Abschirmdienst angeglichen.

Entsprechend sieht das Gesetz nun eine Übermittlung an inländische öffentliche Stellen in drei „Kategorien“ vor: Erstens eine Übermittlung zur Gefahrenabwehr bei Vorliegen einer konkretisierten Gefahr in § 82. Zweitens eine Übermittlung zum „administrativen Rechtsgüterschutz“ (so die Terminologie des Bundesverfassungsschutzgesetzes und des Gesetzes über den Militärischen Abschirmdienst), bei denen in eng umrissenen Ausnahmen auch im „Gefahrenvorfeld“ (so die Terminologie des BND-Gesetzes) eine Übermittlung ermöglicht wird, § 83. Leitend ist insoweit die Überlegung, dass die Übermittlung hier von konkreten Risikofaktoren veranlasst ist, die das Gefährdungspotenzial der jeweiligen Bedrohung steigern und auf die danach zum vorbeugenden Rechtsgüterschutz administrativ-ordnungsbehördlich einzuwirken ist (vgl. hierzu auch die Begründung des bisherigen § 20 des Bundesverfassungsschutzgesetzes in BT-Drs. 20/9345, S. 24). Drittens ist eine Übermittlung dann möglich, wenn die Informationen für Aufgaben der empfangenen Stelle erforderlich sind, die dem Schutz besonders gewichtiger Rechtsgüter dienen und (darüber hinaus) die Wahrnehmung der Aufgaben ohne operative Anschlussmaßnahmen zu Lasten der betroffenen Person erfolgt, § 84. Der bisherige § 11b Absatz 2 wird somit im Ergebnis aufgetrennt und der dort enthaltene Katalog in Teilen von dem notwendigen Ausschluss von „Folgemaßnahmen mit unmittelbarer Außenwirkung“ (in der Terminologie des bisherigen Gesetzes) gelöst.

§ 82 setzt auf dem bisherigen § 11b Absatz 1 auf. Der bisher in § 11b Absatz 1 enthaltene Rechtsgüterkatalog wurde in etwas modifizierter Form aus systematischen Gründen nunmehr in § 2 Absatz 1 übernommen. Eine inhaltliche Änderung mit Blick auf die durch den Bundesnachrichtendienst geschützten Rechtsgüter geht mit der Modifizierung nicht einher, vgl. dazu die Begründung zu § 2 Absatz 1. § 82 enthält nunmehr einen entsprechenden Verweis auf § 2 Absatz 1.

Aufgelöst wurde zudem die vormals enthaltene Bezugnahme auf die „nicht in den §§ 11 und 11a genannten“ öffentlichen Stellen. Diese Einschränkung führte zu Problemen bei der Zuordnung von Behörden, welche sowohl Strafverfolgungs- als auch Gefahrenabwehraufgaben wahrnehmen. Zudem stand sie z.B. einer Übermittlung von Hintergrundinformationen (also solchen, die keinen Bezug zu einem konkreten Strafverfahren haben) an den Generalbundesanwalt entgegen, vgl. hierzu § 83.

Die bisher in § 11b Absatz 3 und 4 enthaltenen Vorgaben entfallen, da § 80 nunmehr die Übermittlung von personenbezogen Daten an die Bundeswehr gesondert regelt.

Zu § 83 (Übermittlung an inländische öffentliche Stellen im Gefahrenvorfeld)

In § 83 geht der bisherige § 11b Absatz 2 auf. Wie oben dargestellt wird insoweit nunmehr zwischen den Übermittlungen „im Gefahrenvorfeld“, welche grundsätzlich auch dann möglich sind, wenn administrativ-ordnungsbehördliche Folgemaßnahmen die Folge sind (§ 83), und Übermittlungen unter Ausschluss von operativen Anschlussmaßnahmen (hierzu § 84) unterschieden.

Zu Absatz 1

Der Katalog in Absatz 1 entspricht dem bisherigen § 11b Absatz 2. Die bisherige Nummer 5 konnte entfallen. Die dort geregelte Fallgruppe geht, da hier operative Anschlussmaßnahmen nicht in Rede stehen, nunmehr in § 84 Absatz 1 auf. Auch Nummer 6 wurde aufgrund der Regelung in § 80 gestrichen.

Soweit nach Nummer 1 eine Übermittlung zur Bereitstellung von Hintergrundinformationen ermöglicht wird, so ist zwar regelmäßig nicht davon auszugehen, dass die so übermittelten Informationen für operative Folgemaßnahme verwendet werden. Ausgeschlossen ist dies indes nicht; möglich wäre es insoweit also, Hintergrundinformationen an die Bundespolizei zu Grenzüberschreitungen zu übermitteln und diese könnte sodann auf Grundlage dieser Informationen (auch) operativ tätig werden. Ergänzt werden – parallel zu den entsprechenden Änderungen im Bundesverfassungsschutzgesetz die Nummer 2 und 3. Zudem wurde Nummer 5 ergänzt.

Zu Absatz 2

Absatz 2 regelt – in Entsprechung des § 20 Absatz 2 des Bundesverfassungsschutzgesetzes - die Datenübermittlungen zur Prüfung der Voraussetzungen begünstigender Maßnahmen. Solche Maßnahmen können die rechtlich geschützten Interessen der betroffenen Person erheblich berühren, haben jedoch weder selbst Zwangscharakter noch können sie mit Zwangsmitteln durchgesetzt werden. Das strenge Erfordernis einer konkretisierten Gefahr als Mindestschwelle der Datenübermittlung gilt für sie daher nicht, während sich die verfassungsrechtlichen Anforderungen an den Rechtsgüterschutz auch auf diese Übermittlungen erstrecken (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 254 ff.).

Zu § 84 (Übermittlung an inländische öffentliche Stellen ohne Möglichkeit operativer Anschlussmaßnahmen)

Zu Absatz 1

In Absatz 1 geht der bisherige § 11b Absatz 2 Nummer 5 auf.

Zu Absatz 2

In Umsetzung der Rechtsprechung des Bundesverfassungsgerichts (vgl. BVerfG, Beschluss vom 17. Juli 2024, 1 BvR 2133/22, Rn. 221ff.) erfolgte eine Änderung des Absatzes 2 dahingehend, dass nunmehr nicht länger darauf abgestellt wird, dass die übermittelten personenbezogenen Daten nicht zur operativen Anwendung unmittelbaren Zwangs genutzt werden dürfen. Hierzu hat das Bundesverfassungsgericht nämlich ausgeführt, dass das „Merkmal der Unmittelbarkeit (…) keine zwingende Voraussetzung für die Geltung der strengeren Anforderungen an die Übermittlung“ ist (BVerfG, Beschluss vom 17. Juli 2024, 1 BvR 2133/22, Rn. 231). Vielmehr ist nun entscheidend, ob die Übermittlung für Aufgaben erforderlich ist, welche die empfangende Stelle ohne „operative Anschlussmaßnahmen“ zu Lasten der betroffenen Person wahrnimmt. Dass insoweit die konkrete, mit den übermittelten Daten verbundene Aufgabenwahrnehmung maßgeblich ist, entspricht ebenfalls der verfassungsgerichtlichen Rechtsprechung (BVerfG, Beschluss vom 17. Juli 2024, 1 BvR 2133/22, Rn. 111).

Zu Absatz 3

In Absatz 3 wird (klarstellend) geregelt, dass eine Nutzung von personenbezogenen Daten durch die empfangende Stelle nur dann für operative Anschlussmaßnahmen zulässig ist, wenn die Übermittlungsvoraussetzungen der §§ 81 und 82 vorliegen. Die Vorschrift entspricht insoweit § 22 Absatz 3 Satz 3 des Bundesverfassungsschutzgesetzes.

Zu Absatz 4

In Absatz 4 ist die Befugnis geregelt, personenbezogene Daten zum Zweck der Forschung und Entwicklung (auch) automatisiert an inländische öffentliche Stellen (z.B. Universitäten) zu übermitteln. Zur Unkenntlichmachung vergleiche die Ausführungen zu § 32 Absatz 3 Nummer 4.

Zu § 85 (Übermittlung an inländische nichtöffentliche Stellen)

Die Regelung ersetzt den bisherigen § 11c und modifiziert diesen. Um den Verwaltungsaufwand zu reduzieren, und die Übermittlungsverfahren effizient zu gestalten, wurde das im bisherige Absatz 2 geregelte Zustimmungsverfahren gestrichen. Ein solches kann untergesetzlich geregelt werden. Die Regelung im bisherigen § 11c Absatz 3 ist durch die neue Regelungssystematik des BND-Gesetzes entbehrlich.

Zu Absatz 1

Absatz 1 wurde sprachlich gegenüber der Regelung im bisherigen § 11c angepasst. In Nummer 1 wird auf die konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut (§ 2 Absatz 1) abgestellt. Zusätzlich enthält Satz 1 nunmehr eine Subsidiaritätsregelung. Eine Übermittlung an nicht öffentliche Stellen kommt beispielsweise nach Nummer 1 bei Cyberangriffen in Betracht, bei denen es erst auf Grundlage von Hinweisen durch den Bundesnachrichtendienst möglich, Bedrohungen zu identifizieren und entsprechende Schutzmaßnahmen einzuleiten.

In Nummer 2 wurde die Aufzählung der Ziele sowie Satz 2 angepasst. Die neu eingefügten Ziele wurden aufgrund der veränderten Bedrohungslage aufgenommen:

Der neu hinzugekommene Schutz in der Informationstechnik (Nummer 2 Buchstabe e) umfasst alle organisatorischen, technischen, personellen und infrastrukturellen Maßnahmen, die darauf abzielen, IT-Komponenten, Anwendungen, Daten, Systeme, Netzwerke und Prozesse ganzheitlich vor Cyberbedrohungen zu schützen. Ziel ist es, die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit sowie Authentizität und Nachvollziehbarkeit sicherzustellen. Der Schutz bezieht sich auf die Prävention, Erkennung, Reaktion und Wiederherstellung im Zusammenhang mit Bedrohungen, die im digitalen Raum entstehen – darunter Schadsoftware, unbefugter Zugriff, Datenlecks, Manipulation, Ausspähung, Sabotage, Denial-of-Service-Angriffe und andere Formen von Cyberangriffen. Dabei sind sowohl klassische IT-Systeme (wie Server, Clients, Netzwerkinfrastruktur, Speicherlösungen) als auch moderne digitale Komponenten (wie mobile Endgeräte, Cloud-Dienste, industrielle Steuerungssysteme, IoT-Geräte, Webanwendungen und KI-Systeme) einzubeziehen.

Der Schutz der Sicherheit in der Informationstechnik wird insbesondere auch durch den regelmäßigen Austausch mit nicht öffentlichen Stellen zu gegenwärtigen Bedrohungen im Cyberraum gewährleistet. Die Sicherheit im Cyberraum ist für die Sicherheit Deutschlands zentral, die nur durch das Zusammenwirken aller betroffener Stellen geschützt werden kann.

Auch der Schutz der Wirtschaft (Nummer 2 Buchstabe f) kann eine Übermittlung an eine nicht öffentliche Stelle erfordern. Wirtschaftsspionage bedroht die deutsche Wirtschaft und ihre Fähigkeiten zunehmend. Fremde Mächte zielen darauf ab sich Innovationen, die es nur in Deutschland gibt, anzueignen, um somit ihre eigene Position auf dem globalen Markt

zu verstärken und deutsche Unternehmen zu schädigen. Zudem werden Sabotageakte mit zunehmender außenpolitischer Spannung immer wahrscheinlicher.

Eine Übermittlung ist erforderlich, um beispielsweise die verdeckte Einflussnahme ausländischer Mächte auf die Wirtschaft, bspw. durch Firmenübernahmen, Technologietransfer oder Wissenstransfer zu verhindern. Es muss sich nicht um einen unmittelbar sicherheitlichen Kontext handeln, sondern vielmehr um eine Gefährdung der wirtschaftlichen Position Deutschlands und seiner Industriezweige. Die Sicherheitsarchitektur Deutschlands fußt noch immer auf dem Konzept der inneren und äußeren Sicherheit, Krieg und Frieden. Dieses bildet nicht die hybride Bedrohungslage ab, in der sich Deutschland, Europa und die westliche Welt befindet. Die Bedrohungen durch Sabotage, Spionage, Cyberangriffe, Desinformationen und illegalen Technologietransfer erfordern eine gesamtgesellschaftliche Kooperation zwischen Staat und Wirtschaft. Daher ist eine Übermittlung an nicht staatliche Stellen erforderlich, um einen bidirektionalen Informationsaustausch zu institutionalisieren.

Eine Übermittlung zum Schutz der Wirtschaft ist dabei auch im Bereich Forschung erforderlich. Das Bestreben einer ausländischen Macht, vollkommen unabhängig von anderen Staaten zu sein, erfordert den Zugang zu diversen Schlüsseltechnologien. Bei ausländischen Mächten, kann die zivile Forschung auch dem militärischen Bereich für mögliche Anwendungsfelder zur Verfügung gestellt werden, was sicherheitspolitische Implikationen für Deutschland und Europa nach sich ziehen kann. Für den Bundesnachrichtendienst muss es möglich sein, auch Informationen zu Forschenden (i.d.R. Gastwissenschaftlern) an Unternehmen weiterzugeben, wenn diese Gastwissenschaftler von der ausländischen Macht gesendet werden, die nach hiesigen Erkenntnissen eng mit militärischen Forschungseinrichtungen kooperieren.

Übermittlungen an die Wirtschaft können auch im Bereich der Energietechnik erforderlich sein. Potentielle Themenfelder sind bspw. KI-gestützte Optimierungen (deep learning) für Stromnetze. Eine Übermittlung kann auch erforderlich sein, um Wirtschaftsunternehmen vor dem Handeln anderer Staaten zu warnen, bspw. im Rahmen der Analyse kritischer Infrastruktur (Wasser-, Gas-, Internetnetze).

Weitere Anwendungsfälle können Übermittlungen für den Schutz im Bereich der Luft- und Raumfahrttechnik oder im Bereich der Überwachungstechnologie sein.

Die Nutzung des deutschen Finanzsystems (Nummer 2 Buchstabe g) zum Transfer von inkriminierten Geldern kann zu einem erheblichen Reputationsverlust der betroffenen Banken führen. Dies kann zu Risikoaufschlägen bei internationalen Transaktionen oder sogar zum Abbruch internationaler Geschäftsbeziehungen führen. Deshalb kann auch zum Schutz des Finanzsystems die Übermittlung von personenbezogenen Daten in besonders schweren Fällen notwendig sein. Eine Übermittlung ist beispielsweise erforderlich, wenn ein deutsches Kreditinstitut eingefrorene Gelder eines Drittstaates transferieren soll. Der Bundesnachrichtendienst kann in diesen Fällen bei der Überprüfung der Transaktion unterstützen. So sollte sichergestellt werden, dass die eingefrorenen Gelder nicht an Unternehmen im Besitz des Drittstaates überwiesen werden.

Deutsche Firmen und Banken werden zudem durch international agierende Akteure zur Geldwäsche genutzt. Zur Verhinderung und Bekämpfung der Geldwäsche ist es daher erforderlich, Daten zu übermitteln, bspw. um deutsche Unternehmen oder Banken auf kriminelle Netzwerke hinzuweisen, die ihre Infrastruktur nutzen oder nutzen wollen.

Durch die nachrichtendienstliche Auslandsaufklärung erlangt der Bundesnachrichtendienst auch Erkenntnisse zu internationalen Forschungsprojekten (Nummer 2 Buchstabe h). Um ein integriertes, vollständiges Lagebild der gewonnenen Erkenntnisse zu erhalten, sind Übermittlungen und Kollaborationen mit bspw. Forschungsinstituten von hoher Bedeutung. Zudem können durch etwaige Übermittlungen die Erforschung und Entwicklung nachrichtendienstlicher Fähigkeiten optimiert werden, indem z.B. eine externe Qualitätskontrolle

durchgeführt wird oder Dritte besser in den Ausbau technischer und nicht-technischer nachrichtendienstlicher Systeme involviert werden können.

Eine Übermittlung zur wissenschaftlichen Erforschung und Bewertung von Bedrohungen kann auch erforderlich sein, wenn zur wissenschaftlichen Bewertung einer solchen Bedrohung eine Expertise benötigt wird (bspw. Fachexperten an Universitäten), zur Bewertung dieser Bedrohung auch eine Einschätzung der Expertise, Zugänge und Fähigkeiten der handelnden Akteure erforderlich ist, ein personenspezifisches Proliferationsrisiko analysiert werden muss, die intentionale Verbreitung von Infektionskrankheiten verhindert werden soll oder es stichhaltige Hinweise auf mögliche relevante (auch geplante) Verstöße gegen Biosicherheitsvorgaben beim Umgang mit (pandemierelevanten) Erregern der biologischen Schutzstufen BSL3 und BSL4 gibt. Auch betroffen hiervon ist der Zugang oder die Zurate-Ziehung wissenschaftlicher Kapazitäten zur Aufklärung besonders schwerer Bedrohungen, wie der Entwicklung und Verbreitung von Massenvernichtungswaffen oder zur Entwicklung nachrichtendienstlicher Fähigkeiten zum Zwecke der Aufklärung besonders schwerer Bedrohungen. Eine Weitergabe von Daten an nicht öffentliche Stellen, die diese im Auftrag des Bundesnachrichtendienstes verarbeiten, stellen keine Übermittlung dar, da die Date weiterhin in der Sphäre des Bundesnachrichtendienst verbleiben und lediglich aus operativ-technischen Gründen (und ohne, dass die empfangende Stelle die Daten für andere Zwecke verwenden kann, wofür Sorge zu tragen ist) zur Verfügung gestellt werden. Dies betrifft etwa die Bereitstellung von Datenproben aus der Erfassung an Entwicklerfirmen kommerzieller Systeme, damit für den Bundesnachrichtendienst entwickelt werden kann.

Zu Absatz 2

Die Regelung entstammt dem bisherigen § 11c Absatz 4. Sie enthält Folgeanpassungen in der Formulierung, die der Angleichung an die anderen nachrichtendienstlichen Fachgesetzen des Bundes dienen.

Zu Absatz 3

In Absatz 3 wird die Möglichkeit geschaffen, personenbezogene Daten für wissenschaftliche Zwecke zu übermitteln. Die Regelung flankiert parallele Möglichkeiten, Daten zu diesen Zwecken an öffentliche Stellen und ausländische Stellen zu übermitteln. Es wird auf die Begründung zu § 84 Absatz 4 verwiesen.

Zu § 86 (Übermittlung an ausländische öffentliche Stellen oder an über- oder zwischenstaatliche Stellen)

Die Regelung entspricht im Wesentlichen dem bisherigen § 11e.

Zu Absatz 1

Absatz 1 ist unverändert geblieben, es wurden nur notwendige sprachliche Anpassungen vorgenommen.

Zu Absatz 2

Absatz 2 enthält eine Folgeanpassung, indem nunmehr auf die besonders gewichtigen Rechtsgüter in § 2 Absatz 1 Bezug genommen wird.

Die bisherige Regelung der Nummer 2 stellt darauf ab, dass die Übermittlung „der Sicherheit des Empfängerstaates“ dient. Insbesondere bei der Übermittlung an über- bzw. zwischenstaatliche Stellen (bspw. NATO) fehlt aber ein direkt betroffener Empfängerstaat, da die über- bzw. zwischenstaatliche Ebene der Empfänger ist. Die Anpassung ist eine Konkretisierung der Norm. Die Übermittlung muss der Sicherheit des Empfängerstaates oder eines Mitgliedstaates der über- oder zwischenstaatlichen Stelle dienen.

Zu Absatz 3

In Absatz 3 wurde zum einen die bisher im Gesetz enthaltene Begrifflichkeit der „Folgemaßnahmen mit unmittelbarer Außenwirkung“ zur allgemeinen Harmonisierung durch den in § 84 verwendeten Begriff der „operativen Anschlussmaßnahmen“ ersetzt (vgl. dort). Zudem wurde als Folgeänderung zu Absatz 2 die Nummer 2 ergänzt (hierzu oben).

Darüber hinaus wurde Nummer 3 neu aufgenommen. Ergänzt wird eine Übermittlungsmöglichkeit zu den besonders gewichtigen Rechtsgütern, die in § 2 Absatz 1 Nummer 1 Buchstaben b und c (Bestand oder Sicherheit von Einrichtungen internationaler Organisationen, sofern die Bundesrepublik Deutschland Mitglieder dieser Organisation ist, oder eines Mitgliedstaates der Europäischen Union, der EFTA oder der NATO) und Nummer 2 (Bündnis- und Verteidigungsfähigkeit der Bundesrepublik Deutschland) genannt werden. Eine Fallkonstellation der neuen Nummer 3 ist folgende: Es ist möglich, dass die NATO selbst Handlungen (Folgemaßnahmen auf Grund einer Übermittlung durch den Bundesnachrichtendienst) vornimmt. Der Bundesnachrichtendienst leistet Beiträge zum Frühwarnsystem der NATO ACO Indications and Warning (ACO I&W). Eine Indikatorenänderung kann zu unmittelbaren Folgemaßnahmen innerhalb der Allianz führen. Die Beiträge des Bundesnachrichtendienstes zu ACO I&W werden zwar nicht direkt, sondern mittelbar über das Operative Führungskommando der Bundeswehr (OpFüKdoBw) erbracht. OpFüKdoBw fungiert mit dem National Watch Center als Schnittstelle zur NATO und bringt den Beitrag des Bundesnachrichtendienstes als national zuständige Stelle entsprechend ein. Eine direkte Übermittlung an die NATO erfolgt aktuell über eine Regelberichterstattung sowie durch die Beantwortung von direkten Anfragen. Die zunehmende Dynamik in der Gesamtverteidigung erfordert jedoch, dass Daten, die der NATO derzeit über den Geschäftsbereich des Bundesministeriums der Verteidigung mittelbar zur Verfügung gestellt werden, direkt und ohne weitere zeitliche Verzögerung zugänglich gemacht werden. Dies gilt auch für den Fall, dass der Bundesnachrichtendienst Informationen hat, deren Übermittlung für den Schutz des Bestandes oder der Sicherheit eines Mitgliedstaates der Europäischen Union erforderlich ist. Auch in diesem Fall muss eine Übermittlung auch mit der Möglichkeit operativer Anschlussmaßnahmen möglich sein, auch unterhalb der Schwelle der konkretisierten Gefahr.

Zu Absatz 4

Die Regelung des Absatz 4 wurde neu aufgenommen. Hierdurch soll der Bundesnachrichtendienst befähigt werden, eine automatisierte Übermittlung zu Zwecken von Forschung und Entwicklung vorzunehmen. Dies ist erforderlich, um im internationalen Verbund mit Partnerdiensten gemeinsam technische Systeme oder Fähigkeiten zu entwickeln. Zur Unkenntlichmachung vergleiche die Ausführungen zu § 32 Absatz 3 Nummer 4.

Zu Absatz 5

Die Vorschrift greift den bisherigen § 11e Absatz 3 Satz 2 auf.

Zu § 87 (Übermittlung an ausländische nichtöffentliche Stellen)

Die Regelung fußt auf dem bisherigen § 11f. Als Folgeanpassung enthält die Regelung nunmehr auch den Bezug auf die besonders gewichtigen Rechtsgüter in § 2 Absatz 1. Eine einschränkende Aufzählung einzelner Rechtsgüter aus der Gruppe der besonders gewichtigen Rechtsgüter wird in der Neufassung nicht mehr vorgenommen. Die Übermittlung zur Minderung der Verwundbarkeit und Stärkung des Schutzes der Sicherheit von informationstechnischen Systemen vor internationalen kriminellen, terroristischen oder staatlichen Angriffen bzw. der Schutz der Informationstechnik ist nach wie vor ein wichtiger Bedarfsfall der Praxis. Diese konkrete Fallkonstellation ist weiterhin durch den Bezug auf die Rechtsgüter in § 2 Absatz 1 abgedeckt. Die gesonderte Regelung der mit dem Zweck der politischen Unterrichtung gekennzeichneten personenbezogenen Daten (bisheriger § 11f Absatz 3) findet sich nun in Absatz 1 Satz 2. Das Erfordernis der Subsidiarität wurde in Absatz 1 nunmehr zusätzlich aufgenommen.

Absatz 2 enthält nach wie vor eine zusätzliche Verfahrensvorgabe bei der Übermittlung von personenbezogenen Daten ins Ausland.

Die Regelung in Absatz 3 entstammt dem bisherigen § 11f Absatz 4. Die Formulierung wurde angepasst, um einen sprachlichen Gleichlauf mit dem MAD-Gesetz und dem BVerfSchG zu erreichen.

Zu § 88 (Übermittlung von sonstigen personenbezogenen Daten)

Zu Absatz 1

Hier wird die Übermittlung von personenbezogenen Daten geregelt, die nicht mit nachrichtendienstlichen Mitteln oder durch spezielle Auskunftsersuchen erhoben wurden. Hierunter fallen beispielsweise Daten aus allgemein zugänglichen Quellen, Daten, die dem Bundesnachrichtendienst von ausländischen Partnern übermittelt wurden oder Daten, die der Bundesnachrichtendienst ohne Eingriffe in Grundrechte (z.B. freiwillige Weitergabe an den Bundesnachrichtendienst im Rahmen einer Befragungen) erhalten hat. Es handelt sich bei diesen Daten damit um solche, die durch jedermann erhoben werden können. Insofern sind strengere Anforderungen an die Übermittlung von Daten z.B. aus allgemein zugänglichen Quellen nicht sachgerecht, da die empfangende Stelle die öffentlich verfügbaren Informationssammlungen auch genauso selbst erheben könnte, wenn sie diese zur Erfüllung ihrer Aufgaben benötigt. Auch Daten, die der Bundesnachrichtendienst von ausländischen Partnern erhalten hat, fallen hierunter, wenn diese zur Weitergabe durch die Partner freigegeben wurden (sog. Third Party Rule). Der Bundesnachrichtendienst hat hierbei keinen Einblick, ob diese vielleicht aus offenen Quellen stammen oder dem übermittelnden Dienst ggf. selbst durch einen anderen Dienst übermittelt wurden. Zumindest sind diese nicht durch Eingriffe in Grundrechte durch den Bundesnachrichtendienst erlangt worden.

Zu Absatz 2

Absatz 2 erlaubt als Art und Weise der Durchführung auch die automatisierte Übermittlung der in Absatz 1 genannten personenbezogenen Daten. Wie allgemein meint dabei die „automatisierte“ Übermittlung solche Fälle, in denen eine vorherige Sichtung der Daten nicht erfolgt. Unter diese Norm fällt auch die Übermittlung von angekauften Datensammlungen z.B. von umfänglichen Werbedaten (sog. ADINT-Daten), oder von im Internet verfügbaren Datenleaks. Solche Daten dürfen, auch in ihrer Gesamtheit, auch automatisiert übermittelt werden.

Nicht unter die Regelung dieser Norm fällt die Übermittlung von personenbezogenen Daten im Rahmen von Kooperationen. Hierfür sieht Abschnitt 3 Unterabschnitt 3 ein spezielles Regelungsregime (die „Kooperationsvorschriften“) vor.

Zu Unterabschnitt 4 (Gemeinsame Dateien)

Zu § 89 (Projektbezogene gemeinsame Dateien mit inländischen öffentlichen Stellen)

Die Regelung ersetzt § 12 des bisherigen Rechts und konkretisiert die Anforderungen an gemeinsame Dateien mit inländischen öffentlichen Stellen. Dabei werden die besonderen Vorgaben, die bei gemeinsame Dateien nach § 89 und § 92 zu beachten sind, wenn diese durch den Bundesnachrichtendienst geführt werden, nunmehr in einer gesonderten Regelung normiert, § 90. Durch die Entkopplung wurde der Regelungsgehalt des § 6 Absatz 2 Satz 6 Bundesverfassungsschutzgesetz in § 89 Absatz 2 integriert.

Zu Absatz 1

In § 89 Absatz 1 wurde der Kreis der möglichen Teilnehmer an einer gemeinsamen Datei erweitert auf inländische öffentliche Stellen. Auf diese Weise sollen unter anderem die an

der Zusammenarbeit im Rahmen des Nationalen Cyber-Abwehrzentrums und des Gemeinsamen Terrorismusabwehrzentrums beteiligten Behörden ergänzt werden. Dies ermöglicht es den beteiligten Behörden, eine gemeinsame Datei unter der Federführung des Bundesnachrichtendienstes zu errichten und sich hieran zu beteiligen.

Das Erfordernis eines Projektbezugs stellt sicher, dass die jeweils beteiligten Stellen den Dateizweck, d.h. eine konkrete projektbezogene Zusammenarbeit, den Projektauftrag und das Projektziel, festlegen. Der Projektbezug ist weit zu verstehen und dadurch begrenzt, dass er im Rahmen der Aufgaben der an der projektbezogenen Zusammenarbeit beteiligten Stellen liegen muss. Die gemeinsame Datei muss dem Bundesnachrichtendienst zur nachrichtendienstlichen Auslandsaufklärung dienen. Da der Dateizweck in den Fällen von gemeinsamen Dateien nach § 89 – anders als im Fall der Antiterrordatei und der Rechtsextremismus-Datei - nicht gesetzlich festgeschrieben ist, ist eine konkrete Vereinbarung der beteiligten Stellen von Projektauftrag, Projektziel und der Verfahrensweisen erforderlich. Diese Vereinbarung kann, sofern die gemeinsame Datei durch den Bundesnachrichtendienst geführt wird, im Rahmen der Errichtungsanordnung erfolgen (§ 90 Absatz 2). Die Anforderungen an die Befristung gemeinsamer Dateien, welche vom Bundesnachrichtendienst geführt werden, sind in § 90 Absatz 1 geregelt.

Zu Absatz 2

§ 89 Absatz 2 hat inhaltlich den Regelungsgehalt von § 12 Absatz 2 des bisherigen Rechts. Abweichend von § 12 Absatz 2 ist nunmehr in Satz 3 Nummer 1 jedoch klargestellt, dass es im Rahmen von gemeinsamen Dateien künftig auch zulässig ist, ein „Rechte“-Management einzurichten, sodass eine Teilnahme auch von solchen Behörden möglich wird, denen einzelne Daten nicht übermittelt werden dürfen, solange die gemeinsame Datei entsprechende Vorkehrungen trifft, dass diese Behörden keinen Zugriff auf die jeweiligen Daten erhalten.

Darüber hinaus wurde lediglich die Kennzeichnungspflicht dahingehend präzisiert, dass sie sich auf die jeweils eingebende Stelle bezieht. Die Eingabe von Daten in eine gemeinsame Datei durch den Bundesnachrichtendienst darf auch automatisiert erfolgen. Voraussetzung hierfür ist, dass eine automatisierte Übermittlung an die beteiligten Stellen ausdrücklich gesetzlich vorgesehen ist und die tatbestandlichen Voraussetzungen hierfür erfüllt sind.

Zu Absatz 3

Absatz 3 entspricht dem Regelungsgehalt des bisherigen § 12 Absatz 1 Satz 3 und wurde redaktionell angepasst. Nicht übernommen wurde die Klarstellung, dass bei der weiteren Verwendung der personenbezogenen Daten die für die jeweiligen beteiligten Stellen geltenden Vorschriften Anwendung finden. Dies bedarf keiner erneuten gesetzlichen Regelung, da sich die Geltung bereits aus den jeweiligen Gesetzen ergibt.

Zu Absatz 4

Die Regelung in Satz 1 entspricht § 12 Absatz 5 des bisherigen Rechts. Satz 2 trägt der Tatsache Rechnung, dass gemeinsame Dateien nun unbegrenzt verlängert werden können, solange das Ziel der projektbezogenen Zusammenarbeit noch nicht erreicht worden ist. Um eine zeitlich unbegrenzte gemeinsame Datenhaltung zu verhindern, weiter wird klargestellt, dass sich die Höchstgrenze der Speicherungsdauer nach den Löschfristen des jeweils für die eingestellten Daten geltenden Fachrecht richtet.

Zu Absatz 5

Die Regelung entspricht § 6 Absatz 2 Satz 4 BVerfSchG, welcher nach § 12 Absatz 3 Satz 1 des bisherigen Rechts auf durch den Bundesnachrichtendienst geführte gemeinsame Dateien Anwendung fand.

Zu § 90 (Führung projektbezogener gemeinsamer Dateien mit inländischen öffentlichen Stellen durch den Bundesnachrichtendienst)

Die Vorschrift regelt die besonderen Anforderungen, die an gemeinsame Dateien nach § 89 und § 92 zu stellen sind, wenn diese durch den Bundesnachrichtendienst geführt werden.

Zu Absatz 1

Wie schon in § 12 des bisherigen Rechts sind projektbezogene gemeinsame Dateien anfänglich auf zwei Jahre zu befristen. Die sich daran anschließende Befristung von projektbezogenen gemeinsamen Dateien wurde angepasst und richten sich nunmehr daran, ob das vereinbarte Projektziel erreicht worden ist. Die Erreichung des Projektziels unterliegt einer turnusmäßigen Überprüfung und kann um jeweils zwei weitere Jahre verlängert werden. Der dadurch möglichen erhöhten Eingriffstiefe durch eine längerfristige Nutzung von Daten in projektbezogenen gemeinsamen Dateien wird dadurch Rechnung getragen, dass nunmehr die Höchstgrenze der Speicherungsdauer von personenbezogenen Daten den Löschungsfristen der jeweiligen in die Datei eingestellten Daten gemäß dem für diese geltenden Fachrecht folgt. Das Anknüpfen der Löschungsverpflichtung an die für die jeweilige beteiligte Behörde geltenden Rechtsvorschriften hält das Bundesverfassungsgericht für Verbunddateien für naheliegend und verfassungsrechtlich vertretbar (BVerfG Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 223).

Eine Ausnahme von dem Grundsatz der Befristung ist für solche gemeinsamen Dateien vorgesehen, die durch den Bundesnachrichtendienst geführt werden und an denen ausschließlich die Bundeswehr beteiligt ist. Für diese gemeinsamen Dateien gilt § 92 als speziellere Regelung.

Zu Absatz 2

Satz 1 entspricht im Wesentlichen § 12 Absatz 6 Satz 1 des bisherigen Rechts. Aus redaktionellen Gründen ist § 12 Absatz 6 Satz 1 Nummer 2 nicht übernommen worden. Die hierin geregelte Angabe der Art der zu speichernden personenbezogenen Daten ist bereits nach § 61 Absatz 2 erforderlich.

Die an der gemeinsamen Datei beteiligten Stellen haben im Rahmen einer Vereinbarung nicht nur den Dateizweck, den Projektauftrag und das Projektziel festzulegen. Vielmehr sind auch die Verfahrensweisen und Nutzungsbedingungen der gemeinsamen Datei zwischen den beteiligten Stellen zu vereinbaren. Hierzu gehören die Angaben aus der Errichtungsanordnung nach § 61 Absatz 2 ebenso wie folgende Festlegungen: Voraussetzungen, unter denen in der Datei gespeicherte personenbezogene Daten an welche Empfänger und in welchem Verfahren übermittelt werden; die jeweiligen Organisationseinheiten, die zur Eingabe und zum Abruf befugt sind sowie die Verpflichtung der beteiligten Stellen, die jeweils eingebende Stelle umgehend über Anhaltspunkte für die Unrichtigkeit eingegebener Daten zu unterrichten, und die Verpflichtung der eingebenden Stelle, die betreffenden Daten umgehend zu prüfen und erforderlichenfalls unverzüglich zu ändern, zu berichtigen oder zu löschen.

Zu Nummer 1

Die Regelung entspricht § 12 Absatz 6 Nummer 1 des bisherigen Rechts.

Zu Nummer 2

Zur Beschleunigung des Errichtungsanordnungsverfahrens für gemeinsame Dateien mit inländischen öffentlichen Stellen bedarf die Errichtungsanordnung nunmehr nach § 90 Absatz 3 nur noch der Zustimmung des Bundeskanzleramtes und nicht mehr aller Fachaufsichten der beteiligten Stellen. Da die Natur einer gemeinsamen Datei aber

wesentlich dadurch beeinflusst wird, wie viele und welche inländischen öffentlichen Stellen an ihr beteiligt sind, sind diese in der Errichtungsanordnung aufzuführen.

Zu Nummer 3

Die Regelung entspricht § 12 Absatz 6 Nummer 3 des bisherigen Rechts.

Zu Nummer 4

Die Regelung entspricht § 12 Absatz 6 Nummer 4 des bisherigen Rechts.

Zu Nummer 5

Die Regelung entspricht § 12 Absatz 6 Nummer 5 des bisherigen Rechts.

Zu Nummer 6

Die Regelung entspricht § 12 Absatz 6 Nummer 6 des bisherigen Rechts.

Zu Nummer 7

Die Regelung entspricht § 12 Absatz 6 Nummer 7 des bisherigen Rechts.

Zu Nummer 8

Die Protokollierungspflichten des Bundesnachrichtendienstes, die in § 12 Absatz 6 Nummer 8 des bisherigen Rechts geregelt waren, sind lediglich redaktionell angepasst worden, um klarzustellen, dass sie den Abruf jeder beteiligten Stelle aus der gemeinsamen Datei umfassen sollen.

Zu Nummer 9

Die Regelung entspricht § 12 Absatz 6 Nummer 9 des bisherigen Rechts.

Zu Absatz 3

Nach Satz 1 bedarf die Errichtungsanordnung für gemeinsame Dateien mit inländischen öffentlichen Stellen nicht mehr – wie nach § 12 Absatz 6 Satz 2 des bisherigen Rechts - der Zustimmung aller für die Fachaufsicht zuständigen obersten Bundes- oder Landesbehörden. Vielmehr bedarf die Errichtungsanordnung der Zustimmung des Bundeskanzleramtes. Eine Anbindung weiterer beteiligter Stellen an die gemeinsame Datei ist hingegen erst mit der Zustimmung des Bundeskanzleramtes zu der Errichtungsanordnung sowie der Zustimmung der für die Fachaufsicht der jeweils anzubindenden beteiligten Stelle zuständigen Bundes- oder Landesbehörde zu der Beteiligung der jeweils anzubindenden beteiligten Stelle. Verlängerungen nach § 90 Absatz 1 Satz 2 sind ohne erneute Durchführung eines Errichtungsanordnungsverfahrens zulässig.

Zu Absatz 4

Absatz 4 soll es dem Bundesnachrichtendienst ermöglichen, mit der Errichtung und Ertüchtigung der gemeinsamen Datei zu beginnen, bevor das Errichtungsanordnungsverfahren abgeschlossen ist.

Zu Absatz 5

Die Verpflichtung zur Auskunft an Betroffene bei durch den Bundesnachrichtendienst geführten gemeinsamen Dateien entspricht der Verpflichtung aus § 12 Absatz 3 i.V.m. § 6 Absatz 2 Satz 5 BVerfSchG des bisherigen Rechts.

Zu § 91 (Erweiterte Nutzung projektbezogener gemeinsamer Dateien mit inländischen öffentlichen Stellen)

Die Norm trägt dem fachlichen Bedarf Rechnung, gemeinsame Dateien mit inländischen öffentlichen Stellen strukturiert zu durchsuchen und auf Zusammenhänge zu analysieren. Da diese Form der Analyse vormals getrennter Daten es ermöglicht, mit informationstechnischen Methoden neue Erkenntnisse zu gewinnen, ist das Eingriffsgewicht dieser Form der Nutzung einer gemeinsamen Datei erhöht (BVerfG vom 10. November 2020 – 1 BvR 3214/15 - Rn. 73).

Zu Absatz 1

Das Bundesverfassungsgericht hat aufgrund des erhöhten Eingriffsgewichts an die erweiterte Nutzung von gemeinsamen Dateien durch Gefahrenabwehr- und Strafverfolgungsbehörden gesteigerte verfassungsrechtliche Anforderungen gestellt. Demgegenüber hat es an die erweiterte Nutzung von gemeinsamen Dateien geringere Anforderungen gestellt, wenn diese durch Nachrichtendienste erweitert genutzt werden (BVerfG Beschluss vom 10. November 2020, 1 BvR 3214/15, Rn. 119). So sei diese bereits zulässig, wenn sie zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten ist (BVerfG Beschluss vom 10. November 2020, 1 BvR 3214/15, Rn. 119). Hintergrund ist, dass Nachrichtendienste von vornherein die Aufgabe haben, besonders gewichtige Rechtsgüter zu schützen (BVerfG Beschluss vom 10. November 2020, 1 BvR 3214/15, Rn. 119). Zudem sei bei der erweiterten Nutzung von personenbezogenen Daten durch Nachrichtendienste maßgeblich, dass bei ihrer Ersterhebung durch Polizeibehörden bereits die Eingriffsschwelle für die operativen Tätigkeiten der Polizei überschritten werden mussten und diese nicht auch für die weitere Nutzung der erhobenen Daten gelten (BVerfG Beschluss vom 10. November 2020, 1 BvR 3214/15, Rn. 119). Insoweit knüpft die erweiterte Nutzung durch den Bundesnachrichtendienst an die erheblichen Bedrohungen aus § 3 Absatz 1 an und fordert, dass eine solche im Einzelfall gegeben ist.

Zu Absatz 2

Absatz 2 definiert die erweiterte Nutzung gemeinsamer Dateien und regelt die hierbei anwendbaren Methoden. Das erhöhte Eingriffsgewicht der erweiterten Nutzung gemeinsamer Dateien liegt vor allem darin, dass hierdurch vorher nicht bekannte Zusammenhänge zwischen verschiedenen in der gemeinsamen Datei gespeicherten Personen und deren Daten hergestellt werden können („Data-mining“). So können im Wege der erweiterten Nutzung gemeinsamer Dateien Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen und eingehende Informationen zu bekannten Sachverhalten zugeordnet werden. Ferner erlaubt die erweiterte Nutzung gemeinsamer Dateien eine statistische Auswertung der in der gemeinsamen Datei gespeicherten Daten (BVerfG Beschluss vom 10. November 2020, 1 BvR 3214/15, Rn. 92).

Zu § 92 (Gemeinsame Dateien mit der Bundeswehr)

Der Bundesnachrichtendienst ist neben seiner Aufgabe als ziviler Nachrichtendienst auch mit der militärischen Auslandsaufklärung betraut und ist insofern technisch und personell eng mit der Bundeswehr verzahnt. Notwendige Voraussetzung für die militärische Lagebearbeitung ist ein möglichst unmittelbarer Austausch der bei den einzelnen Stellen des Systems Militärisches Nachrichtenwesen vorhandenen Lageinformationen und das möglichst zeitnahe Zusammenführen zu einem integrierten Lagebild. Dies soll in einer gemeinsamen Datei, in der die beteiligten Stellen Lese- und Schreibrechte haben und so Informationen unmittelbar einpflegen und am integrierten Lagebild partizipieren können. Ein Beispiel hierfür ist eine IT-basierte Lagekarte, in der mittels Layer die für die jeweilige Stelle relevanten Informationen ausgewählt und dargestellt werden können. So können die beteiligten Stellen

zum Beispiel Positionen von Kriegsschiffen oder Küstenverteidigungssystemen, die aktuelle Belegung von Militärflughäfen, die Position von Radaren oder weitreichenden Luftverteidigungssystemen und militärischen Führungseinrichtungen im Rahmen von integrierten Lagebildern erkennen oder eingeben.

Die Vorschrift ermöglicht es dem Bundesnachrichtendienst entsprechende gemeinsame Dateien zu errichten, zu führen oder sich hieran zu beteiligen. Auf die gemeinsamen Dateien mit der Bundeswehr finden die Vorschriften über gemeinsame Dateien mit inländischen öffentlichen Stellen Anwendung, soweit § 92 keine abweichenden Regelungen trifft.

Zu Absatz 1

Für gemeinsame Dateien des Bundesnachrichtendienstes mit der Bundeswehr bedarf es weder einer zeitlichen Befristung noch eines konkreten Projektbezugs. Die Entbehrlichkeit einer Befristung ist einerseits der Tatsache geschuldet, dass der Bundesnachrichtendienst auch mit der militärischen Auslandsaufklärung betraut ist. Andererseits folgt dies daraus, dass eine Befristung von gemeinsamen Dateien mit der Bundeswehr eine bloße Förmlichkeit darstellen würde, da eine (wiederholte) Verlängerung aufgrund der langfristigen Informationsbedürfnisse der Bundeswehr faktisch nahezu ausnahmslos erfolgen müsste. Ziel einer gemeinsamen Datei ist es auch gerade, dass die Bundeswehr im Spannungs- und Verteidigungsfall die Daten verfügbar hat und die Daten dazu beitragen, dass die Bundeswehr auf diesen Fall bestmöglich vorbereitet ist. In Absatz 1 werden die auch in § 80 Absatz 1 genannten Voraussetzungen für die Übermittlung von Daten an die Bundeswehr als Voraussetzung für die Einrichtung einer gemeinsamen Datei genannt.

Zu Absatz 2

Lediglich klarstellend regelt Absatz 2 Satz 1, dass die Übermittlungsvorschriften für die Eingabe in die gemeinsame Datei gelten. Eine Eingabe durch den Bundesnachrichtendienst darf auch automatisiert erfolgen, soweit dies nach den Vorschriften über die Übermittlung an die Bundeswehr zulässig ist.

Zu Absatz 3

Die Vorschrift trägt der Tatsache Rechnung, dass Absatz 1 es dem Bundesnachrichtendienst ermöglicht, unbefristete gemeinsame Dateien mit der Bundeswehr zu errichten, zu führen oder sich daran zu beteiligen. Um eine zeitlich unbegrenzte gemeinsame Datenhaltung zu verhindern, stellt Satz 3 klar, dass sich die Höchstgrenze der Speicherungsdauer nach den Löschfristen des jeweils für die eingestellten Daten geltenden Fachrecht richtet.

Zu § 93 (Gemeinsame Dateien mit ausländischen öffentlichen Stellen)

Die Regelung erlaubt es dem Bundesnachrichtendienst – angelehnt an § 13 des bisherigen Rechts - gemeinsame Dateien mit ausländischen öffentlichen Stellen zu errichten, zu führen oder sich an ihnen zu beteiligen. Die Zusammenarbeit mit ausländischen öffentlichen Stellen bedarf nun abweichend von § 13 Absatz 3 des bisherigen Rechts nicht mehr der Zustimmung des Bundeskanzleramtes. Vielmehr ist die Zustimmung des Bundeskanzleramts gemäß § 93 Absatz 3 begrenzt auf die Absichtserklärung. Dem Bundeskanzleramt steht es frei, gleichwohl im Rahmen der Fachaufsicht vom Bundesnachrichtendienst eine vorherige Vorlage zu fordern. Diese wiederum ist Voraussetzung für den Beginn der Zusammenarbeit. Die Unterrichtungspflicht an das Parlamentarische Kontrollgremium, die bisher in § 13 Absatz 3 Satz 2 geregelt war, wurde gestrichen. § 96 bündelt die Unterrichtungspflichten an das Parlamentarische Kontrollgremium.

Zu Absatz 1

Absatz 1 führt die Anforderungen des vormaligen § 13 Absatz 1 und Absatz 2 zusammen und ändert diese in Teilen. So ist eine Beschränkung auf bestimmte Gefahrenlagen oder

bestimmte Personenkreise nicht mehr erforderlich. Die gemeinsame Datei ist vielmehr daran zu messen, ob sie für die Aufklärung erheblicher Bedrohungen erforderlich ist und ob in den teilnehmenden Staaten die Einhaltung grundlegende rechtsstaatliche Prinzipien gewährleistet sind. Nicht übernommen wurde das Erfordernis, dass das Prinzip der Gegenseitigkeit gewahrt werden muss. Ein solches Erfordernis ist verfassungsrechtlich nicht vorgegeben und bedarf als Zweckmäßigkeitserwägung keiner gesetzlichen Regelung.

Zu Absatz 2

Vor Beginn der Zusammenarbeit mit ausländischen öffentlichen Stellen ist - wie nach § 13 Absatz 4 des bisherigen Rechts - der Abschluss einer Absichtserklärung erforderlich. Ergänzt wurde lediglich in Nummer 3 das Erfordernis, dass Vereinbarungen für den Fall der Unrichtigkeit von Daten getroffen werden. Dieses Erfordernis war bisher in der Errichtungsanordnung zu verorten. Da es sich aber um eine gegenseitige Verpflichtung der beteiligten Stellen handelt, sollte diese Teil der Absichtserklärung sein. Demnach ist wie nach dem bisherigen § 15 Nummer 10 weiterhin in der Errichtungsanordnung die Verpflichtung festzuhalten, dass die eingebenden ausländischen öffentlichen Stellen umgehend über Anhaltspunkte für die Unrichtigkeit eingegebener Daten zu unterrichten sind. Die sich daran anschließende Verpflichtung zur Sperrung, Berichtigung oder Löschung ist nun in der Absichtserklärung zu regeln.

Zu Absatz 3

Gemeinsame Dateien mit ausländischen öffentlichen Stellen bedürfen einer vorherigen Einbindung der Fachaufsicht des Bundesnachrichtendienstes. Aus diesem Grund sind die Absichtserklärung zwischen dem Bundesnachrichtendienst und den beteiligten ausländischen öffentlichen Stellen dem Bundeskanzleramt vor Zeichnung zur Zustimmung vorzulegen.

Zu Absatz 4

Absatz 4 führt die Anforderungen an die Eingabe personenbezogener Daten in die gemeinsame Datei durch den Bundesnachrichtendienst, die vormals in § 13 Absatz 1 und 2 geregelt waren, zusammen und ändert diese lediglich redaktionell. Klarstellend wird ergänzt, dass die Kennzeichnung der eingegebenen Daten erkennen lassen soll, dass der Bundesnachrichtendienst diese in die gemeinsame Datei eingegeben hat.

Zu Absatz 5

Die Vorschrift ist als Befugnisnorm konzipiert und schafft eine Rechtsgrundlage für den Bundesnachrichtendienst und die anderen, an einer (vom Bundesnachrichtendienst geführten) Datei beteiligten ausländischen Stellen, die Daten abzurufen und zu nutzen. Hiermit ist keine Verpflichtung für den Bundesnachrichtendienst verbunden, bei einer von ihm geführten Datei den zweckkonformen Umgang durch die andere Stelle zu überprüfen. Vielmehr obliegt es dieser Stelle, dafür Sorge zu tragen, dass der Zugriff, die Weiterverarbeitung und die Übermittlung zur Zweckerfüllung erforderlich ist.

Die Regelung entspricht § 16 Absatz 3 des bisherigen Rechts. Sie gilt aufgrund ihrer neuen Verortung nun für alle gemeinsamen Dateien mit ausländischen öffentlichen Stellen und nicht – wie bisher – nur für durch den Bundesnachrichtendienst geführte gemeinsamen Dateien; letzteres ist dabei freilich nur die Befugnisnorm für den Bundesnachrichtendienst und nicht für die ausländischen Stellen.

Zu § 94 (Führung gemeinsamer Dateien mit ausländischen öffentlichen Stellen durch den Bundesnachrichtendienst)

Die Regelung ermöglicht es dem Bundesnachrichtendienst wie § 14 des bisherigen Rechts, gemeinsame Dateien mit ausländischen öffentlichen Stellen zu führen und integriert die Voraussetzungen an eine Errichtungsanordnung des § 15 des bisherigen Rechts. Nicht

übernommen wurde die Regelung in § 14 Absatz 2 des bisherigen Rechts, wonach sich die Berichtigung, Verarbeitungseinschränkung und Löschung von personenbezogenen Daten durch die teilnehmenden ausländischen öffentlichen Stellen nach den für diese jeweils anwendbaren nationalen Regelungen richtet. Da sich die entsprechenden Verpflichtungen unmittelbar aus dem jeweiligen nationalen Recht ergeben, bedarf es keiner gesetzlichen Regelung.

Zu Absatz 1

Absatz 1 normiert die Verpflichtung, für durch den Bundesnachrichtendienst geführte gemeinsame Dateien mit ausländischen öffentlichen Stellen eine Errichtungsanordnung zu treffen. Im Wesentlichen wurden die Anforderungen des § 15 in die neue Regelung übernommen. Diejenigen Voraussetzungen des bisherigen § 15, die aufgrund des Verweises in den neuen § 61 Absatz 2 bereits Bestandteil einer Errichtungsanordnung sein müssen, werden zur Vermeidung von Doppelungen in § 94 Absatz 1 nicht im Einzelnen erneut aufgeführt.

Zu Nummer 1

§ 94 Absatz 1 Nummer 1 entspricht § 15 Nummer 8 des bisherigen Rechts.

Zu Nummer 2

Nummer 2 setzt den bisherigen § 15 Nummer 3 unter Berücksichtigung des oben erläuterten Rechte-Managements um.

Zu Nummer 3

Ebenso wie im Fall der gemeinsamen Dateien mit inländischen öffentlichen Stellen sind die an einer gemeinsamen Datei mit ausländischen öffentlichen Stellen beteiligten Stellen in der Errichtungsanordnung anzugeben.

Zu Nummer 4

Die der Zusammenarbeit zugrunde liegende Absichtserklärung ist wesentliche Voraussetzung für die Rechtmäßigkeit gemeinsamer Dateien mit ausländischen öffentlichen Stellen. Vor diesem Hintergrund muss die Absichtserklärung integraler Bestandteil der Errichtungsanordnung sein, die der Zustimmung des Bundeskanzleramtes unterliegt.

Zu Nummer 5

Die vormals in § 15 Nummer 4 geregelte Anlieferung und Eingabe ist schon aufgrund des Verweises auf § 53 Absatz 3 Teil von Errichtungsanordnungen für gemeinsame Dateien mit ausländischen öffentlichen Stellen. Die vormals ebenfalls in § 15 Nummer 4 vorgesehene Möglichkeit der ergänzenden Eingabe von Daten zu einer Person wird in § 94 Absatz 1 Nummer 5 überführt.

Zu Nummer 6

Die in § 15 Nummer 10 des bisherigen Rechts normierte umgehende Unterrichtung der eingebenden ausländischen öffentlichen Stellen über Anhaltspunkte für die Unrichtigkeit eingegebener Daten wurde in § 94 Absatz 1 Nummer 5 aufgenommen. Die sich nach § 15 Nummer 10 des bisherigen Rechts an eine entsprechende Unterrichtung anschließende Verpflichtung der ausländischen öffentlichen Stelle, die die Daten eingegeben hat, diese unverzüglich zu sperren, zu berichtigen oder zu löschen, ist nunmehr gemäß § 93 Absatz 2 Nummer 3 in die Absichtserklärung aufzunehmen.

Zu Nummer 7

§ 94 Absatz 1 Nummer 7 entspricht § 15 Nummer 9 des bisherigen Rechts.

Zu Nummer 8

Die in § 94 Absatz 1 Nummer 8 geregelte Protokollierung ist durch den die Datei führenden Bundesnachrichtendienst vorzunehmen. Protokolliert werden der Zeitpunkt des Abrufs sowie die für den Abruf jeweils verantwortliche Stelle.

Zu Nummer 9

Die Regelung entspricht § 15 Nummer 11 des bisherigen Rechts.

Zu Absatz 2

Die Errichtungsanordnung bedarf der Zustimmung des Bundeskanzleramtes. Die Errichtungsanordnung muss allerdings gemäß § 94 Absatz 1 Nummer 4 die Absichtserklärung umfassen. Der Abschluss einer Absichtserklärung erfordert oftmals einen hohen zeitlichen Aufwand. Aus diesem Grund darf der Bundesnachrichtendienst bereits mit der Errichtung und dem Betrieb der gemeinsamen Datei beginnen, bevor das Errichtungsanordnungsverfahren abgeschlossen ist. Eine Anbindung anderer beteiligter Stellen ist jedoch erst nach Zustimmung des Bundeskanzleramts zu der Errichtungsanordnung zulässig.

Zu Absatz 3

In Absatz 3 ist die Befugnis enthalten, dass sich an gemeinsamen Dateien des Bundesnachrichtendienstes, die dieser mit ausländischen öffentlichen Stellen führt, auch der Militärische Abschirmdienst und das Bundesamt für den Verfassungsschutz beteiligen dürfen.

Zu Absatz 4

Die Vorschrift entspricht der vergleichbaren Regelung in § 91 Absatz 4 Nummer 1.

Zu Absatz 5

Der Bundesnachrichtendienst als dateiführende Stelle hat die Eingabe in und den Zugriff auf die gemeinsame Datei zu protokollieren.

Zu Abschnitt 7 (Ergänzende Bestimmungen und Kontrollzuständigkeiten)

Zu Unterabschnitt 1 (Dienstvorschriften, Unterrichtungspflichten und Kontrollzuständigkeiten)

Zu § 95 (Dienstvorschriften)

Die Regelung war bisher im Abschnitt 4 bei den Regeln zur Technischen Aufklärung sowie im Abschnitt 1 unter Verweis auf das Bundesverfassungsschutzgesetz verortet. Nunmehr werden die Regelungen hier zusammengeführt und um Absatz 3 ergänzt.

Zu Absatz 1

In der Dienstvorschrift über den Einsatz von nachrichtendienstlichen Mitteln sind die einzusetzenden Mittel abschließend zu benennen. Dabei gilt, dass die nachrichtendienstlichen Mittel auch mit einem gewissen Abstraktionsgrad dargestellt und gruppiert werden können, um die Flexibilität und Effektivität der nachrichtendienstlichen Auslandsaufklärung zu gewährleisten. Entscheidend ist insoweit, dass die jeweiligen konkreten Durchführungsarten der abstrahierten nachrichtendienstlichen Mittel sich in ihrer Typizität und Eingriffsintensität

weitgehend entsprechen. Besteht eine erhebliche Abweichung gegenüber den in der Dienstvorschrift abschließend aufgeführten nachrichtendienstlichen Mitteln, so hat eine gesonderte Aufführung im Rahmen des Katalogs zu erfolgen.

Sollen nach Inkrafttreten dieser Regelung weitere (neue) nachrichtendienstliche Mittel eingesetzt werden, die nicht in der Dienstvorschrift benannt sind, sind Absatz 1 sowie § 19 Absatz 1 zu beachten. Sofern der Katalog der nachrichtendienstlichen Mittel erweitert wird, ist § 97 Absatz 3 Nummer 6 Buchstabe a zu beachten

Zu Absatz 2

Absatz 2 entspricht dem bisherigen § 62 Satz 1.

Zu Absatz 3

Mit der Regelung in Absatz 3 wird eine Verordnungsermächtigung geschaffen, welche es dem Bundesnachrichtendienst ermöglicht, in einer Dienstvorschrift dienst- und arbeitsrechtliche Verhaltenspflichten zu statuieren, die bei einem Verstoß entsprechende dienste- oder arbeitsrechtliche Sanktionen zur Folge haben können. Hierdurch soll letztlich Sicherheitsrisiken begegnet werden, welche z.B. bei besonders sicherheitsrelevantem Verhalten entstehen können, von dem die Bediensteten des Bundesnachrichtendienstes aufgrund ihrer besonderen Tätigkeit Abstand zu nehmen haben. Zwar würden solche Tätigkeiten regelmäßig auch Zweifel an der Zuverlässigkeit der betroffenen Person bei der Wahrnehmung einer sicherheitsempfindlichen Tätigkeit zeitigen, welche nach dem Sicherheitsüberprüfungsgesetz zu berücksichtigen wären. Gleichwohl würde eine bloße Entziehung des Sicherheitsbescheides bei bestimmten gefahrgeneigten Tätigkeiten letztlich nur dazu führen, dass der oder die entsprechende Bedienstete von seiner Tätigkeit beim Bundesnachrichtendienst freigestellt würde. Dies wird dem Umstand nicht gerecht, dass bei diesen Tätigkeiten auch ein sanktionswürdiges Verhalten vorliegen kann – etwa wenn ein vertiefter privater Kontakt zu Angehörigen oder Vertretern von Staaten, die nach Feststellung des Bundesministeriums des Innern besondere Sicherheitsrisiken für die mit sicherheitsempfindlicher Tätigkeit befassten Personen begründen (§ 13 Absatz 1 Nummer 17 des Sicherheitsüberprüfungsgesetz) unterhalten wird.

Die Regelungen der Dienstvorschrift können entsprechend insbesondere vorsehen, dass private Kontakte zu Personen, die eine Staatsangehörigkeit eines Staates mit besonderen Sicherheitsrisiken besitzen oder ihren Wohnsitz oder gewöhnlichen Aufenthalt in einem solchen Staat haben oder hatten, und ähnlichen abgrenzbaren Personengruppen, bei denen ein abstrakt erhöhtes Sicherheitsrisiko für den Bundesnachrichtendienst und seine Mitarbeitenden anzunehmen ist, unverzüglich anzuzeigen und vertiefte private Kontakte zu Personen untersagt sind. Dies setzt naturgemäß voraus – dies ist in der Dienstvorschrift entsprechend sicherzustellen – dass der oder die Bedienstete Kenntnis von diesem Umstand hat oder haben musste; anderenfalls liegt kein Fehlverhalten vor. Ebenfalls regelungsfähig ist, welche sonstigen für die Eigensicherung des Bundesnachrichtendienstes relevanten Umstände unverzüglich anzeigepflichtig sind.

Sofern und soweit das Privatleben der Mitarbeitenden tangiert wird, ist dabei indes zugleich schon gesetzlich dafür Sorge zu tragen, dass keine unverhältnismäßige Beeinträchtigung der privaten Lebensführung erfolgt. So ist eine Beeinträchtigung des Kernbereichs privater Lebensführung per se ausgeschlossen; eine Beeinträchtigung des übrigen Verhaltens außerhalb des Dienstes ist nur zulässig, wenn die entsprechende Verhaltenspflicht unumgänglich ist, um nicht unerheblichen Sicherheitsbedenken zu begegnen (ein Beispiel hierfür wäre ebenfalls die Regelung von Anzeigepflichten und Kontaktverboten bei vertieften, häufigen oder länger andauernden privaten Kontakten zu Personen, die eine Staatsangehörigkeit eines Staates mit besonderen Sicherheitsrisiken besitzen, oder ihren Wohnsitz oder gewöhnlichen Aufenthalt in einem solchen Staat haben oder hatten oder eine anderweitige enge Verbindung zu einem solchen Staat aufweisen, die dem Mitarbeitenden bekannt ist).

Die Vorschrift regelt im Verhältnis zu § 35 Absatz 4 des Sicherheitsüberprüfungsgesetzes nur die hier gesondert genannten Themenfelder und hat (nur) insoweit Vorrang gegenüber dem Sicherheitsüberprüfungsgesetz.

Zu Absatz 4

Die Dienstvorschriften nach den Abätzen 1 bis 3 und bedürfen der Zustimmung durch das Bundeskanzleramt. Inhaltlich unverändert sind die Dienstvorschriften nach Absatz 1 und 2 zudem dem Parlamentarischen Kontrollgremium vorzulegen (vgl. § 96). Die Unterrichtungspflicht an das Parlamentarische Kontrollgremium wurde an dieser Stelle gestrichen und in die oben genannte, zentrale Vorschrift integriert.

Zu § 96 (Unterrichtung des Parlamentarischen Kontrollgremiums und des Deutschen Bundestages)

Diese Vorschrift regelt zentral die Unterrichtungspflichten an das Parlamentarische Kontrollgremium. Dabei ist grundsätzlich zu berücksichtigen, dass eine Reihe von Berichtspflichten an das Parlamentarische Kontrollgremium unmittelbar durch den Unabhängigen Kontrollrat (und im UKRat-Gesetz geregelt) erfolgt.

Zu Nummer 1

Nummer 1 enthält die Unterrichtungspflicht bei CNE-Eingriffen gegenüber Inländern und Deutschen. Dem besonderen Eingriffsgewicht dieser Maßnahmen wird mittels dieser Unterrichtungspflicht durch eine (zusätzliche) parlamentarische Kontrolle begegnet.

Zu Nummer 2

Das Parlamentarische Kontrollgremium ist über Grundanordnungen für die Durchführung erweiterter nachrichtendienstlicher Maßnahmen gesondert und unverzüglich zu unterrichten. Dies folgt schon aus der großen (politischen) Bedeutung, welche von den entsprechenden Maßnahmen ausgehen kann.

Zu Nummer 3

In Nummer 3 ist die Auskunftspflicht für diejenigen Dienstvorschriften geregelt, die der Bundesnachrichtendienst nach § 95 Absatz 1 und 2 zu erlassen hat; also jene zu den nachrichtendienstlichen Mitteln und den technischen und organisatorischen Umsetzungen der Regelungen zum Einsatz besonderer technischer Aufklärungsmaßnahmen. Die Vorschrift entspricht dem bisherigen § 62 Satz 3.

Zu § 97 (Kontrollgegenstände die der Vorabkontrolle unterliegen)

Die Zuständigkeit des Unabhängigen Kontrollrates bestimmt sich anhand des gesetzlichen Zuständigkeitskatalogs. Dieser stellt eine gerichtsähnliche Rechtskontrolle der eingriffsintensiven Aufklärungsmaßnahmen sicher und versieht diese mit einer abschließenden Entscheidungsbefugnis des Unabhängigen Kontrollrates. Es wird unterschieden zwischen der Vorabkontrolle (also der Kontrolle von eingriffsintensiven Maßnahmen vor ihrer Durchführung) und der Einzelfallkontrolle (als gesetzlich bestimmte Kontrolle von Einzelvorgängen). Ergänzend nimmt der Unabhängige Kontrollrat auch die administrative Kontrolle wahr, dies ist im Gesetz über den Unabhängigen Kontrollrat geregelt.

Zu Absatz 1

In Absatz 1 werden die Vorgänge genannt, die dem Unabhängigen Kontrollrat im Wege der Vorabkontrolle vorzulegen sind. Kontrollgegenstand ist die jeweilige Anordnung, auch Verlängerungen von Anordnungen. Werden Maßnahmen über die in § 46 Absatz 3 geregelten Fristen hinaus verlängert, bedarf es jeweils einer Verlängerungsanordnung zur neuerlichen

Rechtmäßigkeitsfeststellung vor Durchführung der (Verlängerungs-)Anordnung. Zur Kontrolle sind die für die Prüfung erforderlichen Informationen vorzulegen. Dies ist in jedem Fall die Anordnung samt Begründung.

Der Maßstab für das Vorsehen einer Vorabkontrolle richtet sich dabei mit den Kriterien der Eingriffsgewichtung (ist dabei aber nicht vollständig deckungsgleich). Der Gesetzgeber legt für eingriffsintensiv wirkende nachrichtendienstliche Maßnahmen höhere materielle Schwellen fest, als für diejenigen nachrichtendienstlichen Maßnahmen, die auf Grundlage des § 18 durchgeführt werden dürfen. Innerhalb der eingriffsintensiv wirkenden nachrichtendienstlichen Maßnahmen werden zudem noch zwei Qualifikationsstufen unterschieden, wobei – mit Ausnahme des eingriffsintensiven Einsatzes einer nachrichtendienstlichen Verbindung nach § 24 Absatz 2 – ausschließlich die Maßnahmen der zweiten Qualifikationsstufe unter das Verfahrenserfordernis der unabhängigen Vorabkontrolle gestellt werden. Dies entspricht den verfassungsrechtlichen Erfordernissen.

In die Vorabkontrolle fallen Auskunftsersuchen und nach § 13 Absatz 1 Satz 2, die sich gegen eine der in § 12 Absatz 2 Nummer 4 und 5 genannten Stellen richten, soweit es sich nicht um Auskunftsersuchen zur Umsetzung von Maßnahmen handelt, die bereits für sich genommen der Vorabkontrolle unterliegen – z.B. eine Telekommunikationsüberwachung, die im Wege der Providerausleitung durch Auskunftsersuchen durchgeführt wird (Nummer 1). Auch Auskunftsersuchen nach § 14 Absatz 2, die bei informationstechnischen Angriffen auf die Herausgabe einer vollständigen Kopie gerichtet sind, unterfallen der Vorabkontrolle (Nummer 2).

Das Betreten einer Wohnung im Inland, um andere nachrichtendienstliche Mittel vorzubereit, unterfällt aufgrund des Eingriffs in Artikel 13 des Grundgesetzes stets der Vorabkontrolle (Nummer 3), ebenso der besondere Einsatz von ND-Mitteln nach § 19 Absatz 1 oder 2. Bei § 19 Absatz 1 oder 2 kommt der unabhängigen Anordnungskontrolle eine wichtige absichernde Funktion zu, da die tatbestandliche Unbestimmtheit dieser Regelung ein spezifisches Risiko von Fehlentwicklungen belässt. Dies gilt auch für den Einsatz neuer nachrichtendienstlicher Mittel, also solchen, die nicht in den vom Unabhängigen Kontrollrat geprüften abschließenden Katalog im Rahmen der Dienstvorschrift zu den nachrichtendienstlichen Mitteln aufgenommen wurden, da sie zum Zeitpunkt der Novellierung des Gesetzes noch nicht bekannt waren, sondern sie im Nachgang entwickelt wurden (vgl. dazu § 95). Um auch beim Einsatz neuer nachrichtendienstlicher Mittel zur Entwicklung und Erprobung die Verfassungskonformität umfassend zu gewährleisten, wird hier festgelegt, dass der jeweilige Einsatz neuer nachrichtendienstlicher Mittel durch den Unabhängigen Kontrollrat kontrolliert wird. Der Unabhängige Kontrollrat kontrolliert den Einsatz neuer nachrichtendienstlicher Mittel und prüft deren Einordnung in das Stufensystem, also die Einordnung unter § 18 Absatz 1 oder die Zuordnung ausnahmsweise zu den eingriffsintensiven nachrichtendienstlichen Mitteln entsprechend § 24ff. Bei einer Zuordnung des nachrichtendienstlichen Mittels unter § 18 Absatz 1 wird dieses in den abschließenden Katalog der nachrichtendienstlichen Mittel in der entsprechenden Dienstvorschrift aufgenommen. Erfolgt die Zuordnung zu den eingriffsintensiven nachrichtendienstlichen Mitteln werden für deren Einsatz in der Entwicklungs- und Erprobungsphase – da der Gesetzgeber diese in ihrer Entwicklungs- und Erprobungsphase noch nicht in einer Sondernorm mit spezifischen materiellen und/oder formellen Voraussetzungen erfassen konnte – besondere materielle Voraussetzungen festgelegt, unabhängig davon, welche Festlegungen durch den Gesetzgeber später für dieses neue nachrichtendienstliche Mittel getroffen werden.

Bei dem Einsatz konkreter nachrichtendienstlicher Mittel (Nummern 5 bis 16) ist anhand des jeweiligen Eingriffsgewichts, durch Durchführungsmodalität oder Zielrichtung indiziert, zu differenzieren. So ist beispielsweise bei einer eingriffsintensiven Observation der ersten Qualifikationsstufe nicht per se mit höchstprivaten Informationen zu rechnen, die eine unabhängige Vorabkontrolle induzieren. Wenn etwa ein Treff eines Mitarbeiters eines fremden Nachrichtendienstes mit seiner in Deutschland geführten Quelle überwacht wird, um Übergaben festzustellen, induziert auch ein Treff im nichtöffentlichen Raum nicht, dass

Höchstprivates ausgetauscht werden wird. Die nichtöffentliche Situation spricht für ein verdecktes Vorgehen, nicht für höchstprivate Kommunikationsinhalte. Bei der technischen Aufenthaltsüberwachung wird erst die Langfristüberwachung nach § 26 Absatz 2 (zweite Qualifikationsstufe) vom Erfordernis unabhängiger Vorabkontrolle erfasst, da mit höchstprivaten Informationen erst zu rechnen ist, wenn infolge langer Überwachung verfestigte Verhaltensmuster erkennbar werden, die besondere örtliche Bezüge der Person erschließen, die auch auf persönliche Beziehungen hindeuten können. Gleiches gilt für Observationen (§ 27 Absatz 2). Für das zusätzliche Erfordernis der Verfahrenssicherung der unabhängigen Vorabkontrolle kommt bei den nachrichtendienstlichen Maßnahmen der Aufenthaltsbestimmung oder der Observation der Dauer einer Maßnahme Bedeutung zu (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 220). Je länger eine solche Maßnahme durchgeführt wird, desto mehr steigert sich die Erwartbarkeit auch höchstprivater Informationen, weshalb diese Maßnahmen bei langer Dauer (§ 26 Absatz 2 sowie § 27 Absatz 2) materiell an die Voraussetzungen der zweiten Qualifikationsstufe gebunden werden und zusätzlich durchgängig der unabhängigen Anordnungskontrolle unterliegen.

Handelt es sich um die Anordnung einer strategischen Aufklärungsmaßnahme, so betrifft die Vorabkontrolle sowohl eine in ihr enthaltene Anordnung der Erhebung wie auch die Einsichtnahme. Dies meint dabei indes nicht, dass die konkrete Einsichtnahme in individuelle Daten von der Vorabkontrolle umfasst sind. Vielmehr ist eine abstrakte Prüfung der Möglichkeit einer Erhebung und Einsichtnahme erforderlich.

Eine Ausnahme bildet § 24. Hier wird auch in den Fällen des § 24 Absatz 2, der entsprechend seines Eingriffsgewichts als materielle Schwelle die Voraussetzungen der ersten Qualifikationsstufe vorsieht, eine unabhängige Vorabkontrolle festgelegt (Nummer 4). § 24 bestimmt Fallkonstellationen des Einsatzes von nachrichtendienstlichen Verbindungen, die über den Standardeinsatz dieses nachrichtendienstlichen Mittels hinausgehen und besonders eingriffsintensiv wirken (und damit höheren materiellen Schwellen unterliegen). Dies ist der Fall bei einem gezielten Einsatz gegen eine Person oder nochmals gesteigert durch eine hinzutretende besondere persönliche Vertrauensbeziehung zwischen der nachrichtendienstlichen Verbindung und der betroffenen Person. Bei diesen Fallkonstellationen sind die materielle Schwelle sowie das Erfordernis der unabhängigen Vorabkontrolle – anders als bei Observationen oder Aufenthaltsbestimmungen – nicht von einer bestimmten Dauer der Maßnahme, also der Dauer der Zusammenarbeit des Bundesnachrichtendienstes mit der nachrichtendienstlichen Verbindung (Führungsdauer) abhängig (abgesehen von der in der Norm festgelegten Erprobungsphase). Diese eingriffsintensiven Einsätze einer nachrichtendienstlichen Verbindung nach § 24 unterliegen insgesamt der unabhängigen Vorabkontrolle.

Zu Absatz 2

Neben den in Absatz 1 aufgeführten Anordnungen einzelner Maßnahmen findet sich in Absatz 2 die Pflicht, Grundanordnungen für die Durchführung erweiterter nachrichtendienstlicher Mittel vorzulegen.

Zu Absatz 3

Absatz 3 regelt die sogenannte Einzelfallkontrolle. Dabei sind die Vorgänge dem Unabhängigen Kontrollrat im jeweiligen Einzelfall zur Kontrolle vorzulegen. Dabei kann die Vorlage sowohl vor Durchführung der jeweiligen Maßnahme als auch nachträglich erfolgen.

Der Einzelfallkontrolle unterfallen insbesondere auch Entscheidungen zur Weiterverarbeitung und Übermittlung von Daten, die einen besonderen Schutzgehalt aufweisen, z.B. aus Vertraulichkeitsbeziehungen. Hier sind eine Übermittlung oder Weiterverarbeitung von personenbezogenen Daten nach § 22 Absatz 3 dem Unabhängigen Kontrollrat vorzulegen. Der Schutz dieser Personen bzw. der Vertraulichkeitsbeziehungen wird so ausreichend

gewahrt (vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 194 am Ende und für Übermittlung Rn. 240).

Im Falle der Vorlage von Dienstvorschriften nach Nummer 6 Buchstabe a) ist zu beachten, dass im Falle einer Ergänzung des Kataloges der nachrichtendienstlichen Mittel erneut eine Vorlage des Vorgangs an den Unabhängigen Kontrollrat erforderlich ist.

Zu Absatz 4

In Absatz 4 ist das Anhörungsverfahren geregelt. Der Unabhängige Kontrollrat wird vor dem Erlass von Errichtungsanordnungen angehört. Im Rahmen der Anhörung soll dem Unabhängigen Kontrollrat die Möglichkeit gegeben werden Bedenken gegen die Ausgestaltung einer Personendatenbank oder Datei nach § 79 und § 83 zu äußern. Der Bundesnachrichtendienst und das Bundeskanzleramt sind an die Stellungnahme des Unabhängigen Kontrollrats nicht gebunden. Sie sollen jedoch durch das Bundeskanzleramt und den Bundesnachrichtendienst geprüft und gegebenenfalls berücksichtigt werden. Der Bundesnachrichtendienst soll die Bemerkungen und Anregungen des Unabhängigen Kontrollrats in die Ermessenswägungen einbeziehen, die dem Betreib der Personaldatenbank zugrunde liegen. Satz 3 verdeutlicht, dass Fristbeginn die Übermittlung der Errichtungsanordnung an den Unabhängigen Kontrollrat ist. Die Frist wird auch durch die Übermittlung einer Sofortanordnung ausgelöst. Dies hat den Vorteil, dass der Bundesnachrichtendienst die Anregungen des Unabhängigen Kontrollrats unmittelbar bei der Erstellung der endgültigen Errichtungsanordnung berücksichtigen kann. Einer erneuten Anhörung bedarf es in diesen Fällen nicht.

Bei einer gemeinsamen Datei mit einer ausländischen Stelle erstreckt sich die Prüfkompetenz des Unabhängigen Kontrollrats lediglich auf die Errichtung der Datei und die durch den Bundesnachrichtendienst dort eingebrachten Daten. Nicht der Prüfkompetenz des Unabhängigen Kontrollrats unterfallen hingegen Daten der ausländischen Stellen oder die Nutzung der Datei durch selbige. Hierdurch soll deutlich gemacht werden, dass der Unabhängige Kontrollrat nicht dazu befugt ist die Nutzung einer gemeinsamen Datei durch die ausländischen Partner zu bewerten.

Zu Absatz 5

Die Kautelen für Maßnahmen bei Gefahr im Verzug wird detailliert im Gesetz über den Unabhängigen Kontrollrat (UKRatG) geregelt. Billigt der Unabhängige Kontrollrat die Maßnahme nicht innerhalb von drei Werktagen sind die erhobenen Daten zu löschen.

Zu Absatz 6

Artikel 13 Absatz 4 GG erfordert eine richterliche Anordnung, weshalb hier abweichend von Absatz 1 ein Gericht vorgesehen ist. Angesichts der geringen erwartbaren Fallzahl erscheint sachgerecht hierzu in Angleichung an § 50 Absatz 1 Nummer 4 VwGO die Zuständigkeit des Bundesverwaltungsgerichts vorzusehen.

Angesichts der gegenständlichen Besonderheit dieses gerichtlichen Feststellungsverfahrens wird es in Absatz 4 besonders geregelt, dies orientiert an den etablierten Vorabkontrollverfahren im nachrichtendienstlichen Bereich, dem neuen UKRat-Gesetz sowie den Geheimschutzregelungen des § 99 Absatz 2 VwGO. Dabei steht es im Ermessen des Gerichts, die Verfahrensbeteiligten vor einer Entscheidung über den Feststellungsantrag anzuhören oder ausschließlich auf Grundlage der eingereichten Unterlagen zu entscheiden. Wie in vergleichbaren Verfahren, etwa zu richterlichen Anordnungen im Ermittlungsverfahren nach der Strafprozessordnung, wird auch vorliegend die Entscheidung durch einen einzelnen Richter adäquat, bei Eilanordnungen eventuell auch verfahrenspraktisch geboten sein. Hiergegen kann allerdings die Entscheidung des Senats beantragt werden, auch um gegebenenfalls zu grundsätzlichen Fragen eine vom gesamten Senat getragene Linie herzustellen.

Zu Absatz 7

Der Absatz trägt den gegenständlichen Besonderheiten des Feststellungsverfahrens nach Absatz 6 verfahrensmäßig Rechnung. Die Ausgestaltung erfolgt einerseits unter Anlehnung an Geheimschutzregelungen des § 99 Absatz 2 VwGO und andererseits orientiert an vergleichbaren Verfahren, etwa zu richterlichen Anordnungen im Ermittlungsverfahren nach der Strafprozessordnung oder dem Verfahren des unabhängigen Kontrollrates nach dem Gesetz über den Unabhängigen Kontrollrat. Dabei steht es im Ermessen des Gerichts, den Bundesnachrichtendienst vor einer Entscheidung über den Feststellungsantrag anzuhören oder ausschließlich auf Grundlage der eingereichten Unterlagen zu entscheiden. Beteiligt ist allein der, eine Beiladung der Zielperson ist naturgemäß ausgeschlossen. Grundsätzlich ist die Entscheidung durch einen einzelnen Richter adäquat, bei Eilanordnungen eventuell auch verfahrenspraktisch geboten. Hiergegen kann allerdings die Entscheidung des Senats beantragt werden, auch um gegebenenfalls zu grundsätzlichen Fragen eine vom gesamten Senat getragene Linie herzustellen

Zu § 98 (Unabhängige Kontrolle durch den Unabhängigen Kontrollrat und die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit)

Ziel der Neuregelung ist eine klare Zuständigkeitsabgrenzung zwischen dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und dem Unabhängigem Kontrollrat. Dabei wird dem Grund nach die Kontrollzuständigkeit für die nachrichtendienstliche Auftragserfüllung beim Unabhängigen Kontrollrat konsolidiert. Der Verweis des bisherigen § 63 in den bisherigen § 28 BVerfSchG wird mit dieser Neuregelung der Norm aufgelöst.

Das Anrufungsrecht nach dem bisherigen § 28 Absatz 1 Bundesverfassungsschutzgesetz entfällt mit der Neuregelung hinsichtlich des oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, da eine Zuständigkeit insoweit ausschließlich beim Unabhängigen Kontrollrat besteht. Ein vergleichbares Anrufungsrecht wird in das Gesetz über die Rechtskontrolle durch den Unabhängigen Kontrollrat aufgenommen.

Zu Absatz 1

Durch die umfassende Rechtskontrolle aus einer Hand und ein Verzicht auf das Aufspalten von zusammengehörenden Vorgängen auf verschiedene Kontrollinstanzen wird die Kontrolle insgesamt gestärkt. Der Unabhängigen Kontrollrat ist nunmehr umfassend zuständig für die Kontrolle der Auftragsdatenverarbeitung durch den Bundesnachrichtendienst. Gleichermaßen ist der Unabhängige Kontrollrat auch für die Kontrolle der Datenverarbeitung im Rahmen von Maßnahmen zum Schutz der Bediensteten, Dienststellen und Verschlusssachen nach Abschnitt 8 zuständig. Die Notwendigkeit hierfür ergibt sich daraus, dass die im Rahmen von Abschnitt 8 erhobenen Daten denkbarerweise auch für die Auftragserfüllung Verwendung finden können. Die Kontrolle durch den Unabhängigen Kontrollrat wird in dem Gesetz über die Rechtskontrolle durch den Unabhängigen Kontrollrat näher geregelt.

Zu Absatz 2

Ausgenommen von der abschließenden Zuständigkeit des Unabhängigen Kontrollrats sind alleine die spezialgesetzlich normierten Kontrollkompetenzen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (etwa im § 36a SÜG, § 10 ATDG, dem § 4 VISZG oder der Art. 19 EU-Verordnung 2018/1860). Grund für die verbleibende Zuständigkeit ist der Umstand, dass sich die Prüfung dieser Systeme auf verschiedene Behörden erstreckt, für deren Kontrolle der Unabhängige Kontrollrat teilweise nicht zuständig ist oder sich der Gesetzgeber im Fall des SÜG dafür entschieden hat, die Kompetenz zentral bei dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu bündeln. Für den Bereich der Datenschutzkontrolle der allgemeinen Verwaltung des

Bundesnachrichtendienstes bleibt der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit das zuständige Kontrollorgan. Die Rügerechte des Unabhängigem Kontrollrates ist den bisherigen Beanstandungsrechten des oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gleichzusetzen. Die Auskunftsrechte gegenüber dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit folgt aus dem Bundesdatenschutzgesetz oder dem jeweiligen Fachgesetz (vgl. § 36a Absatz 1 SÜG).

Zu Absatz 3

Die Informationszugangsrechte für die beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verbleibende Kontrollkompetenz werden nur geringfügig gegenüber dem bisherigen § 28 Absatz 3 des Bundesverfassungsschutzgesetzes modifiziert:

Zunächst werden durch die im Vergleich zum geltenden Recht erfolgte Streichung des Wortes „insbesondere“ die Mitwirkungspflichten des Bundesnachrichtendienstes abschließend geregelt. Ein „jederzeitiges“ Zutrittsrecht (vgl. § 28 Absatz 3 Satz 2 Nummer 2 des Bundesverfassungsschutzgesetzes) erweist sich im Fall einer Behörde die in gesondert gesicherten Liegenschaften arbeitet als nicht durchführbar und zur Ausübung einer effektiven Kontrolle im Rahmen der bei dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verbleibenden Kontrollkompetenz nicht erforderlich.

Zu § 99 (Anwendung anderer Gesetze)

Zu Absatz 1

Absatz 1 entspricht dem bisherigen § 64, der insoweit geändert wurde, dass nunmehr der Unabhängige Kontrollrat den Bundesnachrichtendienst kontrolliert und nicht das Unabhängige Gremium.

Der Bundesnachrichtendienst hat, wie bislang, bei Wahrnehmung fachneutraler Verwaltungsaufgaben die Regelungen des BDSG und der DSGVO in dem genannten Umfang anzuwenden. Von einer fachneutralen Verwaltungsaufgabe ist auszugehen, wenn der Bundesnachrichtendienst Verwaltungsaufgaben wahrnimmt, die typischerweise in einer Vielzahl anderer Behörden anfallen. Dazu gehören etwa die Verarbeitung von Daten von Mitarbeitenden, Gesundheitsdaten selbiger, Bewerberdaten etc. Diese unterliegen den allgemeinen datenschutzrechtlichen Regelungen. Für die fachneutralen Verwaltungsaufgaben des Bundesnachrichtendienstes gilt gemäß § 1 Absatz 8 BDSG auch der Teil 2 des BDSG sowie die Datenschutzgrundverordnung.

Zu Absatz 2

Durch die Regelung sollen für den Bundesnachrichtendienst (bzw. konkret für Bauaufträge der Bundesanstalt für Immobilienaufgaben zur Deckung des Bedarfs des Bundesnachrichtendienstes) die Regelungen des Bundeswehr-Beschaffungsbeschleunigungsgesetzes gelten, welche Vereinfachungen für die Vergabe von Bauaufträgen der Bundesimmobilienanstalt durch Ausnahmen von den Voraussetzungen der Vergabeverordnungen, Ausnahmen vom Haushaltsrecht, Ausnahme von der AVV Klima sowie beschleunigte Nachprüfungsverfahren enthalten. Der Bundesnachrichtendienst ist wie die Bundeswehr ein wesentlicher Bestandteil der äußeren Sicherheit der Bundesrepublik sodass die in den in Bezug genommenen §§ 4 bis 17 des Bundeswehr-Beschaffungsbeschleunigungsgesetzes in gleichem Maße für ihn gelten.

Gegenüber einer generellen Ausnahme von dem Erfordernis eines Vergabeverfahrens (wie etwa in § 145 oder § 107 des Gesetzes gegen Wettbewerbsbeschränkungen vorgesehen) stellt der Verweis auf das Bundeswehr-Beschaffungsbeschleunigungsgesetzes ein milderes Mittel dar, da hier ein Vergabeverfahren noch durchzuführen ist. Im Gegenzug werden hier auch solche Vorhaben erfasst, die nicht einen unmittelbaren Zusammenhang mit der

nachrichtendienstlich Kerntätigkeit haben (sondern zum Beispiel auch Verwaltungsvorhaben).

Zu Unterabschnitt 2 (Mitteilung und Auskunftsverpflichtung)

Zu § 100 (Mitteilung an betroffene Personen)

Nachrichtendienste sammeln Daten grundsätzlich verdeckt. Der Grundsatz der Offenheit der Datenerhebung gilt für sie nicht, und sie sind von Transparenz- und Berichtspflichten gegenüber betroffenen Personen weithin freigestellt. Diese materiespezifischen Besonderheiten sind in der Verfassungsrechtsprechung anerkannt (BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 117; BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 150, 240, 290). Diesen Besonderheiten tragen besondere Kontrollstrukturen Rechnung. Neben der besonderen politischen Kontrolle nach Artikel 45d des Grundgesetzes durch das Parlamentarische Kontrollgremium ist auch und insbesondere eine unabhängige Kontrolle durch den Unabhängigen Kontrollrat eingerichtet, der verbindlich über die Zulässigkeit eingriffsintensiver Maßnahmen entscheidet. Der nachrichtendiensttypischen Aufgabenwahrnehmung ohne Kenntnis betroffener Personen entspricht zudem eine besonders intensive Wahrnehmung der betreffenden Kontrollaufgaben, einschließlich Strukturkontrollen durch den Ständigen Bevollmächtigten des Parlamentarischen Kontrollgremiums, die gewährleisten, dass sich Durchführungspraktiken und das zugrunde liegende Rechtsverständnis nicht ausschließlich innerbehördlich etablieren, sondern sich im Diskurs mit externer Kontrolle entwickeln.

Neben diesen umfänglichen externen Kontrollmöglichkeiten besteht auch gegenüber betroffenen Personen bei bestimmten, eingriffsintensiven Maßnahmen eine Mitteilungspflicht. Dadurch wird die Möglichkeit effektiven Rechtsschutzes nach Art. 19 Abs. 4 Grundgesetz unter Berücksichtigung der Besonderheiten nachrichtendienstlichen Handelns Genüge getan (BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 210 ff.). Die Mitteilungspflichten werden mit § 100 zudem gegenüber dem bisherigen § 59 BND-Gesetz und § 12 Artikel 10-Gesetz erweitert, indem weitere eingriffsintensive Maßnahmen, einschließlich der Wohnraumüberwachung, einbezogen werden, für die das bisher geltende Recht dies nicht vorsah. Die Mitteilungspflichten korrespondieren mit der Eingriffsgewichtung. Umfasst werden somit eingriffsintensive nachrichtendienstliche Maßnahmen, die (mindestens) vom Vorliegen der zweiten Qualifikationsstufe – also Bedrohungen von herausgehobener Bedeutung – abhängig sind.

Die Mitteilungspflicht begründet keine Befugnis zu eingriffsvertiefenden Maßnahmen. Liegt eine zustellungsfähige Anschrift nicht vor, dürfen dazu keine eigenen Ermittlungen erfolgen, so dass hier im Ergebnis eine Mitteilung unmöglich ist. Eine bloße Melderegisterabfrage (§ 34 BMG) hat allerdings keinen hinzutretenden Eingriffsgehalt. Zwar werden dabei personenbezogene Daten verarbeitet, diese Verarbeitung bleibt aber gerade auf die direkte Erhebung der Meldeanschrift begrenzt. Anders ist der Sachverhalt etwa bei einer unbekannt ins Ausland verzogenen Person.

Zu Absatz 1

In Absatz 1 ist zunächst die allgemeine Mitteilungspflicht für besonders geregelte Formen von Auskunftsersuchen (Nummer 1) sowie für solche Maßnahmen geregelt, deren tatbestandliche Voraussetzungen an tatsächliche Anhaltspunkte geknüpft sind, dass mit ihnen Informationen zu Bedrohungen von herausgehobener Bedeutung erlangt werden können (Nummer 2). Zusätzlich hat auch im Falle einer Wohnraumüberwachung, der „Ersatzvornahme“ eines Auskunftsersuchens nach § 14 Absatz 2 durch das nachrichtendienstliche Mittel des „Auslesens technischer Spuren bei informationstechnischen Angriffen“ nach § 36 Absatz 1 und für die sog. „Onlinedurchsuchung“ nach § 37 Absatz 3 eine Mitteilung zu erfolgen (Nummer 3).

Anknüpfungspunkt für die Mitteilung ist die Beendigung der Maßnahme. Dies bezieht sich dabei auf die Beendigung der Gesamtmaßnahme, welche von der jeweiligen Anordnung (oder einer Erweiterungs-, Verlängerungs- oder Folgeanordnung) umfasst ist. Ist also eine Maßnahme auf mehrere Betroffene gerichtet, so hat eine Mitteilung erst dann zu erfolgen, wenn die Maßnahme insgesamt beendet wird, nicht schon, wenn die Maßnahme gegen einzelne der genannten Betroffenen eingestellt (bzw. nicht verlängert oder geändert) wird.

Die in der Norm verankerte grundsätzliche Wertung ist, dass – erst – bei dem Einsatz nachrichtendienstlicher Mittel, deren Eingriffsgewicht wenigstens das Vorliegen einer Bedrohung von herausgehobener Bedeutung erfordert, eine Mitteilungspflicht entsteht. Insoweit ist zur Wahrung der Verhältnismäßigkeit und in Entsprechung des Grundsatzes, dass in diesen Fällen (wenigstens regelmäßig) auch eine unabhängige Vorabkontrolle der jeweiligen Maßnahmen erforderlich ist, davon auszugehen, dass es der betroffenen Person ermöglicht werden muss, von der Maßnahme tatsächlich auch Kenntnis zu nehmen, um nötigenfalls gerichtlich gegen sie vorgehen zu können. Demgegenüber überwiegt bei nachrichtendienstlichen Mitteln, deren jeweiliges Eingriffsgewicht keine Bedrohung von herausgehobener Bedeutung voraussetzt, die Erfordernisse des Quellen- und Methodenschutzes des Bundesnachrichtendienstes. Letztere rechtfertigen dabei – vgl. BVerfG, Beschluss vom 17. Juli 2024, 1 BvR 2133/22, Rn. 73 – ein „abgestuftes Regelungskonzept“, welches durch die an Bedrohungen von herausgehobener Bedeutung (als zweiter Qualifikationsstufe) anknüpfende Mitteilungspflicht gerade abbildet.

Die Auskunft bleibt ausgeschlossen, wenn sie die Aufgabenwahrnehmung der informationsführenden Behörde gefährdet (BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 210). Daher begründet der Einsatz nachrichtendienstlicher Mittel, deren Eingriffsgewicht „nur“ eine erhebliche Bedrohung (erste Qualifikationsstufe) voraussetzt, noch keine Mitteilungspflicht. Die maßgebende Beeinträchtigung des Quellen- und Methodenschutzes ist dabei in zweierlei Hinsicht angelegt: Einerseits geht bereits von einer einzelnen Mitteilung eine (regelmäßig begrenzte) Beeinträchtigung des Quellen- und Methodenschutzes einher, die in Abwägung zu den Rechten der jeweiligen Betroffenen gesetzt werden muss. Andererseits, weitergehend und entscheidend würde aber eine Mitteilungspflicht schon bei nachrichtendienstlichen Mittlen der ersten Qualifikationsstufe dazu führen, dass eine Mitteilung zu einer Vielzahl von nachrichtendienstlichen Maßnahmen des Bundesnachrichtendienstes erfolgen würde, welche in ihrer Gesamtschau ganz beträchtliche Erkenntnisse über die Arbeitsweise, Methoden und Fähigkeiten ermöglichen würde. Hierbei ist besonders zu berücksichtigen, dass diese Erkenntnisse auch durch ausländische Nachrichtendienste gezielt erhoben werden könnten, um die operativen Fähigkeiten des Bundesnachrichtendienstes auszuspähen und einzuschränken. Letzteres wiederum hätte indirekt auch eine Gefährdung der Mitarbeiterinnen und Mitarbeiter des Bundesnachrichtendienstes zur Folge.

Zu Absatz 2

In Absatz 2 findet sich die Mitteilungspflicht infolge einer Einsichtnahme in personenbezogene Daten, die im Wege der strategischen Aufklärung erhoben wurden. Hier besteht eine Mitteilungspflicht – dem geltenden Recht bei veränderter Systematik entsprechend – nur dann, wenn Einsicht in kommunikationsbezogenen Inhaltsdaten genommen wurde. Zudem ist geregelt, dass die Mitteilung in diesem Fall grundsätzlich bereits nach Einsichtnahme erfolgen muss und nicht (erst) bei Beendigung der Maßnahme, da letztere im Rahmen der strategischen Aufklärung häufig länger andauert. Dies greift die bisherige Wertung des § 6 des Artikel 10-Gesetzes auf. In zeitlicher Hinsicht gilt dabei – auch hier –, dass der relevante Zeitpunkt der Einsichtnahme derjenige ist, in dem eine „Meldung“ erstellt wird, welche die personenbezogenen Daten für die inhaltliche Auswertung durch Mitarbeiterinnen und Mitarbeiter des Bundesnachrichtendienstes verfügbar macht.

Zu Absatz 3

Nicht von den Mitteilungspflichten umfasst sind Ausländer im Ausland (Satz 1). Hierunter fallen auch solche Personen, die sich nur vorübergehend in Deutschland aufhalten. Unter „vorübergehend“ ist dabei nicht nur die kurze Durchreise zu verstehen, vielmehr ist darauf abzustellen, inwieweit auch zum Zeitpunkt der Mitteilung – ein Jahr nach Beendigung der Maßnahme – noch ein verstetigter Aufenthalt in der Bundesrepublik Deutschland vorliegt. Es ist nämlich zu beachten, dass die Mitteilung nachrichtendienstlicher Maßnahmen an die in Satz 1 genannten Personen bereits aus Gründen des Schutzes dieser Personen nicht geboten ist, da für sie eine Mitteilung durch den Bundesnachrichtendienst mitunter zu Repressionen ihres Heimatlandes führen könnte.

Im Rahmen der Mitteilungspflicht nach Absatz 1 – also bezüglich zielgerichteter, „nichtstrategischer“ Maßnahmen – ist in Satz 2 zudem grundsätzlich vorgesehen, dass sich die Mitteilungspflicht ausschließlich auf das Aufklärungsziel einer Maßnahme, d.h. die durch die Maßnahme aufklärte Person, bezieht und nicht auch auf Dritte, die etwa als Gesprächspartner oder anderweitig zufällig erfasst worden sind. Diese sind nicht betroffene Person im Sinne des Gesetzes, da sich die nachrichtendienstliche Maßnahme nicht gegen sie richtet. Durch nachrichtendienstliche Mittel werden mitunter eine Vielzahl von personenbezogenen Daten von nachrichtendienstlich irrelevanten Personen erhoben werden. So ist etwa im Rahmen einer Observation mit technischen Mitteln nicht zu vermeiden, dass auch unbeteiligte Dritte von der Maßnahme miterfasst werden. Diese Personen haben regelmäßig weder ein gesteigertes Interesse an einer Mitteilung noch wäre eine solche für den Bundesnachrichtendienst mit verhältnismäßigem Aufwand umsetzbar. Für die strategische Aufklärung handelt es sich insoweit (nur) um eine Person, deren personenbezogener Suchbegriff gesteuert wurde. Eine entsprechende Mitteilungspflicht war auch bislang nicht vorgesehen.

Zu Absatz 4

Zu Nummer 1

In Nummer 1 sind zunächst solche Sacherhalte ausgenommen, bei denen geheimdienstliche Aktivitäten einer fremden Macht zu besorgen sind. Hier würde eine Mitteilung zu dem widersinnigen Ergebnis führen, dass der Bundesnachrichtendienst seine Kontrahenten auf Aufklärungsbemühungen hinweisen und diese so warnen würde. Zudem ist hier auch kein besonderes grundrechtlich gestütztes Interesse der betroffenen Personen an einer Mitteilung gegeben.

Zu Nummer 2

Eine Mitteilung unterbleibt, wenn die Maßnahme in ihrer Durchführung unter Mithilfe menschlicher Quellen erfolgte – in der Terminologie des Bundesnachrichtendienstes sog. „nachrichtendienstliche Verbindungen“, vgl. § 23 Absatz 1. Es würde die nachrichtendienstliche Tätigkeit maßgeblich gefährden, nämlich nahezu ausschließen, menschliche Quellen zu gewinnen, wenn sie erwarten müssten, dass ihre Zusammenarbeit mit einem Nachrichtendienst der betroffenen Person später mitgeteilt wird. Hier ist das Persönlichkeitsrecht der Quelle und die Funktionsfähigkeit nachrichtendienstlicher Aufklärung – zum Schutz herausragender Rechtsgüter – gewichtiger als das Informationsinteresse der betroffenen Person (vgl. BVerfG, Urteil vom 14. Dezember 2022, 2 BvE 8/21, insbesondere Rn. 112ff. sowie auch ständige BVerwG-Rechtsprechung - insbesondere BVerwG, Beschluss vom 24. Oktober 2018, 20 F 15.16, Rn. 27ff.). Das Bundesverfassungsgericht hat in seiner jüngeren Rechtsprechung im Übrigen ausdrücklich darauf hingewiesen, dass auf der Hand liegt, dass Benachrichtigungspflichten Erfordernisse des Quellen- und Methodenschutzes entgegenstehen können (BVerfG, Beschluss vom 17. Juli 2024, 1 BvR 2133/22, Rn. 73). Bereits vorausgegangen (BVerfG, Beschluss vom 16. Dezember 2020, 2 BvE 4/18, Rn. 112) hatte es ausgeführt, dass bei menschlichen Quellen bereits der subjektive Eindruck, die Vertraulichkeit sei nicht gesichert, ausreichen kann, Quellen von einer weiteren Zusammenarbeit

abzuhalten und die Gewinnung neuer Quellen zu erschweren, was wiederum die Aufgabenerfüllung der Nachrichtendienste gefährden kann, die auf den langfristigen Einsatz von Quellen (für den Bundesnachrichtendienst sind dies nachrichtendienstliche Verbindungen) im betreffenden Milieu angewiesen sind.

Zu Nummer 3

Eine Mitteilung unterbleibt ferner dann, wenn in personenbezogene Daten, die im Wege der strategischen Aufklärung erhoben wurden, zwar eine Einsichtnahme erfolgt, die Daten indes unverzüglich hieran anschließend gelöscht oder unkenntlich gemacht werden. Dabei darf die Unkenntlichmachung auch so erfolgen, dass die Eindeutigkeit der Daten erhalten bleibt. Die Unkenntlichmachung soll eine rückwirkende Identifizierung der betroffenen Person unmöglich, jedenfalls aber nur mit unvertretbar hohem Aufwand möglich machen. Die Erhaltung der Eindeutigkeit ist nach der Regelung möglich, jedoch nicht gesetzlich gefordert, wobei eine Eindeutigkeit im Sinne der Vorschrift auch dann erreicht sein kann, wenn die Wahrscheinlichkeit so hoch ist, dass ernsthafte Zweifel nicht mehr bestehen. Bestimmte Anforderungen an das Verfahren zur Unkenntlichmachung werden durch den Gesetzgeber nicht vorgegeben, die Wahl des Verfahrens zur Unkenntlichmachung der Daten bleibt dem Bundenachrichtendienst überlassen. Zur Unkenntlichmachung vergleiche die Ausführungen zu § 32 Absatz 3 Nummer 4.

In diesen Fällen wird durch die unverzügliche Löschung (die faktisch dadurch begründet ist, dass die eingesehenen Daten keinen nachrichtendienstlichen Wert haben) bereits sichergestellt, dass die betroffenen Personen keinerlei nachteilige Folgen (etwa durch Weiterverarbeitung oder Übermittlung) zu befürchten haben. Durch die Unabsehbarkeit der Ergiebigkeit der strategischen Aufklärung würden anderenfalls überbordende Mitteilungspflichten entstehen, weil eben auch eine Vielzahl von „zufälligen“ Miterfassungen erfolgt, die erst im Rahmen der inhaltlichen Auswertung auf ihre nachrichtendienstliche Relevanz geprüft werden können.

Das Ausbleiben einer Mitteilungspflicht in diesen Fällen entspricht der Wertung des bislang geltenden § 59 Absatz 2 Satz 1.

Zu Nummer 4

In Nummer 4 wird dem Bundesnachrichtendienst die Möglichkeit einer Einzelfallprüfung auf Grundlage von Verhältnismäßigkeitskriterien eröffnet. So ist die Mitteilungspflicht gegenüber Betroffenen nicht „absolut“, sondern muss mit den Sicherheitsinteressen (d.h. dem Schutz von besonders gewichtigen Rechtsgütern) in Ausgleich gebracht werden. Hierbei sind Fälle denkbar, in denen eine Abwägung zu dem Ergebnis führt, dass eine Mitteilung zu einer unverhältnismäßigen Beeinträchtigung der geschützten Rechtsgüter führen würde. Um diesem Umstand zu begegnen, kann der Bundesnachrichtendienst bei Zustimmung des Unabhängigen Kontrollrates (vgl. Absatz 4 Satz 2) von einer Mitteilung absehen, ohne dass es einer vorherigen Zurückstellung bedarf.

Die Entscheidung ist dabei „perspektivisch“ auszurichten – anders als in den Fällen der Zurückstellung der Mitteilung nach § 101 ist insoweit entscheidend, dass eine bloße Zurückstellung eine bloße bürokratische Förmlichkeit darstellen würde, da bereits zum Zeitpunkt der Begründung der Mitteilungspflicht mit an Sicherheit grenzender Wahrscheinlichkeit klar ist, dass die Verhältnismäßigkeitsprüfung auch in der Zukunft zu keinem anderen Ergebnis führen kann, als das eine Mitteilung auszubleiben hat. Den letztgenannten Aspekt aufgreifend ist in der Nummer ein entsprechendes Regelbeispiel vorgesehen, welches an die Zurückstellungsgründe einer Mitteilung (hierzu nachfolgend) anknüpft. Liegen tatsächliche Anhaltspunkte schon bei Einstellung der Maßnahme dafür vor, dass diese Zurückstellungsgründe auch in Zukunft gegeben sein werden, ersetzt die Nichtmitteilungsentscheidung die eigentlich vorgesehene Zurückstellung, die in diesem Fall zu einer bloßen Förmelei werden würde.

Zu Nummer 5

Die Wertung der Nummer 2 aufgreifend ist auch dann von einer Mitteilung abzusehen, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Mitteilung nachteilige Folgen für den Betroffenen zeitigen würde. In diesem Fall würde die Mitteilung gerade ihrem eigentlichen Zweck zuwiderlaufen. Auch diesbezüglich ist eine vorherige Zustimmung des Unabhängigen Kontrollrates erforderlich.

Zu Nummer 6

Zuletzt unterbleibt eine Mitteilung dann, wenn die betroffene Person nicht identifiziert werden kann. Dieser Fall der „praktischen Unmöglichkeit“ ist keine Momentaufnahme. Vielmehr greift Nummer 6 nur, wenn auch in Zukunft eine Identifikation der betroffenen Person mit an Sicherheit grenzender Wahrscheinlichkeit nicht erfolgen kann.

Zu Absatz 5

Absatz 5 entspricht dem bisherigen § 12 Absatz 3 Artikel 10-Gesetzes.

Zu § 101 (Zurückstellung der Mitteilung)

Die Vorschrift des § 101 entspricht in ihrem Regelungsgehalt dem bisherigen § 59 Absatz 2 Satz 2 bis 4 sowie des § 12 des Artikel 10-Gesetzes, wobei die Zuständigkeit der G10-Kommission durch die des Unabhängigen Kontrollrates ersetzt wird.

Geregelt wird die Zurückstellung einer – eigentlich nach § 100 Absatz 1 und 2 bestehenden Mitteilungspflicht, die sich nunmehr auf alle Fälle einer bestehenden Mitteilungspflicht bezieht, also insbesondere auch die dort genannten eingriffsintensiven Maßnahmen (bzw. Auskunftsverlangen) mit einschließt.

Die Systematik der bisherigen Regelungen wird abgewandelt und normenklarer gefasst: In Absatz 1 ist die Möglichkeit der Zurückstellung sowie die hierfür bestehenden Voraussetzungen geregelt. In Absatz 2 wird statuiert, dass eine Zurückstellung für länger als zwölf Monate der Zustimmung des Unabhängigen Kontrollrates bedarf, der sodann auch die Dauer der weiteren Zurückstellung bestimmt. In Absatz 3 ist die Möglichkeit eines endgültigen Absehens von der Mitteilung geregelt und die diesbezüglichen Voraussetzungen aufgeführt, wobei letztere teilweise von den bisherigen Regelungen abweichen. Insoweit ist insbesondere unerheblich, ob die Daten noch bei einer anderen Stelle gespeichert sind; dieser Umstand kann für die weitere Speicherung durch den Bundesnachrichtendienst (auch vor dem Gesichtspunkt, dass von dieser Speicherung ein fortwährender Grundrechtseingriff ausgeht) nicht leitend sein.

Zu § 102 (Auskunft an betroffene Personen)

Die Regelungen zu Auskünften an betroffene Personen werden von den Regelungen in § 15 BVerfSchG entkoppelt. Die Entkopplung dient der Klarstellung und besseren Lesbarkeit. Der Auskunftsanspruch wird ferner insoweit eingeschränkt, als bestimmte Datenkategorien von vornherein von dem Auskunftsanspruch ausgenommen werden.

Zu Absatz 1

Die Vorschrift begrenzt den Auskunftsanspruch in Abweichung von dem bisherigen Recht auf solche Daten, die zu einer betroffenen Person in einer Personendatenbank des Bundesnachrichtendienstes gespeichert sind (Satz 1) oder die in anderen Speichermedien des Bundesnachrichtendienstes gespeichert und über die Personendatenbanken des Bundesnachrichtendienstes auffindbar sind (Satz 2). Hierdurch wird auch die Auskunft zu solchen Daten ausgeschlossen, die eine andere verantwortliche Stelle in durch den Bundesnachrichtendienst betriebenen gemeinsamen Dateien gespeichert hat. Dies trägt dem

datenschutzrechtlichen Grundsatz der Verantwortlichkeit der speichernden Stelle Rechnung. Zur Definition der Personendatenbank siehe die Begründung zu § 52 Absatz 3.

Nach der Rechtsprechung des Bundesverfassungsgerichts hat der Gesetzgeber bei der Ausgestaltung der Rechtsgrundlage für den Zugang zu Informationen zu berücksichtigen, welche Bedeutung dieser für die Grundrechte des Betroffenen hat. Hierfür sind insbesondere die Art und die Eingriffsintensität der jeweiligen informationsbezogenen Maßnahme von Bedeutung, über die oder über deren Ergebnisse der Betroffene informiert werden will (BVerfGE 120, 351 (363 f.)). Die grundsätzliche Begrenzung der Auskunft auf Daten in Personendatenbanken und hierüber recherchierbare Daten trägt dieser Erwägung Rechnung. So sind alle Personen, die mit der Aufgabenerfüllung des Bundesnachrichtendienstes in Zusammenhang stehen, über die Personendatenbanken recherchierbar. Die Notwendigkeit hierfür ergibt sich bereits aus operativen und operativ-sicherheitlichen Erwägungen. So muss etwa jede Zielperson und jede nachrichtendienstliche Verbindung zentral recherchierbar sein. Dementsprechend sind über die Personendatenbanken des Bundesnachrichtendienstes nur solche Personen nicht auffindbar, die zwar in den Speichermedien des Bundesnachrichtendienstes gespeichert sind, die aber nicht Gegenstand des nachrichtendienstlichen Interesses des Bundesnachrichtendienstes sind und die dieser im Rahmen seiner Aufgabenerfüllung auch selbst nicht über die Personendatenbanken auffinden würde, zum Beispiel wenn der Name eines Betroffenen als Autor in einem Zeitungsartikel erscheint, welchen der Bundesnachrichtendienst im Rahmen seiner Aufgabenerfüllung abgespeichert hat. In diesen Fällen hat die bloße Speicherung ein geringes Eingriffsgewicht. Für diese Personen besteht keine über die Speicherung hinausgehende Grundrechtsrelevanz, da sie nicht Gegenstand nachrichtendienstlicher Maßnahmen sind. Dem steht ein unverhältnismäßiger Verwaltungsaufwand für den Bundesnachrichtendienst gegenüber, wenn er bei jedem Auskunftsverlangen stets alle automatisiert durchsuchbaren Dateien berücksichtigen müsste.

Vor diesem Hintergrund sieht Satz 3 der Vorschrift eine Ausnahme für solche Fälle vor, in denen der Betroffene konkrete Angaben macht, die das Auffinden seiner Daten in Dateien außerhalb der Personendatenbanken mit einem angemessenen Aufwand möglich macht. Sollte es dem Bundesnachrichtendienst aufgrund moderner Technologien oder der Abschaffung von Papiervorgängen perspektivisch möglich sein, ohne besonderen Aufwand eine Recherche anhand etwa nur des Namens durchzuführen, würde der Satz 3 insoweit häufiger zur Anwendung kommen.

Zu Absatz 2

Absatz 2 schließt bestimmte Arten von Daten von vornherein aus dem Auskunftsanspruch aus. Für diese Daten besteht kein Auskunftsanspruch nach Absatz 1. Eine Einzelfallabwägung des Auskunftsinteresses des Betroffenen mit den jeweils einschlägigen staatlichen Geheimhaltungsinteressen ist nicht durchzuführen. Ein Ermessen besteht nicht. Da die entsprechenden Daten nicht von dem Auskunftsanspruch nach Absatz 1 umfasst sind, erfolgt keine Verweigerung gegenüber dem Betroffenen und es ist keine individuelle Sperrerklärung durch das Bundeskanzleramt abzugeben. Nach der Rechtsprechung kann ein Anspruchsausschluss ohne Einzelfallabwägung dann zulässigerweise festgelegt werden, wenn im Regelfall zu erwarten ist, dass die Belange des Bundesnachrichtendienstes bei Offenlegung der entsprechenden Daten wesentlich intensiver tangiert würden als es das Informationsinteresse des Betroffenen ohne seine Auskunftserteilung würde (BVerwG, NVwZ 2018, 590 (593) Rn. 29). Auf alle in Absatz 2 genannten Daten trifft dies zu.

Zu Nummer 1

Die Auskunft erstreckt sich entsprechend § 15 Bundesverfassungsschutzgesetz des bisherigen Rechts nicht auf die Herkunft der Daten und die Empfänger von Übermittlungen. Das Geheimhaltungsinteresse überwiegt hier regelmäßig das Informationsinteresse des

Betroffenen und die Ausschlussregelung ist geboten, um die wirksame Aufgabenerfüllung des Bundesnachrichtendienstes sicherzustellen (vgl. BVerfG, NVwZ2016, 1487 (1488) Rn.18).

Zu Nummer 2

Nach Absatz 2 Nummer 2 sind Daten, bei deren Offenlegung die erhebliche Gefahr besteht, dass nachrichtendienstliche Verbindungen offengelegt würden, nicht von dem Auskunftsanspruch nach Absatz 1 umfasst. In derartigen Konstellationen hat das Informationsinteresse des Betroffenen gegenüber den staatlichen Geheimhaltungsinteressen zurückzustehen. Der Begriff nachrichtendienstliche Verbindung meint wie in Absatz 3 Nummer 2 den konkreten Ursprung der Information (BVerwG, Urt. v. 24.03.2010 – 6 A 2.09, BeckRS 2010, 52039, Rn. 45). Nach Auffassung des Bundesverfassungsgerichts dient der „Schutz von Informationsquellen und insbesondere von V-Leuten […] nicht nur den Interessen der betroffenen Personen, sondern hat auch für die Arbeitsweise und Funktionsfähigkeit der Nachrichtendienste erhebliche Bedeutung“ (BVerfGE 146, 1 (51), Rn. 112). Besteht im Gegensatz zu Absatz 3 Nummer 2 nicht lediglich die abstrakte Möglichkeit, dass nachrichtendienstlichen Verbindungen – gegebenenfalls mittelbar – gefährdet sein könnten, sondern sogar eine erhebliche Gefahr für ihre Offenlegung, überwiegt das Geheimhaltungsinteresse das Auskunftsinteresse des Betroffenen grundsätzlich. Selbst gewichtigere Informationsinteressen müssen demgegenüber in aller Regel zurückstehen. Umfasst sind neben aktiven nachrichtendienstlichen Verbindungen ebenfalls solche, die zu einem früheren Zeitpunkt für den Bundesnachrichtendienst oder für eine mit ihm zusammenwirkende Dienststelle tätig waren oder eine solche Zusammenarbeit jedenfalls ernstlich angebahnt haben. Sind Angehörige oder sonstige mit der früheren oder aktiven nachrichtendienstlichen Verbindung nicht nur zeitweilig verbundene Personen durch die erhebliche Gefahr der Offenlegung ebenfalls (indirekt) bedroht, sind die sie betreffenden Informationen ebenfalls von dem Auskunftsanspruch ausgenommen, zumal sie üblicherweise Rückschlüsse auf die Identität der nachrichtendienstlichen Verbindung selbst ermöglichen.

Zu Nummer 3

Nach Absatz 2 Nummer 3 erstreckt sich die Auskunft von vornherein nicht auf Daten, bei deren Offenlegung eine Gefährdung operativer Vorgänge des Bundesnachrichtendienstes zu besorgen ist. Operative Vorgänge sind sämtliche – nicht zwingend noch laufende – Maßnahmen, die zur Informationsgewinnung durchgeführt werden. Ausschlaggebend ist nicht allein der Schutz nachrichtendienstlicher Verbindungen, sondern auch die Gefahr, dass durch die Offenlegung operativer Vorgänge deren weitere Durchführung gefährdet oder Rückschlüsse auf die Arbeitsweise des Bundesnachrichtendienstes möglich werden (vgl. BVerwG, NVwZ 2025, 1184 (1185), Rn. 19). Die Annahme, dass dieses Risiko im Rahmen einer Abwägung typischerweise die Interessen des Betroffenen übertrifft, entspricht der Rechtsprechung des Bundesverwaltungsgerichts zum verfassungsunmittelbaren und hoch zu gewichtenden presserechtlichen Informationsanspruch gegen den Bundesnachrichtendienst. Hiernach wird sich das „Interesse an einem Geheimschutz für die operativen Vorgänge […], ohne dass hierzu nähere Darlegungen […] erforderlich sind, regelmäßig in der Abwägung mit dem Informationsinteresse […] durchzusetzen“ (vgl. BVerwG, NVwZ 2025, 1184 (1185), Rn. 19). An dieser zutreffenden Abwägung der sich widerstrebenden staatlichen und betroffenenseitigen Interessenslagen orientiert sich der Ausschluss von operativen Vorgängen des Bundesnachrichtendienstes im Bereich des Auskunftsrechts des Betroffenen.

Außerdem erstreckt sich die Auskunft nach Absatz 2 Nummer 3 von vornherein nicht auf Daten, deren Offenlegung die Funktions- und Kooperationsfähigkeit des Bundesnachrichtendienstes beeinträchtigen könnte. In diesen Fällen überwiegt das Geheimhaltungsinteresse typischerweise das Auskunftsinteresse des Betroffenen. Der Bundesnachrichtendienst ist für seine Aufgabenerfüllung auf die Zusammenarbeit mit anderen Nachrichtendiensten angewiesen. Eine den Vereinbarungen mit Partnerdiensten zuwiderlaufende

Informationsoffenbarung kann das Vertrauensverhältnis zu Partnerdiensten empfindlich stören und die Funktions- und Kooperationsfähigkeit des Bundesnachrichtendienstes dadurch schwerwiegend beeinträchtigen (BVerfGE 143, 101 (145 f.) Rn. 144 ff.). Die weltweite Zusammenarbeit von Nachrichtendiensten ist durch die sog. Third Party Rule geprägt, nach der übermittelte Erkenntnisse ohne Zustimmung des Informationsgebers nicht an Dritte weitergegeben oder für andere Zwecke verwendet werden dürfen. Eine unter Missachtung der Third Party Rule ergehende Beauskunftung dürfte regelmäßig geeignet sein, die Aufgabenerfüllung des Bundesnachrichtendienstes erheblich zu beeinträchtigen. Nach der verfassungsgerichtlichen Rechtsprechung überwiegt in diesem Fall das Geheimhaltungsinteresse sogar gegenüber dem – als wesentlichem Instrumentarium besonders hoch zu gewichtenden – parlamentarischen Informationsinteresse (vgl. BVerfGE 143, 101 (145f.), Rn. 144 ff.). Folglich wird in vergleichbaren Konstellationen das Auskunftsinteresse natürlicher Personen erst recht gegenüber dem staatlichen Geheimhaltungsinteresse zurückstehen müssen.

Zu Absatz 3

In Absatz 3 werden die Versagungsgründe des § 15 Absatz 2 Satz 1 Bundesverfassungsschutzgesetz des bisherigen Rechts aufgeführt. Für das Unterbleiben der Auskunft ist es einer der vier genannten Versagungsgründe nach im Einzelfall zu treffender Abwägung des staatlichen Geheimhaltungsinteresses und des individuellen Informationsinteresses greift (vgl. BVerfG, NVwZ 2001, 185 (187); BVerwG, Urt. v. 24.03.2010 – 6 A 2.09, BeckRS 2010, 52039, Rn. 29). Absatz 3 Satz 2 setzt somit zwingend voraus, dass eine Information im Grundsatz überhaupt von dem Auskunftsanspruch erfasst wird, also insbesondere nicht durch Absatz 1 Satz 3 oder Absatz 2 von vornherein von diesem ausgenommen ist. Absatz 3 Satz 1 ermöglicht eine interessengerechte Abwägung im konkreten Einzelfall, in deren Rahmen neben den Auskunftsbelangen des Betroffenen das Staatswohl sowie Belange Privater Berücksichtigung finden.

Der Absatz betrifft insbesondere auch die „Negativauskunft“ – wenn also keine auskunftspflichtigen Daten gespeichert sind, kann der Bundesnachrichtendienst ebenfalls von einer entsprechenden Mitteilung an den Betroffenen absehen, wenn einer der Ausschlussgründe (hier relevant Nummer 1 und 3) vorliegt.

Zu Absatz 4

Absatz 4 entspricht der Regelung des § 15 Absatz 2 Satz 2 Bundesverfassungsschutz-gesetz des bisherigen Rechts.

Zu Absatz 5

Absatz 5 übernimmt im Wesentlichen die Regelung des bisherigen § 15 Absatz 4 Bundesverfassungsschutzgesetz. Auch die Versagung einer „Negativauskunft“ kann ohne Begründung erfolgen und nur einem pauschalisierenden Verweis auf die Rechtsgrundlage für das Weglassen einer Begründung erfolgen.

Als Konsequenz der Zuständigkeit des Unabhängigen Kontrollrates für die Auftragsdatenverarbeitung des Bundesnachrichtendienstes, darf sich der Betroffene bei der Ablehnung der Auskunftserteilung an den Unabhängigen Kontrollrat wenden. Dieser verfügt im Wesentlichen über die gleichen Rechte wie zuvor die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit mit dem Unterschied, dass dem Unabhängigen Kontrollrat aufgrund seiner besonderen Natur nicht entgegengehalten werden kann, dass im Einzelfall die Sicherheit des Bundes oder eines Landes einer Auskunft an den Unabhängigen Kontrollrat entgegensteht. Die Rechte der betroffenen Personen auf Auskunft werden somit durch die Zuständigkeitsänderung nicht eingeschränkt, sondern allenfalls gestärkt. § 13 Absatz 4 des UKRat-Gesetzes findet entsprechend Anwendung (Satz 4). Die Auskunft darf nicht dazu führen, dass operativ eingesetzte Personen möglicherweise enttarnt werden können.

Zu Absatz 6

In Absatz 6 wird klargestellt, dass dem Betroffenen kein Anspruch auf Akteneinsicht zusteht. Dies entspricht der verwaltungsgerichtlichen Spruchpraxis (BVerwG, NJW 2008, 1398 (1399)).

Zu § 103 (Rechtswegausschluss)

Die Regelung übernimmt den bisherigen § 13 Artikel 10-Gesetz.

Zu Abschnitt 8 (Besondere Bestimmungen zur Sicherung der Bediensteten, Dienststellen und Verschlusssachen)

Der Abschnitt enthält besondere Bestimmungen, die zum Schutz der Bediensteten, Dienststellen und Verschlusssachen des Bundesnachrichtendienstes erforderlich sind. Unberührt bleiben die dem Bundesnachrichtendienst ohnehin weiterhin zustehenden „Jedermann-Rechte“, insbesondere das öffentlich-rechtliche und zivilrechtliche Hausrecht sowie Notwehr- und Festnahmerechte nach strafrechtlichen, strafprozessualen und zivilrechtlichen Maßgaben.

Die Befugnisse des Bundesnachrichtendienstes zur Sicherung von Verschlusssachen (nunmehr in Unterabschnitt 3 enthalten) entsprechen weitgehend den Regelungen im bisherigen Abschnitt 6 (§§ 65a bis 65l).

Hinzugekommen sind besondere Befugnisse des Bundesnachrichtendienstes, seine Bediensteten und Dienststellen vor den Einwirkungen von Dritten zu schützen (Unterabschnitt 2). Die Notwendigkeit solcher Bestimmungen ergibt sich aus der sich verschärfenden Bedrohungslage, bei der die Nachrichtendienste des Bundes im Allgemeinen und der Bundesnachrichtendienst im Speziellen zunehmend ins Blickfeld fremder Mächte geraten. Der Bundesnachrichtendienst soll mit den Befugnissen dieses Abschnitts befähigt werden, die Sicherheit seiner Bediensteten und Dienststellen selbstständig gewährleisten zu können. Der „behördliche Eigenschutz“ ist dabei als Funktionssicherung in der eigentlichen Aufgabe des Bundesnachrichtendienstes der Natur der Sache nach eingeschlossen (ebenso wie z. B. die Personalgewinnung). Hierzu zählen insbesondere die räumliche Sicherung der Dienststellen (in der in diesem Gesetz verwandten inhaltlichen Definition) gegen unbefugten Zugang, Ausspähung und Sabotagehandlungen sowie die vorbeugende Personenüberprüfung anlässlich der Zutrittskontrolle oder der Kontrolle der Berechtigung zum Aufenthalt auch innerhalb der Einrichtungen.

Die Befugnisse zum Schutz der Bediensteten, Dienststellen und Verschlusssachen erstrecken sich auch auf die unmittelbare Umgebung der Dienststellen und Einrichtungen.

Nach alledem werden dem Bundesnachrichtendienst also spezifische Exekutivbefugnisse eingeräumt. Diese Befugnisse sind dem Bundesnachrichtendienst indes nicht zu dem Zweck zugewiesen, hierdurch nachrichtendienstliche Informationen zu erheben; sie stehen explizit nicht im direkten Zusammenhang zur nachrichtendienstlichen Auslandsaufklärung, dem eigentlichen Auftrag des Bundesnachrichtendienstes. Noch weniger begründen sie eine Befugnis, etwaige Zwangsmaßnahmen proaktiv „um ihrer selbst willen“ anzuwenden, etwa um gefahrenabwehrrechtliche Maßnahmen im polizeirechtlichen Sinne zu planen und zu ergreifen. Vielmehr ist der Befugniskreis des Bundesnachrichtendienstes im Rahmen dieses Abschnitts darauf beschränkt, der für seine Auftragserfüllung immanenten Pflicht, für seine eigene Sicherheit Sorge zu tragen, zu entsprechen. Insoweit ähneln die Vorschriften den bislang in Abschnitt 6 geregelten Exekutivbefugnissen bei der Durchführung von Maßnahmen zur Sicherung von Verschlusssachen. Dabei gehen die Befugnisse zum Schutz seiner Bediensteten und Dienststellen indes teilweise weiter: So richten sie sich (anders als im bisherigen Abschnitt 6) vornehmlich gegen Dritte, die in keinem näheren Bezug zum Bundesnachrichtendienst stehen.

Diese neuen Befugnisse berühren das sog. „Trennungsgebot“ (oder gleichsam einem „Aufgliederungsgebot“, vgl. BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 113) zwischen polizeilicher und nachrichtendienstlicher Tätigkeit ebenso wenig wie – da keine Erhebung personenbezogener Daten Ausgangspunkt der Tätigkeit des Bundesnachrichtendienstes ist – ein „informationelles Trennungsprinzip“ als Synonym oder Unterfall des Grundsatzes der hypothetischen Datenneuerhebung (vgl. BVerfG, Beschluss vom 10. November 2020, 1 BvR 3214/15). Diesem Prinzip wohnt der Gedanke inne, dass eine Überlappung polizeilicher und nachrichtendienstlicher Befugnisse grundsätzlich unzulässig ist, um der jeweils unterschiedlichen Ausgestaltung der Erhebungsmöglichkeiten von personenbezogenen Daten Rechnung zu tragen. Insbesondere soll der Bundesnachrichtendienst, der im Vergleich zur Polizei bereits weit im Vorfeld Daten erheben darf, hinsichtlich der Nutzung der erlangten Daten engeren Grenzen unterliegen. Dies bildet im Übrigen auch die verfassungsrechtliche Grundlage für die ausdifferenzierte Systematik der Übermittlungsregelungen: Die Erleichterungen des Bundesnachrichtendienstes auf Seiten der Informationserhebung bedingen, dass eine Übermittlung an Behörden mit „operativen Anschlussbefugnissen“, insbesondere Strafverfolgungs- und Gefahrenabwehrbehörden, nur unter engen Voraussetzungen möglich ist. Die Grenzen der Befugnisse des Bundesnachrichtendienstes zur Sammlung und Auswertung von Informationen dürfen nicht dadurch unterlaufen werden, dass erhobene Daten anlass- und schwellenlos an Polizeibehörden übermittelt werden. Anders liegt der Fall hier. Die Befugnisse zur Sicherung von Bediensteten und Dienststellen stehen im engen räumlichen Zusammenhang mit den Dienststellen des Bundesnachrichtendienstes und sind auf diesen engen räumlichen Zusammenhang gleichermaßen beschränkt (vgl. hierzu auch Manns in GSZ 2025, 30, S. 31 f.). Von dem grundsätzlich bestehenden Erfordernis eines engen räumlichen Zusammenhangs wird lediglich in Fällen abgesehen, in denen ein enger funktionaler Zusammenhang besteht: So kann der Bundesnachrichtendienst künftig in eng begrenzten Ausnahmefällen zur Sicherung seiner Auftragserfüllung auch außerhalb seiner Dienststellen sogenannte „vorübergehende besondere Sicherheitsbereiche“ einrichten, in denen die Anwendung der in Abschnitt 8 genannten Befugnisse ebenfalls zulässig ist. Den Befugnissen liegt gerade nicht die Erhebung von Informationen für die nachrichtendienstliche Auslandsaufklärung zugrunde, sondern ein objektiviertes Verhalten von Dritten, die durch „qualifiziert funktionsgefährdende Tätigkeiten“ den Anlass für die jeweilige Befugnisausübung geben. Darüber hinaus sind die Befugnisse des Bundesnachrichtendienstes in Unterabschnitt 2 darauf gerichtet, lediglich eine kurzfristige Sicherung zu bewirken und sodann das Eintreffen der zuständigen Polizei abzuwarten.

Querschnittlich geregelt in den Unterabschnitten 1, 4 und 5 sind nun die Befugnisse zum Schutz von Bediensteten und Dienststellen einerseits und die Befugnisse zum Schutz von Verschlusssachen andererseits: In Unterabschnitt 1 finden sich die allgemeinen Vorgaben, in Unterabschnitt 4 die Bestimmungen zu der Vollstreckung der besonderen Befugnisse und in Unterabschnitt 5 die besonderen Bestimmungen für den Umgang mit personenbezogenen Daten, die mittels der Befugnisse dieses Abschnitts erhoben wurden.

Die bereits im bisherigen § 65f Absatz 7 Satz 5 aus Gründen des Art. 19 Absatz 1 Satz 2 des Grundgesetzes enthaltene Passage zur Einschränkung des Grundrechts auf körperliche Unversehrtheit (Artikel 2 Absatz 2 Satz 1 des Grundgesetzes) und Freiheit der Person (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes) wurde in § 141 im Abschnitt 11 querschnittlich integriert.

Zu Unterabschnitt 1 (Begriffsbestimmungen und allgemeine Vorgaben)

Unterabschnitt 1 enthält querschnittliche Regelungen zu den Befugnissen zur Sicherung von Bediensteten, Dienststellen und von Verschlusssachen gleichermaßen. Neben den in § 104 enthaltenen Begriffsbestimmungen sind dies insbesondere allgemeine Vorgaben zu den Befugnissen, insbesondere die in § 105 Absatz 1 enthaltene allgemeine Maßgabe, dass bezüglich der Befugnisse der Suspensiveffekt von Widerspruch und Anfechtungsklage ausgeschlossen ist, die Befugnis des Bundesnachrichtendienstes, vorübergehende

besondere Sicherheitsbereiche zu definieren in § 106 und die öffentlichen Hinweispflichten nach § 107, welche für die Rechtfertigung einzelner Zwangsbefugnisse von konstitutiver Bedeutung sind.

Zu § 104 (Begriffsbestimmungen zur Sicherung der Bediensteten, Dienststellen und Verschlusssachen)

Die Vorschrift enthält eine Reihe von Begriffsbestimmungen zur Erleichterung der systematischen Gliederung des Abschnitts.

Zu Nummer 1

In Nummer 1 werden die Dienststellen des Bundesnachrichtendienstes definiert. Da insbesondere die in Unterabschnitt 2 enthaltenen Befugnisse grundsätzlich in ihrem räumlichen Anwendungsbereich auf die Dienststellen oder die unmittelbare Nähe zu diesen Dienststellen begrenzt sind, kommt dieser Definition entscheidende Bedeutung zu.

Nummer 1 definiert den Begriff der Dienststelle dabei als Grundstücke, Gebäude, Gebäudeteile, Anlagen und Einrichtungen des Bundesnachrichtendienstes, womit ausdrücklich eine allumfassende Geltung für die „Räumlichkeiten“ (im weitesten Sinne) des Bundesnachrichtendienstes bezweckt ist. Insbesondere kommt es nicht auf eine zivilrechtliche Betrachtung an, eine Eigentümerstellung des Bundesnachrichtendienstes ist etwa unbeachtlich, Mietobjekte sind erfasst. Vielmehr ist die tatsächliche Herrschaft – etwa durch ein Hausrecht indiziert – entscheidend. Darüber hinaus werden die nach § 107 Absatz 2 vorübergehend zu besonderen Sicherheitsbereichen erklärten Örtlichkeiten von dem Begriff der „Dienststellen des Bundesnachrichtendienstes“ mit umfasst.

Zu Nummer 2

Zu Buchstabe a

Buchstabe a ist in Grundzügen an § 3 Absatz 1 Nummer 1 Buchstabe a des Gesetzes über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und verbündeter Streitkräfte sowie zivile Wachpersonen (nachfolgend mangels Kurzbezeichnung: UZwGBw) angelehnt. Dieses Gesetz regelt die – von einer ähnlichen Systematik und Regelungstechnik geprägte – Materie von Exekutivbefugnissen für Angehörige der Bundeswehr zum Eigenschutz. Wie dort kommt es nicht darauf an, welcher Statusgruppe die Angehörigen des Bundesnachrichtendienstes zuzuordnen sind. Von der Regelung erfasst sind somit alle Mitarbeitenden des Bundesnachrichtendienstes (Beamte, Tarifbeschäftigte und Soldaten). Die Formulierung „mit Strafe bedrohte Handlungen“ im Sinne der Regelung umfasst beispielsweise tätliche Angriffe oder sonstige Übergriffe, die sich gegen Bedienstete des Bundesnachrichtendienstes richten. Die objektive Geeignetheit eines mit Strafe bedrohten Handelns, das die Störung der Ausübung des Dienstes zur Folge hat, indiziert das Vorliegen einer gezielten Störung im Sinne des Buchstabe a.

Zu Buchstabe b

Die Regelung in Buchstabe b wird – wie in Buchstabe a – an das UZwGBw angelehnt (dort auf § 3 Absatz 1 Nummer 2) und bezieht neben Straftaten gegen Bedienstete auch Straftaten gegen Dienststellen und Sachgüter des Bundesnachrichtendienstes in die Definition von qualifiziert funktionsgefährdenden Tätigkeiten ein.

Zu Buchstabe c

Die in Buchstabe c in Bezug genommenen Straftaten entsprechen denen des bisherigen § 65d Absatz 2, die nunmehr aus Gründen der Übersichtlichkeit aus dem Gesetzeswortlaut entfernt wurden. Es handelt sich hierbei um Straftaten, die eine besondere Auswirkung auf

die Sicherheit der Bediensteten, Dienststellen und Verschlusssachen des Bundesnachrichtendienstes haben bzw. von denen eine besondere Bedrohung ausgeht. Hierunter fallen insbesondere Straftaten des Friedensverrats oder des Hochverrats (§§ 80a bis 83 des Strafgesetzbuches), Straftaten der Gefährdung des demokratischen Rechtsstaates (§§ 86 bis 89c, 91 des Strafgesetzbuches), Straftaten des Landesverrats und der Gefährdung der äußeren Sicherheit sowie Straftaten gegen ausländische Staaten (§§ 94 bis 100, 102 des Strafgesetzbuches),Straftaten gegen die Landesverteidigung (§§ 109e bis 109g des Strafgesetzbuches), Straftaten gegen die öffentliche Ordnung (§§ 126a, 133 des Strafgesetzbuches), Straftaten nach den §§ 202a bis 202c und 303a bis 303b des Strafgesetzbuches, soweit diese die Sicherheit von Verschlusssachen beeinträchtigen, und Straftaten nach § 353b des Strafgesetzbuches;

Zu Buchstabe d

Der unzulässige Einsatz von unbemannten Fluggeräten in der Nähe der Liegenschaften des Bundesnachrichtendienstes stellt eine qualifiziert funktionsgefährdende Tätigkeit dar. Grundlage für die Feststellung der qualifiziert funktionsgefährdenden Tätigkeit ist der unzulässige Betrieb eines unbemannten Fluggerätes über und innerhalb eines seitlichen Abstands von 100 Metern von Liegenschaften des Bundesnachrichtendienstes nach § 21h Absatz 3 Nummer 4 der Luftverkehrs-Ordnung.

Die Möglichkeit der Abwehr von unbemannten Fluggeräten ist von stetig wachsender Bedeutung für die Funktionsfähigkeit und Sicherheit des Bundesnachrichtendienstes. Die bisherige Befugnis des § 2 Absatz 1b geht hier bzw. in der Befugnis zur Drohnenabwehr (§ 112) auf. Die Befugnis zur Drohnenabwehr nach § 113 geht zudem partiell über den in Buchstabe d geregelten Bereich hinaus. Der Anwendungsbereich des § 113 Absatz 2 ist bewusst weiter gefasst und umfasst über die Liegenschaften (Nummer 2 Buchstabe d) hinaus auch die Drohnenabwehr in vorübergehenden besonderen Sicherheitsbereichen sowie den Bereich im Umkreis von 100 Metern zu den vom Bundesnachrichtendienst eingesetzten Personen.

Vor dem Hintergrund der fortschreitenden technischen Entwicklung von Aufklärungstechnik (insb. in Bezug auf Audio- und Videoaufzeichnungen) sind Drohnen bereits gegenwärtig in der Lage – und zukünftig in noch stärkerem Maße – aus größerer Entfernung die Dienststellen des Bundesnachrichtendienstes aufzuklären sowie zu stören. Lediglich klarstellend ist zu erwähnen, dass auch dann eine „Gefahr für die öffentliche Sicherheit und Ordnung“ im polizeirechtlichen Sinne vorliegt, die die Dienststellen, Bediensteten und Verschlusssachen des Bundesnachrichtendienstes betrifft, wenn die Drohne in einer Entfernung betrieben wird, die den in § 21h Absatz 3 Nummer 4 der Luftverkehrs-Ordnung normierten Abstand überschreitet. Insofern kann der Bundesnachrichtendienst zur Drohnenabwehr im Rahmen der allgemeinen Vorgaben zur Amtshilfe insbesondere für die Polizeibehörden des Bundes und der Länder sowie die Streitkräfte unterstützend tätig werden.

Zu Nummer 3

Nummer 3 enthält die vormals in § 65f Absatz 2 enthaltene Begriffsbestimmung einer „Kontrolle“ durch den Bundesnachrichtendienst.

Zu Nummer 4

Nummer 4 enthält die vormals in § 65f Absatz 3 enthaltene Begriffsbestimmung einer „Durchsuchung“ durch den Bundesnachrichtendienst.

Zu Nummer 5

Nummer 5 enthält die vormals in § 65a Absatz 1 enthaltene Bestimmung, dass eine „Sicherung von Verschlusssachen“ auf das Erkennen und Verhindern des unbefugten Einbringens und Ausbringens bestimmter Gegenstände (vgl. im Einzelnen den Normtext) gerichtet ist.

Zu Nummer 6

Die Definition des „unmittelbaren Zwangs“ entspricht weitgehend der in § 65f Absatz 7 Satz 1. Die dort enthaltenen Bestimmungen zur „Fesselung“ von Personen sind dabei systematisch neu verortet worden. Darüber hinaus wurde der Einsatz von „Waffen“ aufgenommen, um einen Gleichlauf der Begriffsbestimmungen mit dem Gesetz über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes herzustellen. Zum Schutz von Bediensteten, Dienststellen und Verschlusssachen kann als Ultima Ratio auch der Einsatz von Schusswaffen im Einzelfall notwendig sein.

Zudem wurde die Definition um den Einsatz geeigneter Mittel gegen unbemannte Fluggeräte, deren Steuerungseinheiten oder Steuerungsverbindungen erweitert, um den Besonderheiten der Drohnenabwehr Rechnung zu tragen. Die Definition ist bewusst breit gewählt, sodass insbesondere auch waffengleiche Mittel hierunter fallen, die dem besonderen Schutz vor unbemannten Fluggeräten dienen (z.B. Schrotflinten mit und ohne Spezialmunition).

Zu § 105 (Allgemeine Vorgaben)

§ 105 enthält allgemeine Vorgaben zu den Befugnissen dieses Abschnitts.

Zu Absatz 1

In Absatz 1 ist geregelt, dass Widerspruch und Anfechtungsklage gegen die in den Unterabschnitten 2 und 3 enthaltenen Befugnisse – bei denen es sich regelmäßig um Verwaltungsakte handeln wird – keine aufschiebende Wirkung haben. Im regulären Verfahren sind diese Verwaltungsakte also sofort vollziehbar. Dies entspricht dem bisherigen § 65e Absatz 3, der nunmehr allgemein Anwendung findet.

Ein vorheriger Verwaltungsakt kann im Einzelfall entbehrlich sein (vgl. § 121 Absatz 1 Satz 2 in Verbindung mit § 6 Absatz 2 des Verwaltungs-Vollstreckungsgesetzes), wenn der sofortige Vollzug zur Verhinderung einer rechtswidrigen Tat, die einen Straf- oder Bußgeldtatbestand verwirklicht, oder zur Abwendung einer drohenden Gefahr notwendig ist und die Behörde hierbei innerhalb ihrer gesetzlichen Befugnisse handelt. Im Rahmen des nachgelagerten Vollstreckungsverfahrens findet im Grundsatz – der allgemeinen Verwaltungspraxis entsprechend – zunächst ein zweistufiges Verfahren Anwendung, bei dem zunächst eine Androhung einer Maßnahme erforderlich ist (§ 121 Absatz 3). Dies gilt wiederum dann nicht, wenn der sofortige Vollzug der Maßnahme erforderlich ist, um eine qualifiziert funktionsgefährdende Tätigkeit oder Überflüge von Drohnen, zu deren Abwehr der Bundesnachrichtendienst nach § 113 befugt ist, zu verhindern.

Zu Absatz 2

Der Schutz der Bediensteten, Dienststellen und Verschlusssachen des Bundesnachrichtendienstes (auch soweit dies Teil der Eigensicherung im Rahmen der allgemeinen Auftragserfüllung ist) insbesondere durch technische Einrichtungen dient der Sicherung der Behörde gegen Angriffe auf ihre Funktionsfähigkeit. Allerdings würde eine Mitbestimmung der Personalvertretung beim Einsatz von Maßnahmen der Eigensicherung die Wirksamkeit dieser Eigensicherungsmaßnahmen gefährden. Denn es würde ein größerer Personenkreis von den konkreten Maßnahmen Kenntnis erlangen. Daher werden mit der vorliegenden Regelung Ausnahmen von den Regelungen zur Mitbestimmung in § 80 Absatz 1 Nummer 18 und Nummer 21 Bundespersonalvertretungsgesetz vorgesehen. Damit entfällt bei Maßnahmen der Eigensicherung die Mitbestimmung des Personalrats bei Regelungen der Ordnung in der Dienststelle und des Verhaltens der Beschäftigten (Nummer 18) und Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen (Nummer 21).

Da sich der Zweck dieser Vorschrift am Ziel der wirksamen Eigensicherung ausrichtet, dürfen die nach § 106 Absatz 2 der Mitbestimmung entzogenen Maßnahmen ausschließlich für die hier genannten Zwecke und nicht zur Ordnung allgemeiner Arbeitsverhältnisse (etwa zur Leistungskontrolle) angewendet werden. Zudem muss der Bundesnachrichtendienst auch in diesen Fällen im vertrauensvollen Zusammenwirken mit der Personalvertretung die Belange der Bediensteten sachgerecht berücksichtigen. Angesichts der besonderen Gefährdung des Bundesnachrichtendienstes besteht insoweit allerdings ein genereller Vorrang des Schutzes des Bundesnachrichtendienstes gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten von Innentätern. Mit Blick auf das Ziel, die Funktionsfähigkeit der Behörde zu gewährleisten, überwiegen hier die Aspekte des Gemeinwohls.

Auch eine nähere gesetzliche Eingrenzung der von der Mitbestimmung ausgenommenen Eigensicherungsmaßnahmen bietet sich mit Blick auf das Ziel der Funktionssicherung nicht an. Die nähere Ausgestaltung von Eigensicherungsmaßnahmen muss flexibel bleiben, um an die jeweiligen örtlichen, technischen und situativen Anforderungen angepasst werden zu können. Der Behörde muss also ein Gestaltungsspielraum verbleiben.

Zu § 106 (Besondere Sicherheitsbereiche)

Zu Absatz 1

In Absatz 1 wird dem Bundesnachrichtendienst die Befugnis eingeräumt, „vorübergehende besondere Sicherheitsbereiche“ zu errichten, um ausnahmsweise auch außerhalb seiner Liegenschaften die gesondert geregelten Maßnahmen der Eigensicherung mit Zustimmung des Bundeskanzleramtes durchführen zu können.

Auf materiell-rechtlicher Seite ist die Errichtung eines vorübergehenden besonderen Sicherheitsbereiches nur zulässig, wenn die Errichtung aus Gründen der Sicherheit zur Erfüllung dienstlicher Aufgaben des Bundesnachrichtendienstes unerlässlich ist. Das Gesetz sieht hier eine hohe Hürde vor. Eine Unerlässlichkeit aus Gründen der Sicherheit wird etwa anzunehmen sein, wenn vor dem Hintergrund der aktuellen Lageeinschätzung des Bundesnachrichtendienst eine hohe Wahrscheinlichkeit dafür vorliegt, dass ein Treffen mit hochrangigen Vertretern fremder Staaten durch feindliche Mächte ausgespäht oder angegriffen werden könnte. Denkbar wäre ferner der Test einer technischen Vorrichtung, welcher außerhalb der Liegenschaften stattfinden muss, wenn zugleich Anhaltspunkte dafür bestehen, dass der Test ausgespäht oder gestört werden könnte.

Die Einrichtung eines vorübergehenden besonderen Sicherheitsbereiches wird in aller Regel – d.h. wenn nicht insbesondere Gründe der Geheimhaltung hiergegen sprechen – der zuständigen Polizeibehörde anzuzeigen sein.

Zu Absatz 2

Absatz 2 regelt die durch die Errichtung eines vorübergehenden besonderen Sicherheitsbereiches möglicherweise erforderliche Entschädigung durch Verweis auf § 20 Absatz 2 des Gesetzes über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und verbündeter Streitkräfte sowie zivile Wachpersonen.

Zu § 107 (Öffentliche Hinweispflichten)

Die Norm trifft Vorgaben für die Hinweispflichten durch Beschilderung bzgl. der besonderen Befugnisse dieses Abschnitts.

Wie bereits ausgeführt bedürfen diese Befugnisse, welche dem Bundesnachrichtendienst künftig die Möglichkeit einräumen, nötigenfalls auch unmittelbaren Zwang außerhalb seiner Dienststellen anzuwenden, besonderer Rechtfertigungselemente. Das sind neben einer geringen Anwendungsbreite und – für besondere Sicherheitsbereiche – einer besonderen

Berücksichtigung von Interessen der Allgemeinheit insbesondere die hier geregelten Hinweispflichten. Diese Pflichten sorgen dafür, dass etwaige Dritte, welche sich in unmittelbarer Nähe zu Dienststellen des Bundesnachrichtendienstes aufhalten, über die sie treffenden Sonderpflichten informiert werden.

Die Norm regelt die öffentlichen Hinweispflichten des Bundesnachrichtendienstes vor seinen offen als solche erkennbaren Dienststellen. Da nicht alle Dienststellen des Bundesnachrichtendienstes offen als solche erkennbar sind, gilt die Hinweispflicht in diesen Fällen nicht. Dies dient dem Schutz legendierter oder anderweitig vertarnter Dienststellen des Bundesnachrichtendienstes.

Zu Unterabschnitt 2 (Befugnisse zur Sicherung der Bediensteten und Dienststellen)

In Unterabschnitt 2 finden sich die (besonderen) Befugnisse, welche dem Bundesnachrichtendienst zur Sicherung seiner Bediensteten und Dienststellen (in Abgrenzung zur Sicherung seiner Verschlusssachen) zustehen. Es handelt sich hierbei um solche Befugnisse, welche nötigenfalls und nach Maßgabe des Unterabschnitts 4 auch mit Zwangsmitteln durchgesetzt werden können.

Zu § 108 (Betroffene Personen)

In der Vorschrift wird der Personenkreis geregelt, gegen den der Bundesnachrichtendienst seine Befugnisse ausüben darf. Maßgebliches Anknüpfungskriterium ist dabei grundsätzlich die räumliche Verortung der betroffenen Person. In Ausnahmekonstellationen genügt jedoch auch ein funktionaler Zusammenhang zum Bundesnachrichtendienst, der etwa die Ausübung der Tätigkeit, die Bediensteten, Dienststellen oder auch Gegenstände des Bundesnachrichtendienstes betreffen kann. Ein funktionaler Zusammenhang liegt insbesondere dann vor, wenn eine betroffene Person eine „qualifiziert funktionsgefährdende Tätigkeit“ gegen den Bundesnachrichtendienst plant.

Zu Nummer 1

In Bezug auf die Bediensteten und Dienststellen des Bundesnachrichtendienstes besteht ein besonderes Sicherheitsbedürfnis. Um sicherzustellen, dass sich Unbefugte keinen unrechtmäßigen Zugang zu den Dienststellen verschaffen, sind umfangreiche Sicherheitsvorkehrungen notwendig. Befindet sich die Person innerhalb der Dienststellen des Bundesnachrichtendienstes, ist folglich mit einem besonderen Pflichtenkreis zu rechnen. Besondere, eine gesteigerte Gefährdungslage begründende Tatbestandsvoraussetzungen sind insoweit nicht erforderlich.

Zu Nummer 2

Bei den in Nummer 2 abgebildeten Fallgestaltungen befindet sich die betroffene Person noch nicht innerhalb der Dienststellen des Bundesnachrichtendienstes. Indes tritt als besonderes, qualifizierendes und rechtfertigendes Merkmal hinzu, dass die betroffene Person die Dienststellen betreten will. In diesem Fall ist schon aus sicherheitlichen Erwägungen erforderlich, dass der Bundesnachrichtendienst besondere Befugnisse gegenüber diesem Personenkreis ausüben kann. Überdies muss den betroffenen Personen auch klar sein, dass sie sich mit dem Versuch, eine besonders gesicherte Dienststelle zu betreten, möglicherweise besonderen hoheitlichen Befugnissen aussetzt.

Zu Nummer 3

Der in Nummer 3 genannte Personenkreis knüpft unmittelbar an die Nummern 1 und 2 an und erstreckt die besonderen Befugnisse dieses Unterabschnittes auch auf solche Personen, welche die Dienststellen des Bundesnachrichtendienst zeitlich unmittelbar verlassen haben (1. Alternative) oder diese betreten wollten und daran gehindert wurden (2. Alternative). In beiden Fällen tritt als ergänzendes und verdachtsbegründendes Merkmal hinzu,

dass tatsächliche Anhaltspunkte dafür bestehen, dass die betroffene Person nicht berechtigt ist, sich in den Dienststellen des Bundesnachrichtendienst aufzuhalten.

Erfasst sind hiervon etwa solche Fälle, in denen ein Unbekannter versucht, sich Zutritt zu den Dienststellen des Bundesnachrichtendienstes zu verschaffen, und bei Ansprache die Flucht ergreift. Ebenso fallen hierunter Fälle, in denen sich eine Person offensichtlich widerrechtlich (etwa durch das Überklettern eines Zauns) Zutritt zu den Dienststellen des Bundesnachrichtendienstes verschafft und sofort die Flucht ergreift, weil er vom Wachpersonal gesehen wurde.

Zu Nummer 4

In Nummer 4 ist eine Erweiterung des Anwendungsbereiches der in diesem Unterabschnitt geregelten Befugnisnormen enthalten: Auch die unmittelbare Nähe ist ausnahmsweise hinreichend, um eine Person in den Betroffenenkreis einzubeziehen, sofern ein funktionaler Zusammenhang besteht. Dies ist dann der Fall, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Person eine qualifiziert funktionsgefährdende Tätigkeit nach § 104 Nummer 2 „plant, begeht oder begangen hat“.

In diesem Fall besteht eine verdichtete Verdachtslage, welche ausnahmsweise auch ein Einwirken des Wachpersonals auf Personen erforderlich macht, welche sich „nur“ in unmittelbarer Nähe zu Dienststellen des Bundesnachrichtendienstes aufhalten.

Der Begriff der „unmittelbaren Nähe“ entspricht jenem in § 23 Absatz 1 Nummer 4 des Bundespolizeigesetzes. Von einem Aufenthalt in unmittelbarer Nähe ist demnach auszugehen, wenn die Person von ihrem Standort aus direkt Straftaten an der Dienststelle des Bundesnachrichtendienstes bzw. in Bezug auf die in oder an dieser Dienststelle befindlichen Personen vornehmen kann oder es ihr jedenfalls möglich ist, die Dienststelle in kürzester Zeit zu erreichen (vgl. Schenke, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2018, BPolG § 23 Rn. 17, m.w.N.).

Insbesondere wäre ein Zuwarten auf die örtliche Polizeibehörde insoweit nicht tunlich, da die Ausführung der qualifiziert funktionsgefährdenden Tätigkeit hier gerade schon droht (also verhindert werden muss), begonnen hat (also gestoppt werden muss) oder begangen wurde (also aufgeklärt werden muss). Der zeitliche Verzug, der von einem Zuwarten bis zum Eintreffen der Polizeikräfte ausgehen würde, ist insoweit nicht zu rechtfertigen.

Zu § 109 (Personenüberprüfung)

Zu Absatz 1

Der Bundesnachrichtendienst darf die Identität einer Person nach § 108 feststellen. Die Vorschrift entspricht insoweit inhaltlich den in § 23 des Bundespolizeigesetzes oder in § 42 des Bundeskriminalamtsgesetzes geregelten Vorschriften zur Identitätsfeststellung.

Anders als in den Polizeigesetzen geregelt ist dabei jedoch keine allgemeine gefahrenabwehrrechtliche Befugnis zur Identitätsfeststellung verbunden, sondern nur eine Überprüfung eines eng begrenzten Personenkreis möglich, bei dem entweder ein räumlicher oder funktionaler Zusammenhang zum Bundesnachrichtendienst tatbestandlich gemäß § 109 vorausgesetzt wird.

Zu Absatz 2

Der Bundesnachrichtendienst kann zur Ausübung der Befugnis des Absatz 1 die erforderlichen Maßnahmen treffen, die betroffene Person insbesondere anhalten, sie nach ihren Personalien befragen und verlangen, dass sie Ausweispapiere zur Prüfung aushändigt. Die Vorschrift ist § 23 Absatz 3 Satz 1 und 2 des Bundespolizeigesetzes nachempfunden und – wie auch die Vorschrift des Bundespolizeigesetzes – nicht abschließend.

Die Befugnis schließt die Verpflichtung der betroffenen Person ein, am Ort der Überprüfung solange zu verweilen, bis die Identitätsfeststellung abgeschlossen ist. Eine Person kann grundsätzlich auch befragt werden, allerdings nur insoweit, als dies für die Überprüfung der Identität notwendig ist. Ausweispapiere sind alle geeigneten amtlichen Lichtbilddokumente (insbesondere aber nicht ausschließlich Personalausweise und Reisepässe); diese müssen ausgehändigt werden.

Zu Absatz 3

Die in Absatz 3 enthaltene Befugnis, eine betroffene Person nötigenfalls zu einer hierfür durch die Behördenleitung des Bundesnachrichtendienstes bestimmten Person zu bringen, soll sicherstellen, dass auch in Ausnahmesituationen eine Überprüfung möglich bleibt. Eine solche Situation liegt etwa vor, wenn die unmittelbare Überprüfung durch das Wachpersonal aus faktischen Gründen erschwert oder unmöglich ist (etwa bei tumultartigen Menschenaufläufen), wenn aufgrund der Verweigerung einer Mitwirkung eine Überprüfung nicht stattfinden kann oder wenn der Verdacht besteht, dass die Ausweispapiere gefälscht sind.

Die Befugnis beinhaltet das Recht, die betroffene Person „festzuhalten“, womit gemeint ist, dass der Betroffene „über die üblicherweise zur Durchführung einer Identitätsfeststellung benötigten Zeit hinaus gehindert wird, den Ort der Identitätsfeststellung zu verlassen“ (Schenke in Schenke/Graulich/Ruthig, 2. Aufl. 2018, BPolG § 23 Rn. 41). Die von der Behördenleitung des Bundesnachrichtendienstes bestimmte Person ist dabei in der Regel ein besonders geschulter Mitarbeiter, welcher insbesondere vertiefte Rechtskenntnis aufweist. Eine Befähigung zum Richteramt ist insoweit indes nicht Voraussetzung. Es können auch mehrere Personen von der Behördenleitung hierzu bestimmt werden, um die zeitliche und örtliche Verfügbarkeit zu gewährleisten.

Um sicherzustellen, dass die Person nicht länger als unbedingt nötig festgehalten wird, muss sie nach Satz 2 sofort überprüft werden. Liegen die Voraussetzungen des Satzes 1 vor, können die betroffene Person sowie die von ihr mitgeführten Sachen nach Gegenständen durchsucht werden, die der Identitätsfeststellung dienen. Sobald die Identität einer Person durch die Durchsuchung bestimmt ist, muss die Durchsuchung abgebrochen werden, es sei denn, es liegen die Voraussetzungen für eine weitere Durchsuchung vor.

Zu § 110 (Durchsuchung, Sicherstellung und Beschlagnahme)

Zu Absatz 1

Der Bundesnachrichtendienst ist nach § 110 Absatz 1 befugt, eine der in § 108 genannten betroffenen Personen zu durchsuchen. Dies setzt voraus, dass tatsächliche Anhaltspunkte dafür bestehen, dass die betroffene Person eine qualifiziert funktionsgefährdende Tätigkeit plant begeht oder begangen hat (Nummer 1; dies entspricht insoweit auch den Voraussetzungen dafür, dass eine Person in unmittelbarer Nähe zu einer Dienststelle des Bundesnachrichtendienstes überhaupt zu dem Kreis der betroffenen Personen zählen kann, vgl. § 108 Nummer 4) und dass die Durchsuchung zur Auffindung von Gegenständen führt, die durch eine qualifiziert funktionsgefährdende Tätigkeit hervorgebracht wurden oder zur Begehung einer solchen Handlung geeignet sind oder als Beweismittel für die Untersuchung von Bedeutung sein können (Nummer 2).

Die Voraussetzung der Nummer 2 sorgt dabei insbesondere dafür, dass eine Durchsuchung keineswegs bei jeder der betroffenen Personen des § 108 (sowie aufgrund der tatbestandlichen Überschneidung insbesondere des § 108 Nummer 4) in Betracht kommt. Vielmehr ist erforderlich, dass ein konkreter Zusammenhang zwischen der qualifiziert funktionsgefährdenden Tätigkeit und dem Ziel der Durchsuchung besteht.

Zu Absatz 2

Die Vorschrift entspricht dem § 7 Absatz 2 des Gesetzes über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und zivile Wachpersonen. Wegen der Behandlung amtlicher Schriftstücke und beschlagnahmefreier Gegenstände wird ebenfalls auf die Vorschriften der §§ 96, 97 und 110 der Strafprozessordnung verwiesen, die unmittelbar anzuwenden sind.

Zu Absatz 3

Die Vorschrift entspricht dem § 7 Absatz 3 des Gesetzes über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und zivile Wachpersonen. In Satz 3 und Satz 4 erfolgt eine Anpassung dahingehend, dass bei Gegenständen, welche der Verfügungsgewalt des Bundesnachrichtendienstes unterfallen, eine Weitergabe an die Polizei ausnahmsweise ausgeschlossen ist. Dies ist schon aus Geheimhaltungsgründen unverzichtbar. In diesem Fall ist nach Satz 4 der Polizei oder der Staatsanwaltschaft für ihre Ermittlungen ein Verzeichnis der (nicht weitergegebenen) Gegenstände zu übersenden. Hierbei ist Geheimhaltungsbedürfnissen ebenfalls Rechnung zu tragen.

Zu § 111 (Erweiterte Befugnisse bei qualifiziert funktionsgefährdenden Tätigkeiten)

Zu Absatz 1

Der Bundesnachrichtendienst darf eine Person, die sich in einer Dienststelle des Bundesnachrichtendienstes oder in unmittelbarer Nähe zu einer Dienststelle des Bundesnachrichtendienstes aufhält und bei der tatsächliche Anhaltspunkte dafür bestehen, dass sie eine qualifiziert funktionsgefährdende Tätigkeit plant, begeht oder begangen hat aus der unmittelbaren Nähe zu der Dienststelle verweisen oder ihr (vorübergehend) das Betreten dieses Bereichs verbieten.

Die Vorschrift ist dem § 38 des Bundespolizeigesetzes nachempfunden und soll sicherstellen, dass der Bundesnachrichtendienst eine Handhabe hat, um qualifiziert funktionsgefährdende Tätigkeiten unmittelbar zu unterbinden, ohne auf ein Eintreffen der Polizeibehörde zu warten.

Diese Befugnis ist räumlich (auf die unmittelbare Nähe zu oder innerhalb einer Dienststelle des Bundesnachrichtendienstes) und zeitlich (enger als ein dem Bundesnachrichtendienst nicht zustehendes Aufenthaltsverbot) begrenzt. Sie kann durch unmittelbaren Zwang durchgesetzt werden, was auf ein physisches Entfernen aus dem räumlichen Bereich hinausläuft. Anders als bei Polizeibehörden scheidet eine Verbringung auf die Dienststelle durch Ingewahrsamnahme aus, da dies dem Ziel einer Platzverweisung denknotwendigerweise widersprechen würde.

Zu Absatz 2

Bei Gefahr im Verzug kann der Bundesnachrichtendienst bestimmte Personen, auch vorübergehend bis zum Eintreffen der zuständigen Polizeibehörde festhalten. Voraussetzung ist es dabei, dass das Festhalten der betroffenen Person unerlässlich ist, um die unmittelbar bevorstehende Begehung oder Fortsetzung einer qualifiziert funktionsgefährdenden Tätigkeit durch diese Person zu verhindern (Satz 1 Nummer 1), oder die betroffene Person bei einer qualifiziert funktionsgefährdenden Tätigkeit auf frischer Tat betroffen oder verfolgt wird oder einer qualifiziert funktionsgefährdenden Tätigkeit dringend verdächtig ist (Satz 1 Nummer 2).Die Befugnis dient einzig dazu, die Zwischenzeit bis zum Hinzutreten der zuständigen Polizeibehörde zu überbrücken. Diese ist deshalb unverzüglich über die Maßnahme zu informieren (Satz 2). Die Maßnahme ist zu beenden, sobald eine Überstellung der betroffenen Person an die zuständige Polizeibehörde möglich ist (Satz 3). Zum Schutz der

betroffenen Person finden im Übrigen die §§ 40 bis 42 des Bundespolizeigesetzes entsprechende Anwendung.

Zu § 112 (Maßnahmen gegen den unbefugten Betrieb unbemannter Fluggeräte)

Die Vorschrift enthält die Befugnis des Bundesnachrichtendienstes, Maßnahmen gegen den unbefugten Betrieb unbemannter Fluggeräte zu treffen. Der „unbefugte Betrieb“ knüpft hierbei explizit nicht an § 105 Nummer 2 Buchstabe d an, nach welchem lediglich die Liegenschaften des Bundesnachrichtendienstes im Rahmen einer qualifizierten funktionsgefährdenden Tätigkeit umfasst sind. Vielmehr zielt die Norm zusätzlich auch darauf ab, sowohl die vorübergehend zu besonderen Sicherheitsbereichen erklärten Örtlichkeiten sowie die vom Bundesnachrichtendienst eingesetzten Personen vor der Aufklärung oder Einwirkung durch fremde unbemannte Fluggeräte zu schützen.

Zu Absatz 1

Absatz 1 erlaubt zunächst die Aufklärung der sich im Umfeld von den eingesetzten Personen sowie Dienststellen des Bundesnachrichtendienstes befindlichen unbemannten Fluggeräte. Um einen effektiven Schutz, beispielsweise bei gezielten Angriffen gegen Personen, zu gewährleisten, besteht hier keine konkrete räumliche Beschränkung der Aufklärung. Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass ein unbemanntes Fluggerät für eine qualifiziert funktionsgefährdende Tätigkeit genutzt wird, können auch Maßnahmen nach den §§ 110, 111 und 112 Absatz 2 gegen die Person, die das unbemannte Fluggerät steuert, angewendet werden.

Zu Absatz 2

Nähert sich ein unbemanntes Fluggerät in den Nahbereich von 100 Metern (Nummer 1) zu den vom Bundesnachrichtendienst eingesetzten Personen oder seinen Dienststellen, so darf dieser das Fluggerät mit den erforderlichen Mitteln abwehren. Hiervon umfasst sind sowohl technische, als auch nicht-technische Mittel. Die Notwendigkeit dieser Norm erwächst durch die gesteigerte Bedrohung durch Drohnen, welche durch ihre Geschwindigkeit und ihr Schadenspotenzial im Falle eines Angriffs eine besondere Gefahr für die Funktionsfähigkeit des Bundesnachrichtendienstes darstellen. Der zusätzliche Bezug auf § 21h Absatz 3 Nummer 4 der Luftverkehrs-Ordnung (Nummer 2) bleibt ebenfalls erhalten, da er den Überflug ohne Höhenbegrenzung auf 100 Meter einbezieht. Die Regelungen beziehen sich auf das geografische Gebiet, unabhängig davon, ob womöglich eine in der Vorschrift vorbehaltene Zustimmung der zuständigen Stelle vorliegt. In der gegenwärtigen Situation des Überflugs muss die Befugnis zur wirksamen Abwehr an dem feststellbaren Sachverhalt anknüpfen. Falls – grundsätzlich nicht erwartbar – eine Zustimmung vorliegt, sind etwaige Schäden nach Absatz 4 zu regulieren. In Nummer 3 wird darüber hinausgehend eine Abwehr auch dann ermöglicht, wenn neben die geographische Nähe auch tatsächliche Anhaltspunkte für qualifiziert funktionsgefährdende Tätigkeiten hinzutreten. In diesen Fällen darf nicht nur eine Maßnahme gegen den Pilot erfolgen (Absatz 1), sondern – erst recht – auch eine Abwehr der Drohne.

Zu Absatz 3

Die Vorschrift regelt, dass abgewehrte Fluggeräte durch den Bundesnachrichtendienst sichergestellt und untersucht werden können. Hierdurch wird geregelt, dass die Drohnen, Teile von Drohnen, Steuerungseinheiten, Signalverstärker oder weitere im Zusammenhang mit dem Einsatz von Drohnen stehende Gegenstände den Gefahrenabwehr- und Strafverfolgungsbehörden zumindest nicht unverzüglich überlassen werden müssen, sondern dass der Bundesnachrichtendienst zunächst zur eigenen Auftragserfüllung, d.h. der nachrichtendienstlichen Auslandsaufklärung, also auch zur Eigensicherung und Eigenbefähigung, das unbemannte Fluggerät analysieren kann.

Zu § 113 (Einsatzsicherung)

Zu Absatz 1

Die Regelung schafft eine spezielle ausdrückliche Befugnis für Abwehrmaßnahmen im Rahmen von Sicherungseinsätzen des Bundesnachrichtendienstes, die bislang auf die allgemeine Befugnis zur Nothilfe gestützt wurden. Wenn durch den Bundesnachrichtendienst eingesetzte Personen in besonders gefahrgeneigten Situationen operieren, bedürfen sie einer Absicherung durch im Umfeld verdeckt eingesetzte Sicherungskräfte, die nötigenfalls zur Gefahrenabwehr einschreiten. Dies ist nicht auf die Absicherung von Treffen mit nachrichtendienstlichen Verbindungen beschränkt, sondern kann gleichermaßen Observationseinsätze oder auch die Ansprache von Personen betreffen, die als nachrichtendienstliche Verbindung angeworben werden sollen, aber womöglich aggressiv darauf reagieren könnten. Geschützt werden können auch Einsatzmittel von bedeutendem Wert wie etwa ein zur Observation eingesetztes Personenkraftfahrzeug. Auch die Exfiltration und Evakuierung von Personen, die für den Bundesnachrichtendienst tätig sind, ist von der Befugnis zur Einsatzsicherung umfasst. Beispielsweise fällt darunter die Fallkonstellation, dass eine nachrichtendienstliche Verbindung des Bundesnachrichtendienstes der unmittelbaren Enttarnung und Festnahme bedroht ist und durch eine Maßnahme der Einsatzsicherung exfiltriert werden muss.

Eine solche Einsatzsicherung gilt originär der Eigensicherung im weiteren Sinne, dient also primär der Sicherung der Bediensteten des Bundesnachrichtendienstes und anderen Personen, die mit dem Bundesnachrichtendienst zusammenarbeiten. Es sind aber auch Sachverhalte naheliegend, in denen Nothilfe für Dritte erforderlich werden kann, wenn beispielsweise eine Zielperson observiert wird, die während der Observation einen Angriff gegen Dritte ausführt. Satz 2 erstreckt hierfür die Befugnis zu gefahrenabwehrenden Maßnahmen auch auf solche Nothilfekonstellationen. Hierdurch wird nicht etwa Nothilfe in anderen Situationen ausgeschlossen. Dies betrifft beispielsweise den Personenschutz des Präsidenten des Bundesnachrichtendienstes, wenn dieser – außerhalb eines Einsatzzusammenhangs – angegriffen wird. Auch in diesem Fall sind diese Bediensteten dabei durch Nothilfe gerechtfertigt.

Zu Absatz 2

Der Absatz enthält eine spezielle Befugnis zur Einsatzsicherung, die sich inhaltlich an bestehenden Regelungen orientiert (speziell § 28a BPolG und § 34 BKAG). Die Anordnung liegt – angelehnt an die Vorbildregelungen – bei der Behördenleitung oder einer von ihr bestimmten Vertretung (§ 46 Absatz 1).

Das Aufklärungsfeld des Bundesnachrichtendienstes – u.a. terroristische Akteure sowie Operationen fremder Mächte – ist geprägt von einer starken Abschottung und von einem konspirativen Verhalten des nachrichtendienstlichen Gegenübers, mitunter auch von gewaltsamem Vorgehen. Einsätze erfolgen danach oftmals in einem hoch gefährlichen Umfeld. Erfolgt der Kontakt von Personen, die für den Bundesnachrichtendienst tätig sind, zu aufzuklärenden Personen in Wohnungen erhöht sich die Gefährdung, weil eine verdeckt begleitende Absicherung von der Wahrnehmung des Geschehens ausgeschlossen bleibt, also nicht ohne technische Unterstützung erkennen kann, wenn sich eine Gefahrensituation derart zuspitzt, dass ein rettendes Eingreifen nötig wird.

Die Eigensicherungsmaßnahme dient ausschließlich dem Schutz der für den Bundesnachrichtendienst tätigen Person. Sie soll die Möglichkeit einer umgehenden Reaktion (Rettung) eröffnen. Deshalb unterliegt sie nach Artikel 13 Absatz 5 des Grundgesetzes nicht den engen Voraussetzungen des Artikel 13 Absatz 4 des Grundgesetzes, was sich in den gegenüber § 29 erweiterten Voraussetzungen des § 113 abbildet. Für den Bundesnachrichtendienst tätige Personen sind insbesondere seine Mitarbeiterinnen und Mitarbeiter oder auch nachrichtendienstliche Verbindungen.

Zu Absatz 3

Der Absatz enthält die nach Artikel 13 Absatz 5 des Grundgesetzes gebotenen Weiterverarbeitungsbeschränkungen für die nach Absatz 2 erhobenen personenbezogenen Daten. Ergänzt wird dies mit der in § 124 Absatz 4 enthaltenen Regelung, wonach eine Zweckänderung nur zulässig ist, wenn die unabhängige, quasi-richterliche Vorabkontrolle der Maßnahme (§ 98 Absatz 1 Nummer 10) zuvor erfolgt ist. Da Artikel 13 Absatz 5 des Grundgesetzes ebenso wie Artikel 13 Absatz 4 des Grundgesetzes eine „richterliche“ Entscheidung voraussetzt, wird hier ebenso wie bei der Wohnraumüberwachung die Zuständigkeit des Unabhängigen Kontrollrats vorgesehen.

Aus der Zweckbegrenzung folgt auch, dass Aufzeichnungen, wenn sie für die zulässigen Zwecke nicht mehr erforderlich sind, zu löschen sind. Soweit eine Weiterverarbeitung für zulässige Zwecke erforderlich ist, sind dazu die hierfür geltenden Bestimmungen zu beachten, also z.B. zur Übermittlung für Strafverfolgungszwecke.

Zu § 114 (Anordnung von Maßnahmen zur Sicherung der Bediensteten und Dienststellen)

Die Ausübung der besonderen Befugnisse dieses Unterabschnittes bedürfen regelmäßig einer Anordnung durch die Behördenleitung des Bundesnachrichtendienstes oder durch eine von ihr bestimmte Vertretung. Dies trägt dem Umstand Rechnung, dass es sich bei den hier in Rede stehenden Maßnahmen gerade nicht um „nachrichtendienstliche Standardbefugnisse“ handelt, wie dies etwa bei vergleichbaren polizeilichen Maßnahmen der Fall ist. Insoweit ist das Erfordernis einer Anordnung ein notweniges Korrektiv und ein erster Kontrollmechanismus.

Die Anordnung hat dabei die in den Nummern 1 bis 5 enthaltenen Angaben zu enthalten (Art und Beschreibung der Maßnahme, die betroffenen Personen, Anlass der Maßnahme und Begründung der Maßnahme) und ist zu dokumentieren. Dies ist schon deshalb geboten, um eine nachträgliche Überprüfung im Verwaltungsrechtswege zu eröffnen.

Ausgenommen von der Anordnungspflicht sind dabei einerseits diejenigen Maßnahmen, welche in ihrer Eingriffsintensität als gering einzustufen sind (betrifft v.a. Personenüberprüfung sowie Verweisung und Betretungsverbot) und die zudem aufgrund ihrer Natur ohnehin in aller Regel einer besonderen Eilbedürftigkeit unterfallen. Andererseits können auch die übrigen Maßnahmen nach Maßgabe des Absatzes 2 ohne vorherige Anordnung durchgeführt werden, wenn ansonsten der Zweck der Maßnahme vereitelt oder wesentlich erschwert würde. Relevant sind insbesondere akute Gefährdungssituationen, bei denen qualifiziert funktionsgefährdende Tätigkeiten unmittelbar bevorstehen (oder schon begonnen haben) und jeder Zeitverzug eine Gefahrenabwehr unmöglich machen würde. Gleiches gilt, wenn in Fällen eines bereits eingetretenen Schadens die verursachende Person versucht, sich dem Zugriff des Wachpersonals zu entziehen.

Zu Unterabschnitt 3 (Befugnisse zur Sicherung von Verschlusssachen)

Die in Unterabschnitt 3 enthaltenen Befugnisse entsprechend im Wesentlichen denen, die im bisherigen Recht in den §§ 65a bis 65e enthalten waren. Dabei wurden diesen Vorschriften zur systematischen Harmonisierung mit dem vorangegangenen Unterabschnitt nunmehr eine Regelung vorangestellt (§ 115), welche den betroffenen Personenkreis definiert und damit das Anwendungsfeld der Vorschriften eingrenzt. Die vormals in § 65f enthaltene Bestimmung zur Durchführung der Maßnahmen wurde in Unterabschnitt 4 verschoben.

Zu § 115 (Betroffene Personen; Mitwirkungspflicht; Belehrung)

Zu Absatz 1

§ 115 Absatz 1 entspricht in seinem Regelungsgehalt den bisherigen § 65a Absatz 2 (Nummern 1 bis 3) und § 65f Absatz 6 (Nummer 4), die nunmehr gebündelt und allgemein „vor die Klammer“ gezogen wurden. Dabei wird klargestellt, dass nicht nur die Zwangsbefugnisse (des bisherigen § 65f) in unmittelbarer Nähe zu den Dienststellen des Bundesnachrichtendienstes ausgeübt werden können, sondern auch die den Verwaltungszwang zugrundeliegenden Maßnahmen.

Zu Absatz 2

Absatz 2 entspricht dem bisherigen § 65a Absatz 2 Satz 2. Wie im bisherigen Recht kann eine Weigerung, an der Durchführung von Maßnahmen zur Sicherung von Verschlusssachen mitzuwirken, für betroffene Bedienstete statusrechtliche, disziplinarrechtliche oder arbeitsrechtliche Maßnahmen nach sich ziehen.

Zu Absatz 3

Absatz 3 entspricht dem bisherigen § 65a Absatz 3. Mit Blick auf die besonderen Befugnisse des Bundesnachrichtendienstes zur Sicherung von Verschlusssachen und die hiervon ausgehenden potentiellen Grundrechtseingriffe ist es geboten, die betroffenen Personen über den Umgang mit Verschlusssachen, die besonderen Sicherungsbefugnisse und die sie treffenden Mitwirkungspflichten zu belehren.

Zu § 116 (Kontrolle und Durchsuchung von Personen, Taschen und Fahrzeugen zur Sicherung von Verschlusssachen)

Die Norm entspricht dem bisherigen § 65b. Auf die Begründung (BT-Drs. 20/8627, S. 66ff.) wird verwiesen.

Zu § 117 (Kontrolle und Durchsuchung von Räumen zur Sicherung von Verschlusssachen)

Die Norm entspricht dem bisherigen § 65c. Auf die Begründung (BT-Drs. 20/8627, S. 68f.) wird verwiesen.

Zu § 118 (IT-Kontrollen zur Sicherung von Verschlusssachen)

Die Norm entspricht im Wesentlichen dem bisherigen § 65d. Insoweit wird auf die Begründung (BT-Drs. 20/8627, S. 69ff.) verwiesen.

Die Regelung hat dabei jedoch einige Änderungen erfahren. Diese sind zum Teil nur redaktioneller Art: So wurde der vormals in Absatz 2 enthaltene Straftatenkatalog nunmehr in die allgemeine Begriffsbestimmung zu qualifiziert funktionsgefährdenden Tätigkeiten (§ 104 Nummer 2 Buchstabe c) verschoben und konnte aus diesem Grund hier entfallen.

Die Befugnis des Bundesnachrichtendienstes in Absatz 3 zur Sicherstellung von Geräten der Informations- und Kommunikationstechnik, die eine Person vorschriftswidrig in Dienststellen des Bundesnachrichtendienstes eingebracht hat, wurde zudem erweitert. Nunmehr ist nicht länger erforderlich, dass tatsächliche Anhaltspunkte für den Verdacht bestehen, dass die Person eine Straftat nach § 104 Nummer 2 Buchstabe c plant, begeht oder begangen hat. Vielmehr ist eine Sicherstellung nunmehr auch dann möglich, wenn die Person das Gerät vorschriftswidrig in die Dienststellen eingebracht hat. Dieser Umstand alleine ist künftig hinreichend, um eine Sicherstellung (oder, wenn die betroffene Person der Sicherstellung widerspricht, die Erstellung eines Abbildes der auf dem Gerät gespeicherten Informationen einschließlich personenbezogener Daten) zu rechtfertigen. Diese Verschärfung

ist notwendig, um der veränderten Sicherheitslage zu begegnen, in der eine Aufklärung des Bundesnachrichtendienstes durch fremde Mächte eine zunehmende Gefahr darstellt.

Handelt es sich bei dem unbeabsichtigten verbotswidrigen Einbringen offensichtlich um ein bloßes Versehen, wäre eine sofortige Sicherstellung oder Abbilderzeugung unverhältnismäßig, so beispielsweise in Fällen, in denen ein Bediensteter etwa durch sichtbare Warnhinweise oder technische Mittel unmittelbar nach Betreten der Dienststelle gewarnt wird, dass er ein Gerät der Informations- und Kommunikationstechnik bei sich führt und er daraufhin ohne großen zeitlichen Verzug umkehrt, um das Gerät in dem dafür vorgesehenen Behältnis einzuschließen. Falls die oder der Bedienstete mit einer Sicherstellung seines Gerätes nicht einverstanden ist, kann der Bundesnachrichtendienst stattdessen ein Abbild der gespeicherten Daten erstellen; dies ist von dem oder der Bediensteten zu dulden. Die Aufnahme dieser Option dient dazu, die Maßnahme möglichst grundrechtsschonend auszugestalten. Dies hat den Hintergrund, dass die Sicherstellung oder Abbilderzeugung individuell unterschiedliche belastende Wirkungen auf die betroffene Person entfalten kann, die möglichst gering gehalten werden soll, ohne den Zweck der Maßnahme zu vereiteln.

Ein Auslesen des Gerätes oder Abbildes ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die betroffene Person eine Straftat nach Absatz 2 Satz 1 und 2 plant, begeht oder begangen hat. Dies bedeutet, dass die Sicherstellung/Abbilderzeugung noch nicht die Befugnis beinhaltet, die Daten auch auszulesen. Hierfür muss vielmehr ein weiterer, verdachtserhärtender Umstand hinzukommen, welcher sich etwa aus vorherigen sicherheitsrelevanten Vorkommnissen im Zusammenhang mit der oder dem Bediensteten ergeben kann. Werden im Rahmen einer Prüfung im Anschluss an die Sicherstellung/Abbilderzeugung keine entsprechenden tatsächlichen Anhaltspunkte gefunden, so ist das Gerät unverzüglich zurückzugeben bzw. das Abbild zu löschen. Anderenfalls ist das Gerät innerhalb von zwei Wochen zurückzugeben, solange es nicht im Rahmen eines Strafverfahrens benötigt wird (dies entspricht dem geltenden Recht).

Zu § 119 (Besondere Maßnahmen zur Sicherung von Verschlusssachen)

Wie § 36 Absatz 2 enthält auch § 119 eine besondere, aktive Einwirkungsmöglichkeit des Bundesnachrichtendienstes. Dabei handelt es sich aber bei der hier in Rede stehenden Befugnis, in informationstechnische Systeme einzugreifen (Absatz 1) und unbefugt gespeicherte Verschlusssachen oder geheimhaltungsbedürftige Informationen zu löschen (Absatz 2) nicht um eine ordnungsrechtliche Befugnis der Gefahrenabwehr, sondern um eine Befugnis zur Sicherung der Funktionsfähigkeit des Bundesnachrichtendienstes im Allgemeinen und der Sicherheit von Informationen (insbesondere Verschlusssachen und damit indirekt auch dem Schutz seiner Bediensteten) im Besonderen.

Zu Absatz 1

In Absatz 1 ist die besondere Befugnis des Bundesnachrichtendienstes geregelt, in informationstechnische Systeme einzugreifen, wenn der dringende Verdacht besteht, dass auf dem informationstechnischen System unbefugt Verschlusssachen oder geheimhaltungsbedürftige Informationen des Bundesnachrichtendienstes gespeichert werden.

Schon die Anknüpfung an die Tatbestandsvoraussetzung eines „dringenden Verdachtes“ zeigt insoweit die systematische (wie materielle) Unterscheidung zu den aufklärenden Tätigkeiten des Bundesnachrichtendienstes: Es reichen gerade nicht „tatsächliche Anhaltspunkte“ aus, vielmehr muss beim dringenden Verdacht inhaltlich eine hohe Wahrscheinlichkeit bestehen. Dabei ist – anders als bei dem strafprozessualen Begriff des dringenden Tatverdachtes – keine Straftat das Anknüpfungsmerkmal der Wahrscheinlichkeit, sondern der objektive Umstand, dass auf einem System unbefugt Verschlusssachen oder geheimhaltungsbedürftige Informationen des Bundesnachrichtendienstes gespeichert werden. Die in Absatz 3 vorgesehene, entsprechende Anwendung des § 39 Absatz 1 Satz 2 stellt sicher, dass nur solche Systeme von der Maßnahme betroffen sein können, bei denen eine

Verantwortlichkeit des Betreibers mit dem unrechtmäßigen Abfluss der Verschlusssachen besteht. Dabei ist insbesondere ein unmittelbarer Zusammenhang zwischen der Verbreitung der Verschlusssachen und dem Systembetreiber regelmäßig bereits durch die objektiven Umstände der Speicherung auf dem Gerät indiziert. Dies ist hingegen etwa dann nicht der Fall, wenn z.B. der Bundesnachrichtendienst Kenntnis erhält, dass einer Journalistin oder einem Journalisten geheimhaltungsbedürftige Informationen zugespielt wurden. Hier besteht kein unmittelbarer Zusammenhang, da davon auszugehen ist, dass die Informationen anonym geteilt wurden und somit der Journalist/die Journalistin keinerlei Kenntnis über die näheren Umstände des Abflusses haben. Im Übrigen wäre ein Eingriff hier auch unverhältnismäßig.

Der Begriff der „geheimhaltungsbedürftigen Informationen“ des Bundesnachrichtendienstes ist weit zu verstehen und geht über die Bedeutung des Begriffs der Verschlusssache hinaus. Er schließt insbesondere auch Informationen über die durch den Bundesnachrichtendienst eingesetzten Personen (Bedienstete und nachrichtendienstliche Verbindungen) ein. Eine denkbare Fallgruppe besteht darin, dass Informationen über Bedienstete oder nachrichtendienstliche Verbindungen auf Servern im Ausland gespeichert sind, was zu einer Bedrohung nicht nur der Auftragserfüllung des Bundesnachrichtendienstes führen kann, sondern Leib, Leben und Freiheit der betroffenen Personen unmittelbar gefährden kann. In diesen Fällen muss dem Bundesnachrichtendienst ein Instrument an die Hand gegeben werden, die entsprechenden Informationen zu entfernen. Dabei ist die Befugnis freilich den allgemeinen Schranken der Verhältnismäßigkeit unterworfen. Handelt es sich beispielsweise um das System einer journalistischen Unternehmung – sei es eine Zeitung, sei es ein privat betriebener, journalistischer Blog – so hat im Rahmen der Angemessenheit eine umfangreiche Abwägung mit Artikel 5 Absatz 1 des Grundgesetzes zu erfolgen. Dabei wird regelmäßig eine akute Gefährdung einer Person – etwa durch Veröffentlichung der Tätigkeit für den Bundesnachrichtendienst in einem Staat, in dem dieser Umstand bereits eine Lebensgefahr begründet – vorliegen müssen.

Zu Absatz 2

Die in Absatz 2 1. Halbsatz geregelte Befugnis, die gespeicherten Daten zu löschen, flankiert die Eingriffsbefugnis des Absatzes 1. Neben der Löschung darf der Bundesnachrichtendienst nach Absatz 2 2. Halbsatz auch personenbezogene Daten erheben, wenn diese „geeignet sind, die Umstände der Speicherung aufzuklären“. Dies beinhaltet zuvorderst diejenigen personenbezogenen Daten, welche Rückschlüsse darauf zulassen, woher die Verschlusssachen bzw. die geheimhaltungsbedürftigen Informationen stammen, ob etwa ein Informant (oder hauptamtlicher Mitarbeiter eines fremden Dienstes) den Bundesnachrichtendienst unterwandert hat oder ein Verräter oder eine Verräterin in den eigenen Reihen die Informationen geteilt hat.

Zu Absatz 3

Da es sich bei der hier geregelten Befugnis um eine besondere Form des Eingriffs in informationstechnische Systeme handelt, gelten eine Reihe von Vorgaben entsprechend. Letzteres enthält dabei im Vergleich zu § 120 zusätzliche Vorgaben – dort diejenigen, die auf die §§ 37 und 38 verweisen, wobei spiegelbildlich zur Abgrenzung im Einzelnen die Art des Systems („privat genutzt“), der Umfang einer Datenerhebung (in aller Regel nur eine beschränkte Erhebung) und der Inlandsbezug (vgl. § 37 Absatz 3 und § 38 Absatz 2 Nummer 1) entscheidend ist. Aufgrund der potentiell hohen Eingriffsintensität ist auch eine Vorabkontrolle durch den Unabhängigen Kontrollrat erforderlich.

Zu § 120 (Anordnung von Maßnahmen zur Sicherung von Verschlusssachen)

Die Norm entspricht dem bisherigen § 65e. Auf die Begründung (BT-Drs. 20/8627, S. 72f.) wird verwiesen. Dabei wurde die in § 65e Absatz 3 enthaltene Regelung (Widerspruch und Anfechtungsklage haben keine aufschiebende Wirkung) nunmehr allgemein für die

Befugnisse dieses Abschnittes in § 105 Absatz 1 geregelt. Dies betrifft ausdrücklich auch Kontrollen nach § 116 Nummer 1, die im bisherigen Recht missverständlich vom Wortlaut ausgenommen blieben.

Zu Unterabschnitt 4 (Durchführung von Maßnahmen)

Zu § 121 (Vorgaben zur Durchführung von Maßnahmen durch unmittelbaren Zwang)

Die Vorschrift baut auf dem bisherigen § 65f (vgl. die Begründung in BT-Drs. 20/8627, S. 73ff.) auf und regelt nunmehr umfassend die Durchführung – das heißt die Vollstreckung – der Maßnahmen dieses Abschnittes. Dabei wurde die Vorschrift systematisch angepasst, um normenklarere Regelungen zu treffen.

Zu Absatz 1

Der Absatz regelt zunächst die grundsätzliche Befugnis des Bundesnachrichtendienstes, solche Maßnahmen dieses Abschnitts (insofern also auch auf die neuen Befugnisse des Unterabschnitts 2 erstreckt) die auf die Herausgabe einer Sache oder auf die Vornahme einer Handlung oder auf Duldung gerichtet sind, durch unmittelbaren Zwang durchsetzen. Einer solchen Befugnis bedarf es schon deshalb, weil das Gesetz über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes für die Bediensteten des Bundesnachrichtendienstes, bei denen es sich nicht um Vollzugsbeamte des Bundes handelt, keine Anwendung findet.

Absatz 1 entspricht dem bisherigen § 65f Absatz 7, dessen Satz 5 nunmehr in der allgemeinen Regelung zu Grundrechtseinschränkungen („Zitiergebot“) aufgeht.

Die vormals in § 65f Absatz 7 Satz 2 enthaltene Regelung, die unmittelbaren Zwang bei „Kontrollen nach § 65b Nummer 1 an Eingängen zum Zwecke des § 65a Absatz 1 Nummer 1“ ausgeschlossen hat, findet sich nunmehr – in ihrem Regelungsgehalt identisch – in § 122 Absatz 2 Nummer 2. Wie bislang kann der Bundesnachrichtendienst in diesen Fällen, wenn eine betroffene Person im Sinne des § 115 die Mitwirkung verweigert, den Zutritt zur Dienststelle verweigern. Dass z. B. eine Mitarbeiterin oder ein Mitarbeiter in diesem Fall unentschuldigt den Dienst nicht antritt, wäre weiterhin (nur) durch arbeitsrechtliche Maßnahmen oder disziplinarrechtlich zu ahnden.

Die zwangsweise Durchsetzung von Kontrollen zum Zweck der Verhinderung des vorschriftswidrigen Ausbringens, also beim Verlassen der Dienststelle, ist hingegen (weiterhin) zulässig.

Zu Absatz 2

Die Norm entspricht dem bisherigen § 65f Absatz 1. Auf die Begründung (BT-Drs. 20/8627, S. 74) wird verwiesen. Der – deklaratorische – Hinweis, dass der Grundsatz der Verhältnismäßigkeit zu beachten ist, gilt für alle Maßnahmen dieses Abschnitts, welche durgeführt werden.

Zu Nummer 1

Nummer 1 trifft Vorgaben für die Durchführung (d.h. Vollstreckung) von Maßnahmen zur Sicherung der Bediensteten und Dienststellen des Bundesnachrichtendienstes. Die Vorschrift entspricht dabei § 9 des Gesetzes über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und zivile Wachpersonen.

Zu Nummer 2

Nummer 3 trifft Vorgaben für die Durchführung (d.h. Vollstreckung) von Maßnahmen zur Sicherung von Verschlusssachen des Bundesnachrichtendienstes. Dabei ist der unmittelbare Zwang bei Zugangskontrollen nach § 116 Nummer 1 zum Zweck des § 104 Nummer 5 Buchstabe a ausgeschlossen. Wie bislang kann der Bundesnachrichtendienst in diesen Fällen, wenn eine betroffene Person im Sinne des § 115 die Mitwirkung verweigert, den Zutritt zur Dienststelle verweigern. Die zwangsweise Durchsetzung von Kontrollen zum Zweck der Verhinderung des vorschriftswidrigen Ausbringens, also beim Verlassen der Dienststelle, ist hingegen (weiterhin) zulässig (vgl. hierzu bereits oben).

Zu Absatz 3

In Absatz 3 finden sich besondere Vorgaben für die Durchführung von Maßnahmen der Unterabschnitte 2 und 3. So etwa die Vorgabe, dass die Durchführung einer Maßnahme durch Anwendung unmittelbaren Zwangs grundsätzlich anzudrohen ist. Etwas anderes gilt nur dann, wenn der sofortige Vollzug der Maßnahme zur Verhinderung einer qualifiziert funktionsgefährdenden Tätigkeit notwendig ist.

Zu § 122 (Besondere Vorgaben zur Durchführung von Maßnahmen zur Sicherung von Verschlusssachen)

Die Vorschrift enthält die besonderen Vorgaben, welche im bisherigen Recht in § 65f Absatz 4 (Absatz 1) sowie in § 65f Absatz 5 (Absatz 2) enthalten waren. Auf die Begründung (BT-Drs. 20/8627, S. 74) wird verwiesen.

Zu Unterabschnitt 5 (Verarbeitung von personenbezogenen Daten aus Maßnahmen zur Sicherung von Verschlusssachen)

Der Unterabschnitt enthält die im bisherigen Recht in Abschnitt 6 Unterabschnitt 2 enthaltenen besonderen Vorgaben für die Weiterverarbeitung von personenbezogenen Daten, welche mittels der in diesem Abschnitt geregelten Befugnisse erhoben wurden.

Im Vergleich zum geltenden Recht wurde dabei die Regelungssystematik stark vereinfacht: Die vormals in §§ 65h, 65i und 65k enthaltenen Vorgaben für personenbezogene Daten, welche den Kernbereich privater Lebensführung betreffen (§ 65h) oder aus Vertraulichkeitsbeziehungen (§ 65i) entstammen sowie die besonderen Protokollvorgaben (§ 65k) wurden aufgehoben. Stattdessen gelten für diese Daten nunmehr die allgemeinen Regelungen, was bezüglich der bisherigen §§ 65h und 65i in § 124 Absatz 1 Satz 3 geregelt wird und für § 65k – da die allgemeine Protokollpflicht entfällt – keiner besonderen Regelung bedarf.

Zuständig für die Kontrolle der Verarbeitung von personenbezogenen Daten ist – da es sich hierbei oftmals um Daten handelt, welche eine spezifische nachrichtendienstliche Natur aufweisen – der Unabhängige Kontrollrat.

Zu § 123 (Besondere Bestimmungen zur Verarbeitung personenbezogener Daten)

Zu Absatz 1

Absatz 1 regelt die Befugnis zur Verarbeitung von personenbezogenen Daten in dem Maße, welches für die Befugnisse nach diesem Abschnitt erforderlich ist. Wie in § 65g Absatz 1, auf dem die Vorschrift basiert (vgl. die Begründung in BT-Drs. 20/8627, S. 75), ist auch eine Kennzeichnungspflicht erhobener Daten vorgesehen. Ergänzt wurde die Vorschrift aufgrund des Wegfalls von §§ 65h und 65i um einen Verweis auf die §§ 21 und 22, welche die Erhebung von Daten, die den Kernbereich privater Lebensführung betreffen, sowie aus Vertraulichkeitsbeziehung regeln und nunmehr entsprechende Anwendung finden.

Zu Absatz 2

Die Regelung entspricht dem bisherigen § 65g Absatz 2. Auf die Begründung (BT-Drs. 20/8627, S. 75) wird verwiesen.

Zu Absatz 3

Die Regelung basiert auf dem bisherigen § 65g Absatz 3 (vgl. hierzu die Begründung in BT-Drs. 20/8627, S. 75), enthält indes eine Reihe von Abweichungen:

Zunächst wurde dem Umstand Rechnung getragen, dass nicht länger nur personenbezogene Daten von den in § 115 genannten Personen – bei denen es sich um Personen mit einer besonderen „Innenbeziehung“ zum Bundesnachrichtendienst handelt – aufgrund von Maßnahmen zur Verschlusssachensicherung betroffen sind. Vielmehr sind nunmehr auch die Daten von „Störern“ im Sinne des § 108 eingeschlossen, welche im Rahmen von Maßnahmen zum Schutz der Bediensteten und Dienststellen erhoben wurde.

Dieser Differenzierung tragen die Regelungen in Absatz 3 Nummer 1 und Nummer 2 Rechnung: Nach Nummer 1 ist eine Weiterverarbeitung und Übermittlung von personenbezogenen Daten, welche aufgrund von Maßnahmen zum Schutz der Bediensteten und Dienststellen erhoben wurden, dann statthaft, wenn tatsächliche Anhaltspunkte dafür bestehen, dass dies für zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist. Hierunter fallen insbesondere auch die Eigensicherung/Eigenbefähigung des Bundesnachrichtendienstes. Dies ist schon deshalb geboten, weil nicht auszuschließen ist, dass gezielte Störungen gegen den Bundesnachrichtendienst von anderen Nachrichtendiensten orchestriert werden. Entsprechend muss der Bundesnachrichtendienst in der Lage sein, diese Daten im Bedarfsfall auch für seine eigentliche Kernaufgabe verfügbar machen zu können.

Die in Nummer 2 geregelte Weiterverarbeitung und Übermittlung von personenbezogenen Daten, welche im Rahmen von Maßnahmen nach Unterabschnitt 3 (also zur Sicherung von Verschlusssachen) erhoben wurden, ist demgegenüber – entsprechend dem geltenden Recht – auf besondere Fälle beschränkt. Eine Weiterverarbeitung ist insoweit möglich, wenn tatsächliche Anhaltspunkte für eine der genannten Bedrohungen vorliegen, also eine Gefährdung von Personen, die für den Bundesnachrichtendienst tätig sind, Einrichtungen, geheimhaltungsbedürftigen Informationen oder Gegenstände des Bundesnachrichtendienstes durch sicherheitsgefährdende oder geheimdienstliche Tätigkeiten (Nummer 4) oder sicherheitsgefährdende oder geheimdienstlichen Strukturen sowie sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten mit Auswirkungen auf die Bundesrepublik Deutschland oder Mitgliedstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrags, es sei denn, die Tätigkeiten sind offenkundig ungeeignet, ihre Ziele zu erreichen (Nummer 11). In diesen Fällen, in denen die Verschlusssachenkontrolle also (wenigstens auch) zu tatsächlichen Anhaltspunkten führte, dass eine konkrete Spionagetätigkeit (im weitesten Sinne) zu besorgen ist, muss der Bundesnachrichtendienst die entsprechenden personenbezogenen Daten mit seinen übrigen Auftragsdaten abgleichen können.

In Nummer 3 ist eine moderate Erweiterung der Weiterverarbeitungs- und Übermittlungsmöglichkeiten vorgesehen. Das bisherige Recht enthält insoweit die unbeabsichtigte Lücke, dass die Daten nicht zu arbeitsrechtlichen oder disziplinarrechtlichen Maßnahmen genutzt werden können. Dies ist aber – insbesondere im Rahmen von Maßnahmen nach Unterabschnitt 3 – zwingend, um nötigenfalls Konsequenzen gegenüber Bediensteten (und Externen) ergreifen zu können, welche widerrechtlich mit Verschlusssachen umgehen. Gleiches gilt für die Weiterverarbeitungs- und Übermittlungsmöglichkeit zur Strafverfolgung in Nummer 4.

Nummer 5 entspricht der Regelung im bisherigen Recht (vgl. den Verweis in § 65g Absatz 3 auf § 2 Absatz 1 Nummer 2).

Es handelt sich bei den Vorgaben des § 123 nicht um eigene Übermittlungsregelungen, sondern um Zweckbeschränkungen. Die allgemeinen Übermittlungsvorschriften finden Anwendung, d.h. – da es sich bei den in Abschnitt 7 geregelten Befugnissen nicht um besondere Befugnisse der Datenerhebung im Sinne des § 6 Absatz 1 handelt – insbesondere die Vorschrift des § 88.

Zu Absatz 4

Absatz 4 beinhaltet spezielle Bestimmungen zur Weiterverarbeitung und Übermittlung von Daten, die nach § 114 Absatz 2 im Rahmen der Befugnis zur Einsatzsicherung in im Bundesgebiet befindlichen Wohnungen erhoben wurden, soweit diese zum Zweck der Strafverfolgung erfolgt. Eine Weiterverarbeitung und Übermittlung ist nur dann zulässig, wenn die Maßnahme nach § 114 Absatz 2 zuvor gemäß § 98 Absatz 5 zur unabhängigen Vorabkontrolle der Rechtmäßigkeit vorgelegt wurde und die Rechtmäßigkeit der Anordnung festgestellt wurde. Soweit eine Maßnahme den in Absatz 1 genannten Zwecken, d.h. zur Abwehr von Gefahren für Leib, Leben oder Freiheit von Personen, die für den Bundesnachrichtendienst tätig sind, dient, ist eine Weiterverarbeitung und Übermittlung ausnahmsweise auch dann zulässig, wenn die Rechtmäßigkeit der Anordnung im Rahmen der Vorabkontrolle nicht festgestellt worden ist.

Zu Absatz 5

Die Regelung zur besonderen Übermittlungsmöglichkeit an eine herausgebende Stelle von Verschlusssachen entspricht dem bisherigen § 65l Absatz 2. Auf die Begründung (BT-Drs. 20/8627, S. 77) wird verwiesen.

Zu § 124 (Schutz von minderjährigen Personen)

Die Norm entspricht weitgehend dem bisherigen § 65j, wobei die Altersgrenzen an die allgemeine Differenzierung zwischen dem Kindes- und Jugendalter angepasst wurde, die beispielsweise im Jugendschutzgesetz (§ 1 Abs. 1 JuSchG) sowie im Gesetz über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes (§ 12 Absatz 3 UZwG) etabliert sind. Personenbezogene Daten zu minderjährigen Personen, die noch nicht 14 Jahre alt sind, dürfen grundsätzlich nicht weiterverarbeitet werden. Bei minderjährigen Personen, die mindestens 14 Jahre alt sind, ist eine Verarbeitung lediglich dann zulässig, wenn diese zu den in § 109 oder § 116 genannten Personen gehören – die Speicherung ist insofern nur zulässig, wenn ein räumlicher oder funktionaler Zusammenhang zur Dienststelle oder Tätigkeit des Bundesnachrichtendienstes besteht. Dies ist beispielsweise der Fall, wenn eine jugendliche Person eine funktionsgefährdende Tätigkeit gegen den Bundesnachrichtendienst plant, begeht oder begangen hat (§ 109 Nummer 4). Wenngleich fremde Dienste im Zuge ihrer Spionage- und Sabotagetätigkeit keine Rücksicht auf Altersgrenzen nehmen, ist im Grundsatz dennoch aus verfassungsrechtlichen Erwägungen ein besonderer Schutz zum Schutz von Kindern und Jugendlichen im Rahmen der Verarbeitung von Daten zum Schutz von Bediensteten, Dienststellen und Verschlusssachen vorgesehen. Die stufenweise erfolgende Differenzierung zwischen Kindern, Jugendlichen und Erwachsenen dient sowohl der Einheit der Rechtsordnung als auch dem Schutz des Kindeswohls. Zugleich werden durch die Ausgestaltung der Norm die spezifischen sicherheitlichen Belange des Bundesnachrichtendienstes berücksichtigt.

Zu Abschnitt 9 (Landes- und Bündnisverteidigung)

Artikel 80a Absatz 1 Satz 1 des Grundgesetzes sieht vor, dass der einfache Gesetzgeber bei Feststellung des Eintritts des Spannungsfalles in Bundesgesetzen über die Verteidigung einschließlich des Schutzes der Zivilbevölkerung eine Anwendungssperre vorsehen kann. Die Gesetzgebungsbefugnis ergibt sich neben den Auswärtigen Angelegenheiten des Artikel 73 Absatz 1 Nummer 1 Variante 1 des Grundgesetzes insofern auch aus Artikel 73 Absatz 1 Nummer 1 Variante 2 des Grundgesetzes. Die Regelungen dienen der von Artikel 80a des Grundgesetzes bezweckten Erhöhung der militärischen und zivilen

Verteidigungsbereitschaft zur Bewältigung von Notstandslagen und sind insofern Bestandteil des Notstandsrechts.

Die in diesem Abschnitt vorgesehenen Befugnisse modifizieren den normativen Handlungsrahmen des Bundesnachrichtendienstes in außergewöhnlichen Notstands- und Krisenlagen. Dies dient der Stärkung der Bündnis- und Verteidigungsfähigkeit sowie dem Schutz der Zivilbevölkerung. Die Regelungen stärken die nationale Souveränität der Bundesrepublik Deutschland und stellen sicher, dass Deutschland im Rahmen der Gesamtverteidigung sowie im Einklang mit seinen Bündnisverpflichtungen handlungsfähig bleibt. Der Bundesrepublik Deutschland muss es möglich sein, Angriffen und Bedrohungen von außen mit den erforderlichen Mitteln wirksam entgegenzutreten. Aufgrund seiner geostrategischen Lage und seiner Einbindung in Verteidigungsbündnisse ergeben sich für die Bundesrepublik Deutschland zudem Bündnisverpflichtungen auch in ihrer Rolle als Aufmarsch- und Transitzone für verbündete Streitkräfte sowie als rückwärtiger Operationsraum für Einsatzoptionen des Nordatlantikbündnisses im zentraleuropäischen Raum. Die dafür erforderliche Unterstützung der Bündnispartner als Transit- und Gastnation ist eine gesamtstaatliche Aufgabe, innerhalb derer der Bundesnachrichtendienst mit seiner Tätigkeit als ziviler und militärischer Auslandsnachrichtendienst als ein maßgeblicher Leistungserbringer funktionieren muss.

Die Regelungen dieses Abschnitts dienen dazu, für die Tätigkeit des Bundesnachrichtendienstes auch in Krisenzeiten geeignete rechtliche Maßgaben zu setzen.

In einem Verteidigungs-, Spannungs- oder auch einem Zustimmungsfall im Sinne des § 125 Absatz 3 besteht eine besondere Bedrohungslage für den Staat und die Bevölkerung in ihrer Gesamtheit. Der Bundesnachrichtendienst muss in diesem Fall seine Fähigkeiten konzentrieren und verstärken können. Die Regelungen ermöglichen flexible Reaktionen auf Notstandslagen in diesen Fällen. Es werden bzw. im Spannungs- oder Zustimmungsfall im Sinne des § 125 Absatz 3 können insbesondere Pflichten der Prüfung und Dokumentation von Maßnahmen und Daten auf ein Mindestmaß beschränkt werden, um die Ressourcen des Bundesnachrichtendienstes situationsgerecht einsetzen zu können. Der Staat kann nur so seiner Verantwortung als Garant für Sicherheit nachkommen und außenpolitisch handlungsfähig bleiben.

Das Verhältnismäßigkeitsprinzip als ein tragendes Verfassungsprinzip ist dabei auch bei Anwendung der Regelungen des Abschnittes 9 zu beachten.

Zu § 125 (Verteidigungs-, Spannungs- und Zustimmungsfall)

Damit der Bundesnachrichtendienst auch in äußeren Konfliktsituationen (Verteidigungs-, Spannungs- sowie dem Zustimmungsfall), funktionsfähig bleibt und seinen Beitrag zur Verteidigung der Bundesrepublik Deutschland oder seiner Verbündeten leisten kann, werden in diesem Abschnitt besondere Regelungen getroffen. Der Bundesnachrichtendienst wird unmittelbar in die (aktive) Verteidigung der Bundesrepublik Deutschland eingebunden. Die Notwendigkeit hierfür folgt letztlich schon daraus, dass der Bundesnachrichtendienst einerseits in seiner Rolle als Informationsbeschaffer und Informationsauswerter der nachrichtendienstlichen Auslandsaufklärung aber insbesondere auch mittels erweiterter nachrichtendienstlicher Maßnahmen in der Lage ist, die zum Schutz der Bundesrepublik und seiner Bevölkerung erforderlichen Tätigkeiten gegenüber Bedrohungen aus dem Ausland auszuüben.

§ 125 knüpft dabei (verfassungsunmittelbar) an den Verteidigungsfall (Absatz 1), den Spannungsfall (Absatz 2) an. Darüber hinaus wird in Absatz 3 ein dritter Fall abgebildet, der sich am (verfassungsunmittelbaren) Zustimmungsfall orientiert. Diese drei staatswohlrelevanten Sachlagen bilden zugleich ein gestuftes System, bei dem der Verteidigungsfall die letzte Eskalationsstufe darstellt und entsprechend zu einer vollständigen Anwendung der

Vorschriften des Abschnittes 9 führt. Die weiteren Stufen lassen – in Ansehung der konkreten Lage – auch die Anwendung lediglich einzelner Vorschriften zu.

Zu Absatz 1

Zum Verteidigungsfall siehe Artikel 115a des Grundgesetzes (Notstandsverfassung).

Zu Absatz 2

Zum Spannungsfall siehe Artikel 80a des Grundgesetzes (Notstandsverfassung).

Mit der Regelung in Absatz 2, 2. Halbsatz wird dem Umstand Rechnung getragen, dass die Situation des Spannungsfalls graduell von der Situation im Rahmen des Verteidigungsfalls abweichen kann. Im Spannungsfall als Vorstufe des Verteidigungsfalls sollen die Regelungen dieses Abschnitts daher erst dann Anwendung finden, wenn ein zusätzlicher Beschluss vorliegt, welcher – neben der allgemeinen Proklamation des Spannungsfalls mit seiner generellen Folge der Freischaltung von Notstandsvorsorgeregelungen in einer Vielzahl einfacher Gesetze – gerade die besonderen Regelungen des Abschnittes 9 freischaltet. Mit diesem zusätzlichen Beschluss kann die Bundesregierung die Umstände, die zur Ausrufung des Spannungsfalls geführt haben, im konkreten Fall im Verhältnis zur Freischaltung der Regelungen dieses Abschnitts beurteilen. Die Regelungen kommen dann zur Anwendung, wenn aufgrund der äußeren Umstände eine bedeutende Intensivierung der nachrichtendienstlichen Tätigkeit geboten ist. Dabei ist es auch möglich, dass mit der Feststellung einzelne Regelungen dieses Abschnitts von der Anwendung ausgenommen werden bzw. nur bestimmte Regelungen Anwendung finden.

Der in der Vorschrift angelegte auslegungsbedürftige Rechtsbegriff der „Gründe der Verteidigung“ ist weit zu verstehen. Gemeint sind alle Umstände, die der (militärischen und zivilen) Gesamtverteidigung dienen und der Abwendung oder Einschränkung der Bedrohung oder des drohenden Angriffs zumindest förderlich sind. Mit der Einschränkung, dass aus diesen Gründen eine Anwendung „zwingend“ notwendig sein muss, wird dem Grundsatz der Verhältnismäßigkeit in besonderer Weise Rechnung getragen. Ob tatsächlich eine zwingende Notwendigkeit vorliegt, ist eine gerichtlich überprüfbare Entscheidung, bei der der Bundesregierung indes eine Einschätzungsprärogative zuzugestehen ist. Eine zwingende Notwendigkeit aus Gründen der Verteidigung ist materiell letztlich dann anzunehmen, wenn andere Mittel nicht geeignet sind, um in gleich effektiver Weise zur Gesamtverteidigung beizutragen.

Zu Absatz 3

Absatz 3 regelt eine dem Spannungs- oder Verteidigungsfall vorgelagerte Konstellation. Er orientiert sich an dem sog. Zustimmungsfall des Artikel 80a Absatz 2 des Grundgesetzes, ist aber hier spezifisch für den nachrichtendienstlichen Kontext ausgestaltet. Liegen weder Verteidigungs- noch Spannungsfall vor, kann das für die parlamentarische Kontrolle zuständige Parlamentarische Kontrollgremium der Anwendung der Notstandsvorschriften (ggf. beschränkt auf einzelne Regelungen) des Abschnittes 9 besonders zustimmen. Dieser Fall ist ebenfalls als eine Vorstufe zum Verteidigungsfall anzusehen und bedarf regelmäßig solche der Ernsthaftigkeit des Spannungsfalls nahe kommenden oder vergleichbaren äußeren Umstände. Ziel dieser Regelung – wie auch des Artikel 80a Absatz 2 des Grundgesetzes – ist es, ggf. weniger weitreichende, z.B. auch nur einzelne Verteidigungsvorbereitungen (hier speziell im nachrichtendienstlichen Bereich) zu treffen. Im Zustimmungsfall nach § 125 Absatz 3 kommen also (einzelne oder alle) Regelungen des Abschnittes 9 dann zur Anwendung, wenn aufgrund der äußeren Umstände eine bedeutende Intensivierung der Verteidigung, insbesondere auch im nachrichtendienstlichen Tätigkeitsbereich, geboten ist, ohne dass dabei eine Proklamation des Spannungs- oder eines Verteidigungsfalls erfolgen soll, aber beispielsweise auch im Einklang mit den Bündnisverpflichtungen der Bundesrepublik Deutschland eine erhöhte Handlungsbereitschaft des Bundesnachrichtendienstes hergestellt werden muss.

Aus Gründen des Missbrauchsschutzes kann die Bundesregierung die Feststellung nach Absatz 3 nicht alleine treffen, sondern ist an die Zustimmung des Parlamentarischen Kontrollgremiums nach Art. 45d des Grundgesetzes gebunden. Da in diesen Situationen eine vorherige Befassung des Bundestages nicht vorliegt, weil der Verteidigungs- oder Spannungsfall nicht beschlossen wurde, ist es gleichwohl geboten, diese besondere Feststellung an die Zustimmung eines Gremiums der Legislative zu knüpfen. Für diese Aufgabe eignet sich das Parlamentarische Kontrollgremium besonders, weil es laufend mit aktuellen sicherheitspolitischen Entwicklungen und nachrichtendienstlichen Erkenntnissen befasst ist und seine Mitglieder deshalb in herausgehobener Weise über nachrichtendienstliche Expertise verfügen.

Zu Absatz 4

Zur Korrektur des exekutivischen Handelns im äußeren Notstand kann der Bundestag im Fall des Absatzes 2 jederzeit mit einfacher Mehrheit die Aufhebung der Entsperrung verlangen, die aufgrund der Anwendbarkeit von Notstandsvorschriften ergangen sind. Im Fall des Absatzes 3 obliegt die Zustimmung zum Beschluss der Anwendbarkeit von Notstandsregeln und damit auch ein parlamentarisches Verlangen nach dessen Aufhebung dem Parlamentarischen Kontrollgremium. Berechnungsgrundlage der erforderlichen Zweidrittelmehrheit in Nummer 2 sind die jeweils aktuell ins Parlamentarische Kontrollgremium gewählten Mitglieder (vgl. zur Formulierung auch § 7 Absatz 2 oder § 11 Absatz 2 PKGrG).

Zu Absatz 5

Soweit in diesem Abschnitt Befugnisse vorgesehen werden, die im Regelbetrieb so nicht vorgesehen sind, ist der Bundesnachrichtendienst ermächtigt, die erforderlichen Vorbereitungen eigenständig bereits vor dem Anwendungsfall dieses Abschnitts zu treffen. Andernfalls stünde zu befürchten, dass die jeweilige Befugnis nicht zeitgerecht zur Wirkung gebracht werden kann. Absatz 5 weist klarstellend darauf hin. Vorbereitungen im Sinne dieses Absatzes können insbesondere der Auf- und Ausbau technischer, struktureller oder organisatorischer Voraussetzungen für die Anwendung der in diesem Abschnitt getroffenen Regelungen sein. Damit soll sichergestellt werden, dass die notwendigen Maßnahmen gerade im Rahmen der Landes- und Bündnisverteidigung im Bedarfsfall schnell und effektiv umgesetzt werden können, vgl. dazu auch die Festlegungen der Rahmenrichtlinie für die Gesamtverteidigung vom 5. Juni 2024 – RRGV.

Zu § 126 (Unterstützung durch andere Stellen)

Zu Absatz 1

Die grundsätzlich bestehende Möglichkeit des Bundesnachrichtendienstes, andere Behörden um Amtshilfe zu bitten, erweitert sich in einer Notstandslage. So kann eine andere Behörde den Bundesnachrichtendienst bei der Ausübung seiner Befugnisse unterstützen, ohne dass die unterstützende Behörde selbst über diese Befugnisse verfügen muss. Dies kann insbesondere aufgrund bestehender Material- und Kapazitätsgrenzen des Bundesnachrichtendienstes erforderlich sein. Es können dabei auch bestehende Fähigkeiten anderer Behörden genutzt werden, um eine schnellere und effektivere Durchführung von Notstandsmaßnahmen zu gewährleisten.

Die allgemeine Grenze der Amtshilfe, dass durch die ersuchte Behörde keine Maßnahmen durchgeführt werden dürfen, zu denen diese nicht befugt ist, gilt insoweit nicht. Beispiel dafür wäre, dass das Bundesamt für Sicherheit in der Informationstechnik gebeten ist, den Bundesnachrichtendienst bei der Umleitung von Telekommunikationsverkehren zu unterstützen.

Zu Absatz 2

Hier findet sich die Verpflichtung inländischer nicht öffentlicher Stellen, insbesondere Unternehmen (darunter Anbieter von Telekommunikationsdienstleistungen und digitalen Diensten), dem Bundesnachrichtendienst bei der Aufgabenerfüllung Unterstützungsleistungen zu gewähren, wie insbesondere den Zugang zu Räumlichkeiten und technischen Systemen. Dies kann auch die Bereitstellung von Personal, das beispielsweise für die technische Unterstützung erforderlich ist, umfassen. Hierdurch wird die Möglichkeit geschaffen, über die Verpflichtung zur Kooperation im Einzelfall für den Zeitraum des Spannungs-, Verteidigungs- und Zustimmungsfalls Unterstützungsleistungen wahrzunehmen, z.B. durch Zusammenarbeit mit Fachpersonal von Unternehmen, soweit keine Ablehnungsgründe geltend gemacht werden. Die nach dieser Norm verpflichteten Unternehmen werden vom Bundesnachrichtendienst für die erbrachten Leistungen entschädigt.

Zu Absatz 3

Die Schriftform dient dazu, die Unterstützungsleistung näher zu bestimmen. Sie ist aber nicht zwingend erforderlich. Zudem gelten Verschwiegensheits- und Geheimhaltungspflichten.

Zu Absatz 4

Sofern das Ziel der Unterstützungsleistung die Datenerhebung zur nachrichtendienstlichen Auslandsaufklärung ist, richtet sich diese nach § 128. Es ist aber denkbar, dass auch anlässlich einer Unterstützung nach § 127 Daten erhoben werden.

Zu § 127 (Datenerhebung unter Mitwirkung anderer Stellen)

Zu Absatz 1

Absatz 1 stellt klar, dass die Regelungen des genannten Abschnitts – hier: Abschnitt 2 (Datenerhebung unter Mitwirkung anderer Stellen) – in den Notstands- und Krisenlagen des Abschnittes 9 nur in modifizierter Form gelten. Sofern in den nachfolgenden Absätzen jeweils eigene Maßgaben vorgesehen sind, modifizieren diese die betreffenden Regelungen des Abschnittes 2.

Zu Absatz 2

Aus der Befugnis des Bundesnachrichtendienstes nach § 7, jede andere Stelle um die Übermittlung von Informationen zu ersuchen, die für die Erfüllung seiner Aufgaben erforderlich ist, folgt in einer Notstandslage die Übermittlungspflicht der angefragten Stelle. Außerhalb der Notstandslage grundsätzlich bestehende gesetzliche Übermittlungsregelungen, insbesondere auch Übermittlungsverbote, aber auch ggf. entgegenstehende vertragliche Beschränkungen, finden insoweit keine Anwendung.

Zu Absatz 3 zu Absatz 4

Die Regelungen dienen der Verfahrensbeschleunigung und der effektiven Nutzung vorhandener Ressourcen unter Berücksichtigung der besonderen Bedrohungslage, die diesem Abschnitt zugrunde liegt. Die vorübergehende Reduzierung administrativer Vorgaben stellt eine notwendige, zweckmäßige und angemessene Anpassung dar, um eine schnelle und effiziente Ressourcennutzung zu gewährleisten. Wesentliche verteidigungswichtige Maßnahmen können dadurch ohne Verzögerungen umgesetzt werden. So können in den Krisenfällen des § 125 die im Regelbetrieb vorgehenen Befristungen der Anordnungen situationsangepasst bestimmt werden.

Zu Absatz 5

Dieser Absatz enthält die Verpflichtung der anderen Stellen.

Zu § 128 (Einsatz nachrichtendienstlicher Mittel)

Zu Absatz 1

Absatz 1 stellt klar, dass die Regelungen des genannten Abschnittes – hier: Abschnitt 3 (Einsatz nachrichtendienstlicher Mittel) – in den Notstands- und Krisenlagen des Abschnittes 9 nur in modifizierter Form gelten. Sofern in den nachfolgenden Absätzen jeweils eigene Maßgaben vorgesehen sind, modifizieren diese die betreffenden Regelungen des Abschnittes 3.

Zu Absatz 2

Die Vorschrift regelt die materielle Voraussetzung für den Einsatz nachrichtendienstlicher Mittel in den Krisenfällen dieses Abschnitts. Für den zur Aufklärung der Bedrohungslagen des § 125 notwendigen Einsatz nachrichtendienstlicher Mittel kann eine Abwägung der jeweiligen Eingriffsintensität pauschaliert und zugunsten der öffentlichen Sicherheit erfolgen: Die in Abschnitt 9 geregelten Krisenlagen sind derart existenziell, dass die im „Normalbetrieb“ gebotene Differenzierung zwischen heimlicher nachrichtendienstlicher Erhebungsbefugnis und dem Grundrecht auf informationelle Selbstbestimmung (bzw. den spezielleren Grundrechten des IT-System-Grundrechts, Artikel 13 oder Artikel 10 des Grundgesetzes) verfassungsrechtlich eine andere Gewichtung erfährt. Ist der Bestand des Staates bedroht, tritt der auf die Privatheit von Daten bezogene Grundrechtsschutz im Rahmen einer Gesamtabwägung zurück.

Zu Absatz 3

Zu Nummer 1 und Nummer 2

Im Verteidigungs-, Spannungs- oder Zustimmungsfall muss es dem Bundesnachrichtendienst möglich sein, flexibel und ohne Zeitverlust auf die konkrete Situation reagieren zu können. Hierzu muss er sich zur Erfüllung seiner Aufgaben aller nachrichtendienstlicher Mittel, bedienen können, ungeachtet von im Regelfall grundsätzlich bestehenden allgemeinen Einschränkungen, wie z.B. Anbahnungsverboten hinsichtlich nachrichtendienstlicher Verbindungen. Die allgemeinen Vorgaben zum Einsatz von nachrichtendienstlichen Mitteln finden daher keine Anwendung.

Zu Nummer 3

Im Verteidigungs-, Spannungs- oder Zustimmungsfall darf der Bundesnachrichtendienst alle im Rahmen der strategischen Aufklärung erhobenen personenbezogenen Daten weiterverarbeiten, soweit dies für die Erfüllung seiner Aufgaben notwendig ist. Es gelten keine höheren Voraussetzungen für die Weiterverarbeitung von Kommunikationsdaten mit qualifiziertem Inlandsbezug.

Zu Absatz 4 und Absatz 5

Die Regelungen dienen der Verfahrensbeschleunigung und der effektiven Nutzung vorhandener Ressourcen unter Berücksichtigung der besonderen Krisenlagen, die diesem Abschnitt zugrunde liegen. Die vorübergehende Reduzierung administrativer Vorgaben stellt eine notwendige, zweckmäßige und angemessene Anpassung dar, um schnelle und effiziente Ressourcennutzung zu gewährleisten. Wesentliche verteidigungswichtige Maßnahmen können dadurch ohne Verzögerungen umgesetzt werden. So können Anordnungen abstrahiert und zusammengefasst und im Verteidigungsfall auch die im Regelbetrieb vorgehenen Befristungen der Anordnungen situationsangepasst bestimmt werden.

Zu Absatz 6

Auch hier gelten die zu Absatz 4 bereits ausgeführten Effizienzerwägungen. Da die Prüf-, Lösch- und Protokollierungspflichten lediglich für die Dauer des Verteidigungs-, Spannungs- oder Zustimmungsfalls ausgesetzt sind und anschließend wieder aufgenommen werden müssen, wird nicht unverhältnismäßig in die Grundrechte eingegriffen.

Zu § 129 (Erweiterte nachrichtendienstliche Maßnahmen)

Der Bundesnachrichtendienst darf nach Abschnitt 4 bereits erweiterte nachrichtendienstliche Maßnahmen vornehmen. Im Verteidigungs-, Spannungs- oder Zustimmungsfall darf der Bundesnachrichtendienst erst recht aktiv wirken und Maßnahmen jenseits des Ziels der Informationsgewinnung mit dem Ziel der Abwendung oder Einschränkung der Bedrohungslage für die Bundesrepublik Deutschland und ihrer Bündnispartner vornehmen. Befugt ist er dabei insbesondere auch zu solchen Maßnahmen, die geeignet sind, die gegnerischen Angriffsfähigkeiten zu schwächen. Dies beinhaltet auch das unmittelbare Einwirken durch den Bundesnachrichtendienst, in Ansehung der vorliegenden Lage nötigenfalls auch mit kinetischen Mitteln. Die Regelung ermöglicht ein flexibles sicherheitspolitisches Krisenmanagement mittels flexibler Reaktionen auf die Notstandslage, die ihrerseits im Einzelnen unvorhersehbare Herausforderungen bereithält, denen die Bundesrepublik Deutschland mithilfe ihrer staatlichen Struktur begegnen muss.

Zu Absatz 1

Absatz 1 stellt klar, dass die Regelungen des genannten Abschnittes – hier: Abschnitt 4 (Erweiterte nachrichtendienstliche Maßnahmen) – in den Notstands- und Krisenlagen des Abschnittes 9 nur in modifizierter Form gelten. Sofern in den nachfolgenden Absätzen jeweils eigene Maßgaben vorgesehen sind, modifizieren diese die betreffenden Regelungen des Abschnittes 4.

Zu Absatz 2

Absatz 2 legt fest, dass anders als in Abschnitt 4 vorgesehen, keine spezifische Gefährdungslage festgestellt werden muss. Im Verteidigungs-, Spannungs- oder Zustimmungsfall gilt diese als vorliegend.

Zu Absatz 3

Bei Vorliegen eines Verteidigungsfalls entfällt das Erfordernis einer Grundanordnung nach § 50; eine Kontrolle der Art und des Umfangs der Maßnahmen findet durch das Bundeskanzleramt statt.

Zu Absatz 4

Das in Abschnitt 4 vorgesehene Subsidiaritätserfordernis sowie dort festgelegte Grenzen der Maßnahmen finden im Verteidigungsfall keine Anwendung. Auf einen solchen Extremfall der äußeren Bedrohungslage, der für die Bundesrepublik Deutschland unvorhersehbare Herausforderungen bereithält, muss situationsgepasst, flexibel und wirksam reagiert werden können.

Zu § 130 (Weiterverarbeitung personenbezogener Daten)

Zu Absatz 1

Absatz 1 stellt klar, dass die Regelungen des genannten Abschnittes – hier: Abschnitt 5 (Weiterverarbeitung personenbezogener Daten) – in den Notstands- und Krisenlagen des Abschnittes 9 nur in modifizierter Form gelten. Sofern in den nachfolgenden Absätzen je-

weils eigene Maßgaben vorgesehen sind, modifizieren diese die betreffenden Regelungen des Abschnittes 5.

Zu Absatz 2

Die Vorschrift regelt die materielle Voraussetzung für die Weiterverarbeitung – auch mittels automatisierter Verfahren – von personenbezogenen Daten im Rahmen der Aufklärung, Abwendung oder Einschränkung der Bedrohungslagen des § 126. Auch hier kann eine Abwägung der jeweiligen Eingriffsintensität pauschaliert und zugunsten der öffentlichen Sicherheit erfolgen: Die in Abschnitt 9 geregelten Krisenlagen sind derart existenziell, dass eine im „Normalbetrieb“ gebotene differenzierte Betrachtung der Weiterverarbeitung von personenbezogenen Daten und damit verbundenen Grundrechtseingriffen verfassungsrechtlich eine andere Gewichtung erfährt. Ist der Bestand des Staates bedroht, tritt der auf die Privatheit von Daten bezogene Grundrechtsschutz im Rahmen einer Gesamtabwägung zurück.

Zu Absatz 3

Für personenbezogene Daten, die erst nach der Feststellung des Verteidigungs-, Spannungs- oder des Zustimmungsfalls erhoben wurden, setzt die Löschüberprüfungsfrist nach Beendigung dieser Krisenlagen ein. Die Erforderlichkeit dieser personenbezogenen Daten ist nach Beendigung unverzüglich zu überprüfen, d.h. sukzessive zu bearbeiten sein. Auch diese Modifizierung dient der schnellen und effizienten Ressourcennutzung in den genannten Krisenfällen.

Zu Absatz 4

Diese Regelung dient der Verfahrensbeschleunigung und der effektiven Nutzung vorhandener Ressourcen unter Berücksichtigung der besonderen Krisenlagen, die diesem Abschnitt zugrunde liegen. Die vorübergehende Reduzierung administrativer Vorgaben stellt eine notwendige, zweckmäßige und angemessene Anpassung dar, um eine schnelle und effiziente Ressourcennutzung zu gewährleisten. Da die Protokollierungspflicht lediglich für die Dauer des Verteidigungs-, Spannungs- oder des Zustimmungsfalls ausgesetzt ist und anschließend wieder aufgenommen werden muss, wird nicht unverhältnismäßig in die Grundrechte eingegriffen.

Zu § 131 (Übermittlung von personenbezogenen Daten)

Zu Absatz 1

Absatz 1 stellt klar, dass die Regelungen des genannten Abschnittes – hier: Abschnitt 6 (Übermittlung von personenbezogenen Daten) – in den Notstands- und Krisenlagen des Abschnittes 9 nur in modifizierter Form gelten. Sofern in den nachfolgenden Absätzen jeweils eigene Maßgaben vorgesehen sind, modifizieren diese die betreffenden Regelungen des Abschnittes 6.

Zu Absatz 2 und Absatz 3

Die Modifizierungen, die mit diesen Regelungen an den Vorgaben des Abschnittes 6 vorgenommen werden, stellen die notwendige Handlungsfähigkeit im Verteidigungs-, Spannungs- oder Zustimmungsfall sicher. Die Erhöhung der militärischen und zivilen Verteidigungsbereitschaft bedingt notwendigerweise den umfassenden und zeitverzugslosen Informationsfluss zwischen den staatlichen und zivilen Akteuren im In- und Ausland. Dies gilt für den Bundesnachrichtendienst als Auslandsnachrichtendienst in besonderem Maße, sodass tatbestandlich nunmehr eine Übermittlung von personenbezogenen Daten im Rahmen der nachrichtendienstlichen Aufklärung, Abwendung oder Einschränkung der Bedrohungslagen des § 125 auf der Erforderlichkeit basiert. Auch hier kann eine Abwägung der jeweiligen Eingriffsintensität pauschaliert und zugunsten der öffentlichen Sicherheit erfolgen: Die in

Abschnitt 9 geregelten Krisenlagen sind derart existenziell, dass eine im „Normalbetrieb“ gebotene differenzierte Betrachtung der Übermittlung von personenbezogenen Daten und damit verbundenen Grundrechtseingriffen verfassungsrechtlich eine andere Gewichtung erfährt. Ist der Bestand des Staates bedroht, tritt der auf die Privatheit von Daten bezogene Grundrechtsschutz im Rahmen einer Gesamtabwägung zurück.

Die Modifizierung des Abschnittes 6 wirkt sich auch auf die die Übermittlung von Daten in Kooperationsregimen aus. Die Vorgaben der §§ 41 bis 45 verlieren dementsprechend auch ihre Bedeutung, da die Übermittlung von Daten unter Anwendung des § 131 auch außerhalb der Kooperationsregime automatisiert umfassend und zeitverzugslos möglich ist.

Zu Absatz 4 und Absatz 5

Der notwendige umfassende und zeitverzugslose Informationsfluss kann auch mittels gemeinsamer Dateien vollzogen werden, dabei gelten die Maßgaben des § 131. Unter den Voraussetzungen der Absätze 4 und 5 ist dabei auch die automatisierte Eingabe von personenbezogenen Daten in die gemeinsame Datei zulässig. Führt der Bundesnachrichtendienst die Datei, muss er zwar keine Errichtungsanordnung erstellen, aber die grundsätzlichen Bestimmungen (Bezeichnung, Zweck, beteiligte Stellen) festlegen.

Die Führung gemeinsamer Dateien nach dieser Vorschrift ist streng zweckgebunden bis zur Beendigung des Verteidigungs-, Spannungs- oder Zustimmungsfalls § 125 Absatz 3. Ist danach die Weiterführung der gemeinsamen Datei, die der Bundesnachrichtendienst führt, gewünscht, müssen die Voraussetzungen der einschlägigen Regelungen des Abschnitt 6 Unterabschnitt 4 vorliegen.

Zu § 132 (Ergänzende Bestimmungen)

Zu Absatz 1

Absatz 1 legt fest, dass im Interesse einer effektiven Nutzung vorhandener Ressourcen unter Berücksichtigung der besonderen Krisenlagen des § 125 die Vorschriften zur administrativen Kontrolle keine Anwendung finden.

Zu Absatz 2

Absatz 2 stellt klar, dass die Regelungen des genannten Abschnittes – hier: Abschnitt 7 (Ergänzende Bestimmungen und Kontrollzuständigkeiten) – in den Notstands- und Krisenlagen des Abschnittes 9 nur in modifizierter Form gelten. Sofern in den nachfolgenden Absätzen jeweils eigene Maßgaben vorgesehen sind, modifizieren diese die betreffenden Regelungen des Abschnittes 7.

Zu Absatz 3 und Absatz 4

Um die Handlungsfähigkeit des Bundesnachrichtendienstes im Verteidigungs-, Spannungs- oder im Zustimmungsfall des § 125 Absatz 3 zu erhalten, werden in diesen Fällen die bestehenden Kontrollmechanismen angepasst.

Durch diese Modifikationen werden Kapazitäten freigesetzt, die der Bundesnachrichtendienst zur Stärkung seiner Aufklärungsfähigkeiten nutzen kann. Insbesodnere wird die Einzelfallkontrolle durch eine nachträgliche Unterrichtungspflicht ersetzt bzw. im Verteidigungsfall die Vorab- und Einzelfallkontrolle vollständig aufgehoben.

In den Fällen des § 97 Absatz 2 findet bei der Feststellung der Rechtmäßigkeit die Regelung des § 129 Absatz 2 Beachtung, nach der in den besonderen Bedrohungslagen des § 125 die spezifische Gefährdungslage angenommen wird und daher keine zusätzlichen Ausführungen zur Gefährdungslage erfolgen vorgenommen werdne müssen.

Zu Absatz 5

In einem Spannungs- oder im Zustimmungsfall muss der Bundesnachrichtendienst seine Kapazitäten bündeln und kann diese nicht für die sehr zeitaufwändigen Prüfpflichten verwenden. Dies gilt nicht nur für die Mitteilungsentscheidung als solche, sondern auch für die Vorbereitung, d.h. die Prüfung, ob eine Mitteilung möglich ist und entsprechende Vorlage an den Unabhängigen Kontrollrat; beides kann bis zur Beendigung des Verteidigungs-, Spannungs- oder des Zustimmungsfalls entfallen. Im Verteidigungsfall sind die Mitteilungspflichten nicht nur vorübergehend ausgesetzt, sondern entfallen vollständig.

Zu § 133 (Besondere Bestimmungen zum Schutz der Bediensteten, Dienststellen und Verschlusssachen)

In einem Verteidigungs-, Spannungs- oder im Zustimmungsfall unterliegen die Liegenschaften und Einrichtungen, die Bediensteten und auch die Verschlusssachen des Bundesnachrichtendienstes einer ungleich höheren Gefährdungslage. So ist zu erwarten, dass andere Staaten versuchen, die Informationsgewinnung für die Bundesrepublik Deutschland zu stören oder selbst versuchen, an interne Informationen des Bundesnachrichtendienstes zu gelangen. Ein besonderer Schutz ist daher erforderlich. Aufgrund der im Vorfeld nicht im Einzelnen einschätzbaren konkreten Gefährdungssituation ist es daher erforderlich, keine schematisch abschließende Regelung zu treffen, sondern dem Bundesnachrichtendienst eine flexible Reaktion, welche durch die konkrete Bedrohung veranlasst wird, zu ermöglichen.

Der Wegfall der Lösch- und Prüfpflichten dient der effizienten Ressourcensteuerung in den besodneren Krisenlagen, vgl. dazu auch die Ausführungen zu § 131.

Zu Abschnitt 10 (Unternehmenspflichten, Anzeigepflichten, Straf- und Bußgeldvorschriften)

Zu § 134 (Kontrolle und Durchsetzung von Unternehmenspflichten)

Die Vorschrift regelt die Rechtsfolgen, die von einem (wiederholten oder intensiven) Verstoß gegen die in § 134 genannten, besonderen Pflichten ausgehen. Die Regelung ist dabei an § 183 Absatz 1 bis 3 des Telekommunikationsgesetzes angelehnt. Die ganz oder teilweise erfolgende Untersagung des Betriebs eines Unternehmens oder des Erbringens eines betreffenden Dienstes ist zur Durchsetzung der Verpflichtungen erforderlich. Um das Ziel der Durchsetzung von Verpflichtungen zu erreichen, ist es notwendig, dass sich wiederholte oder intensive Verstöße gegen die Verpflichtungen aus unternehmerischer Sicht als unwirtschaftlich erweisen.

Zu § 135 (Besondere Anzeige- und Genehmigungspflicht für ausgeschiedene Bedienstete des Bundesnachrichtendienstes)

Die Vorschrift stellt sicher, dass die in § 105 Absatz 2 bis 6 des Bundenbeamtengesetzes auch für Arbeitnehmende des Bundesnachrichtendienstes sowie für solche Beamtinnen und Beamte gelten, bei denen es sich nicht um solche mit Versorgungsbezügen oder Anspruch auf Altersgeld handelt. Von letzterer Personengruppe erfasst sind etwa Fälle, bei denen Beamtinnen oder Beamte als Folge eines Disziplinarverfahrens aus dem Dienst entfernt werden. Die besondere, sicherheitssensitive Situation ausgeschiedener Bedienste-ter bedarf insoweit einer besonderen Berücksichtigung auch im Anschluss an eine Tätig-keit beim Bundesnachrichtendienst. Entsprechend bedürfen Tätigkeiten – zeitlich befristet – einer Anzeige oder einer Genehmigung. Hierbeit ändert sich der pflichtauslösende Um-stand nicht dadurch, dass die betroffene Person in einem Beamten- oder in einem Ange-stelltenverhältnis stand. Verstöße gegen diese Pflcihten sind in § 137 bußgeldbewehrt.

Zu § 136 (Strafvorschriften)

Diese Regelung entspricht dem bisherigen § 66. Ergänzt wird mit Satz 2 ein durch konkrete Gefährdungsfolgen qualifizierter besonders schwerer Fall mit erhöhtem Strafrahmen.

Zu § 137 (Bußgeldvorschriften)

Die Bußgeldvorschrift basiert auf dem bisherigen § 67. Ein Bußgeld ist vorgesehen, wenn einem verpflichtenden Auskunftsersuchen (Nummer 1) oder einer Anordnung nach § 135 Absatz 1 Satz 2 (Nummer 2) nicht entsprochen wird. Gleiches gilt, wenn eine in diesem Zusammenhang bestehende Geheimschutzvorgabe nicht erfüllt wird (Nummern 2 und 3). Ebenfalls wurden Verstöße gegen die neu geschaffenen Anzeige- und Genehmigungspflichten für ehemalige Bedienstete des Bundesnachrichtendienstes mit eigenen Bußgeldern bewehrt.

In Absatz 2 wurde das zu verhängende Bußgeld deutlich erhöht, um dem besonderen Unrechtsgehalt der hier sanktionierten Verhaltensweisen Rechnunt zu tragen, bzw. für gewisse Tatbestände neue Bußgeldbewehrungen geschaffen.

Absatz 3 entspricht dem geltenden Recht.

Zu Abschnitt 11 (Schlussvorschriften)

Zu § 138 (Verordnungsermächtigung)

In § 139 wird eine eigene Ermächtigung für den Erlass einer Verordnung zur Übermittlung von Informationen an den Bundesnachrichtendienst (Verordnung über die Übermittlung von Auskünften an die Nachrichtendienste des Bundes) erlassen. Ermächtigungsadressaten sind auch das Bundesministerium des Innern und das Verteidigungsministerium, da aufgrund entsprechender Ermächtigungen im Bundesverfassungsschutzgesetz und MAD-Gesetz, die aber, soweit sie sich gegenständlich entsprechen, inhaltlich synchron zu gestalten sind.

Zu § 139 (Einschränkung von Grundrechten)

Die Vorschrift erfüllt das Zitiergebot nach Artikel 19 Absatz 1 Satz 2 des Grundgesetzes.

Zu § 140 (Übergangsvorschriften)

Die Übergangsvorschriften in § 141 sind erforderlich, um bereits laufende Maßnahmen angemessen einem Regelungsregime zuzuordnen.

Zu Artikel 3 (Gesetz über die Rechtskontrolle durch den Unabhängigen Kontrollrat)

Für den mit dem Gesetz zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts vom 19. April 2021 (BGBl. I S. 771) errichteten Unabhängigen Kontrollrat wird ein eigenes Stammgesetz geschaffen. Damit wird der Ausweitung der Kontrollzuständigkeit des Unabhängigen Kontrollrats auf alle Nachrichtendienste des Bundes Rechnung getragen. Die Regelung in einem eigenen Stammgesetz folgt dem Vorbild anderer Gesetze über Kontrollgremien wie das Parlamentarische Kontrollgremiumsgesetz, das Artikel 10-Gesetz oder das Bundesrechnungshofgesetz. Mit der Novellierung des BND-Gesetzes durch das Gesetz zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts vom 19. April 2021 (BGBl. I S. 771) wurde die oberste Bundesbehörde Unabhängiger Kontrollrat als Nachfolger des Unabhängigen Gremiums geschaffen. Beginnend am 1. Januar 2022 war der Unabhängige Kontrollrat sodann für die Rechtskontrolle über die technische Aufklärung des Bundesnachrichtendienstes zuständig.

Die nachrichtendienstlichen Befugnisse, die in Folge des Urteils des Bundesverfassungsgerichts aus dem Jahr 2022 zum bayerischen Verfassungsschutzgesetz neu geregelt oder angepasst werden mussten, werden entlang der Vorgaben des Bundesverfassungsgerichts mit einer effektiven Rechtskontrolle flankiert. Der Unabhängige Kontrollrat wird insoweit nunmehr die Aufgabenwahrnehmung des Bundesnachrichtendienstes und des Bundesamtes für den Verfassungsschutz auf ihre Rechtmäßigkeit hin kontrollieren. Die Rechtskontrolle des Unabhängigen Kontrollrats stellt das Bindeglied zwischen der rechtsstaatlich abgesicherten, nachrichtendienstlichen Aufgabenwahrnehmung und der politischen Kontrolle über die Tätigkeit der Nachrichtendienst dar. Eine stringente gerichtsähnliche Spruchpraxis bei umfassender Betrachtung der nachrichtendienstlichen Aufgabenwahrnehmung gewährleistet Handlungssicherheit für die Nachrichtendienste des Bundes bei ihrer zum Teil grundrechtsrelevanten Tätigkeit.

Die integrale Rechtskontrolle des Unabhängigen Kontrollrats wird aufbauend auf der zunächst für die strategische Fernmeldeaufklärung des Bundesnachrichtendienstes entwickelten Kontrollarchitektur fortentwickelt. Kernelemente dieser Kontrollarchitektur sind die beiden Kontrollsäulen der gerichtsähnlichen und der administrativen Rechtskontrolle unter dem Dach einer einheitlichen, ministerialfreien obersten Bundesbehörde.

Die gerichtsähnliche Vorabkontrolle kann in Anbetracht der verfassungsgerichtlichen Rechtsprechung klar konturiert werden. Hierbei ist – insoweit durch die verfassungsgerichtliche Rechtsprechung teilweise vorgezeichnet, vgl. BVerfG, Beschluss vom 8. Oktober 2024, 1 BvR 1743/16 u.a. – auch eine Verlagerung der Vorabkontrolle, welche bislang der G10-Kommission vorbehalten war, auf den Unabhängigen Kontrollrat angezeigt. Die Ausführungen des Bundesverfassungsgerichts zu den strukturellen Defiziten der G10-Kommission sind in ihrer Wertung auch auf die Individualbeschränkungsmaßnahmen (vormals § 3 des Artikel 10-Gesetzes) zu übertragen (hierzu umfassend und überzeugend: Friedrich in JZ 2025, S. 403ff.).

Demgegenüber folgt die administrative Rechtskontrolle einem durch den Gesetzgeber auszutarierenden Zusammenspiel bundesverfassungsgerichtlicher Vorgaben und nachrichtendienstlicher Erfordernisse. Bei diesen Erfordernissen ist das Leitbild des Geheimschutzes und der Vermeidung von informatorischen Schnittstellen zum einen zwischen dem jeweiligen Nachrichtendienst und der Kontrollbehörde aber auch potenziell von der Kontrollbehörde zu weiteren Kontrollbehörden tragend. Bereits der Anschein, dass nachrichtendienstliche Informationsbeschaffung und Methoden durch verschiedenste Hände gehen (müssen), beschädigt die Glaubwürdigkeit der Nachrichtendienste im notwendigen internationalen Verbund nachrichtendienstlicher Zusammenarbeit. Der Unabhängige Kontrollrat gewährleistet mithin nicht eine bloße integrale Rechtskontrolle über die nachrichtendienstliche Befugnisausübung und deren Kopplung an die parlamentarische Kontrolle. Vielmehr bietet die einheitliche behördliche Struktur anhaltend Gewähr für die Sicherstellung der Auftragserfüllung der Nachrichtendienste des Bundes.

Die Schaffung einer integralen Rechtskontrolle über die Aufgabenwahrnehmung von Bundesnachrichtendienst und Bundesamt für Verfassungsschutz begegnet zudem dem wiederholt festgestellten Zustand der Zersplitterung der Kontrolle. Diese einheitliche Struktur führt zu einem effektiveren Grundrechtsschutz, da zunehmend auch das Zusammenfallen nachrichtendienstlicher Befugnisausübungen einer Verhältnismäßigkeitsprüfung unterzogen werden kann. Der bisherige Zustand gedoppelter Kontrollstrukturen wird ebenfalls beendet. Neben einem Kontrollmehrwert durch eine einheitliche gerichtsähnliche und administrative Rechtskontrolle aus einer Hand werden zudem die Ressourcen der Nachrichtendienste des Bundes geschont, die bislang teilweise in erheblichem Maße mit Doppelkontrollen belastet sind, ohne dass die doppelten Kontrollstrukturen einen rechtsstaatlichen Mehrwert geboten hätten. Dieser Umstand und die hiermit verbundene Stärkung der Kontrolle durch einen integralen Ansatz ist es auch, weshalb die Zuständigkeit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Bereich der nachrichtendienstlichen Kontrolle nunmehr auf das administrative Kontrollorgan übergeht. Insoweit wird dem vielfach

geäußerten Vorschlag einer gebündelten Kontrolle entsprochen (vgl. Höning, Externe Rechtskontrolle der Nachrichtendienste, S. 267ff. dort freilich mit dem Vorschlag einer gegenläufigen Zuständigkeitsverlagerung).

Die neu geschaffene Möglichkeit, dass neben den sechs richterlichen Mitgliedern nunmehr auch zwei nicht-richterliche Mitglieder in das gerichtsähnliche Kontrollorgan aufgenommen werden können, soll – in Entsprechung der Vorgaben des Bundesverfassungsgerichts (BVerfG 1 BvR 2835/17, Rn. 286) – eine Öffnung des Kontrollorgans bewirken. Hierdurch sollen Erfahrungen und Perspektiven aus anderen juristischen Berufen Eingang in das gerichtsähnliche Kontrollorgan finden. Dabei ist durch das Verhältnis von richterlichen (sieben) zu nichtrichterlichen (zwei) Mitgliedern zugleich sichergestellt, dass der richterlichen Perspektive ein maßgebliches Gewicht zukommt.

Neben der Ausweitung der Kontrollzuständigkeit des Unabhängigen Kontrollrats bilden klarstellende Anpassungen zur behördlichen Ausgestaltung und dabei insbesondere zum Verhältnis von gerichtsähnlichem und administrativem Kontrollorgan sowie zur Rolle der Mitglieder des Senats beim Unabhängigen Kontrollrat einen weiteren wesentlichen Bestandteil des Gesetzes.

Zu Abschnitt 1 (Unabhängiger Kontrollrat und Aufgaben)

Zu § 1 (Unabhängiger Kontrollrat)

Die Stellung des Unabhängigen Kontrollrats bleibt grundsätzlich unverändert, vgl. den bisherigen § 41 Absatz 1 des BND-Gesetzes. Der Unabhängige Kontrollrat ist eine ministerialfreie oberste Bundesbehörde, die der Exekutive zugeordnet ist. Zur Wahrung der Unabhängigkeit des Unabhängigen Kontrollrats muss er weisungsfrei sein. Der Unabhängige Kontrollrat verfügt institutionell („unabhängige oberste Bundesbehörde“) und bezogen auf die Mitglieder des gerichtsähnlichen Kontrollorgans (§ 15) über eine aufgaben- und funktionsbezogen umfassend gesicherte Unabhängigkeit.

Zu § 2 (Aufgaben des Unabhängigen Kontrollrats)

Zu Absatz 1

In Absatz 1 wird die Grundaufgabe des Unabhängigen Kontrollrats beschrieben: Er kontrolliert die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten durch die Nachrichtendienste des Bundes bei der Wahrnehmung der im Rahmen der jeweiligen Fachgesetzen geregelten Aufgaben. Hierbei ist die Kontrolle auf die Wahrung der Grundrechte der Betroffenen auszurichten und gilt der Sicherung und praktischen Effektivierung der rechtlichen Grenzen der staatlichen Überwachungstätigkeit (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 272).

Damit ist, dem Regelungsgehalt der nachrichtendienstlichen Fachgesetze entsprechend, eine Prüfung der Bestimmungen verbunden, welche die Erhebung, Weiterverarbeitung und Übermittlung von personenbezogenen Daten regeln. Dies korrespondiert mit der Eingriffsdimension „staatliche Überwachungstätigkeit“, die letztlich auf die Verarbeitung von personenbezogenen Daten gerichtet ist. Dies betrifft dabei auch die Anwendung einer Befugnis (also sowohl des versuchten wie des abgeschlossenen Einsatz) für nachrichtendienstliche Mittel, deren Eingriffslast sich aus den besonderen Umstände der Maßnahme ergibt (wie etwa einer längerfristigen Observation oder einer längerfristigen Standortbestimmung), da – gerade – auch hier die staatliche Überwachung darauf gerichtet ist, umfangreiche Informationen (d.h. personenbezogene Daten) zu Personen zu gewinnen. Die verfahrenssichernden Vorgaben der Fachgesetze, besondere Einschränkungen für geschützte Personen, Beschränkungen in den Zeiträumen, Weiterverarbeitungs- und Übermittlungsbestimmungen, Protokollierungs- und Kennzeichnungspflichten etc. sind letztlich allesamt Vorgaben, welche die Verarbeitung von personenbezogenen Daten betreffen und unterliegen dergestalt der Kontrolle durch den Unabhängigen Kontrollrat. Gegenstand der Kontrolle ist

insbesondere auch, ob es sich bei bestimmten Daten um solche mit Personenbezug handelt oder nicht.

Die Prüfung erfolgt also darauf, ob die nachrichtendienstlichen Maßnahmen und die hiervon ausgehende und die sich hieran anschließende Verarbeitung von personenbezogenen Daten den gesetzlichen Bestimmungen entsprechen und den Verhältnismäßigkeitsgrundsatz wahren. Erstmals wird damit die Aufgabenwahrnehmung von Bundesnachrichtendienst und Bundesamt für Verfassungsschutz einer einheitlichen integralen Rechtskontrolle durch eine unabhängige oberste Bundesbehörde unterworfen.

Lediglich klarstellend sei darauf hingewiesen, dass die Einhaltung der Vorschriften über die Informationserhebung (bzw. der grundrechtsrelevanten Untermenge der Erhebung von personenbezogenen Daten) im Rahmen der nachrichtendienstlichen Auftragsdatenverarbeitung (all)umfassend in der Prüftätigkeit des Unabhängigen Kontrollrats aufgeht. Erfasst sind also auch mögliche Eingriffe in Artikel 13 des Grundgesetzes wie in andere Grundrechte, wenn dies Teil des Erhebungs- (bzw. Verarbeitungsprozesses insgesamt) ist. Damit übernimmt der Unabhängigen Kontrollrat künftig die Rolle des (einzigen) behördlichen Kontrollorgans über die Tätigkeit der Nachrichtendienste und vereint damit die datenschutzrechtliche Kontrolle, die vormals der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vorbehalten war, sowie die auftragsbezogenen Kontrolltätigkeiten der G10-Kommission (vgl. zu der bereits seit längerem erhobenen Forderung, eine einheitliche Kontrolle zu schaffen, ausführlich: Höning, Externe Rechtskontrolle der Nachrichtendienste, S. 267ff.).

Zu Absatz 2

Die Rechtskontrolle durch den Unabhängigen Kontrollrat gliedert sich in grundsätzlich drei Bereiche. Hierbei handelt es sich um die Vorabkontrolle und Einzelfallkontrolle, die dem gerichtsähnlichen Kontrollorgan vorbehalten ist (geregelt in Abschnitt 3 Unterabschnitt 1) und die administrative Kontrolle, die durch das administrative Kontrollorgan erfolgt (Abschnitt 3 Unterabschnitt 2). In den Fällen der Vorabkontrolle und der Einzelfallkontrolle obliegt es den Nachrichtendiensten des Bundes, den Kontrollvorgang durch eine Vorlage zu initiieren. Demgegenüber finden in den Fällen der administrativen Kontrolle, die als datenschutzrechtliche Strukturkontrolle über die Tätigkeiten der Nachrichtendienste des Bundes ausgestaltet ist, eine selbst initiierte Prüfung durch das administrative Kontrollorgan anhand des Prüfprogrammes statt.

Zu Absatz 3

Der Unabhängige Kontrollrat wird bei den Verfahren der Errichtungsanordnungen (vormals: Dateianordnungen) von den Nachrichtendiensten des Bundes nach Maßgabe der in Absatz 3 genannten fachgesetzlichen Bestimmungen angehört. Dieses Anhörungsverfahren, welches bislang dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zufiel, geht zuständigkeitshalber nun an den Unabhängigen Kontrollrat. Es komplettiert die integrale Kontrolle durch den Unabhängigen Kontrollrat über die Aufgabenwahrnehmung der Dienste und wirkt der Zuständigkeitszersplitterung entgegen. In materieller Hinsicht bleibt das Anhörungsverfahren unverändert erhalten.

Zu Absatz 4

Mit der einheitlichen Rechtskontrolle über Bundesnachrichtendienst und Bundesamt für Verfassungsschutz und der damit verbundenen, systematischen Berichtslegung über die Kontrollausübung gegenüber dem Parlamentarischen Kontrollgremium unterstützt der Unabhängige Kontrollrat die parlamentarische Kontrolle. Diese gegenüber der bisherigen Regelung im BND-Gesetz erfolgte Ergänzung ist klarstellender Natur und entspricht der vergleichbaren Regelung in § 1 Satz 2 des Bundesrechnungshofgesetzes.

Die Unterstützungsfunktion lässt dabei die gesetzlich verankerte Unabhängigkeit des Unabhängigen Kontrollrats unangetastet. Der Unabhängige Kontrollrat wird dadurch nicht zu einem Hilfsorgan des Parlaments, vielmehr bildet die Rechtskontrolle das Scharnier zwischen der effektiven Aufgabenwahrnehmung der Nachrichtendienste und der rechtstaatlich gebotenen parlamentarischen Kontrolle. Das zentrale Element dieser Unterstützungsleistung sind die Berichte, die der Unabhängige Kontrollrat dem Parlamentarischen Kontrollgremium vorzulegen hat. Über die Berichtspflichten hinaus, unterstützt der Unabhängige Kontrollrat das Parlamentarische Kontrollgremium zudem auch bedarfsabhängig zu allgemeinen Angelegenheiten seiner Tätigkeit. Dies kann durch schriftliche Gutachten oder mündliche Ausführungen im Rahmen von Sitzungen auf entsprechende Bitten des Parlamentarischen Kontrollgremiums erfolgen. Grundsätzlich steht es dem Parlamentarischen Kontrollgremium dabei frei, die Form der jeweiligen Unterstützungshandlung zu wählen.

Zugleich ist das Zusammenwirken auf Unterstützungshandlungen „beschränkt“, was insbesondere auch weiterhin die Beachtung der Third Party Rule sichert. Denn während der Unabhängige Kontrollrat durch diese nicht in seiner Kontrolltätigkeit beschränkt ist, gilt die Third Party Rule gegenüber dem parlamentarischen Raum.

Im Rahmen der unabhängigen Rechtskontrolle des Unabhängigen Kontrollrates darf er nicht durch die Geltung der Third Party-Rule beschränkt werden. Im Gegensatz zur Fachaufsicht von Bundeskanzleramt, Bundesministerium des Innern, sowie Bundesverteidigungsministerium über die ihrem jeweiligen Geschäftsbereich unterfallenden Nachrichtendienste ist eine Kontrolle über Zweckmäßigkeit der Tätigkeit der Nachrichtendienste nicht mit der Rechtskontrolle durch den Unabhängigen Kontrollrat verbunden. Von der Rechtskontrolle zu unterscheiden ist weiterhin die einen anderen Charakter aufweisende, parlamentarische Kontrolle (BVerfG Urteil vom 19. Mai 2020, 1 BvR 2836/17, Rn. 298), da die Geheimhaltung im parlamentarisch-politischen Umfeld faktischen Grenzen unterliegt, weshalb die Third Party Rule dort zu beachten bleibt. Unter Berücksichtigung dieser Unterschiedlichkeit der Kontrollausübung muss der Unabhängige Kontrollrat dem Parlamentarischen Kontrollgremium regelmäßig über seine Kontrolltätigkeit berichten (BVerfG Urteil vom 19. Mai 2020, 1 BvR 2836/17, Rn. 298). Die Kontrolle durch das Parlamentarische Kontrollgremium „hat eine eigene, nicht speziell auf die Rechts- und Grundrechtskontrolle begrenzte Funktion und ist Ausdruck der allgemeinen parlamentarischen Verantwortung für die sachgerechte und politisch angemessene Aufgabenwahrnehmung der Exekutive.“ (BVerfG Urteil vom 19. Mai 2020, 1 BvR 2836/17, Rn. 300).

Zu § 3 (Zuständigkeit; Anwendbarkeit des Bundesdatenschutzgesetzes)

§ 3 grenzt im Absatz 1 die Zuständigkeit des Unabhängigen Kontrollrats von der der Bundesbeauftragten oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (angelehnt an § 28 Absatz 2 Satz 2 des bisherigen Bundesverfassungsschutzgesetzes) ab.

Absatz 2 nimmt Verarbeitungen, die im Rahmen der Rechtskontrolle des Unabhängigen Kontrollrats vorgenommen werden, durch Verweis auf die im Bundesdatenschutzgesetz für die justizielle Tätigkeit von Bundesgerichten geltende Regelung von der Aufsicht der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit aus. Insoweit ist auch für die (unabhängige) administrative Kontrolle – welche gerade die Zuständigkeit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für die Nachrichtendienste des Bundes übernimmt – keine „Rückkontrolle“ geboten. Eine solche würde zudem auch erneut Abgrenzungsschwierigkeiten nach sich ziehen.

Zu Abschnitt 2 (Organisation und behördlicher Aufbau des Unabhängigen Kontrollrats)

Zu Unterabschnitt 1 (Organisation des Unabhängigen Kontrollrats)

Zu § 4 (Sitz)

Der Unabhängige Kontrollrat hat seinen Dienstsitz in Berlin. Um den unterschiedlichen Dienstsitzen und Außenstellen von Bundesnachrichtendienst und Bundesamt für Verfassungsschutz Rechnung zu tragen, kann der Unabhängige Kontrollrat im Bedarfsfall auch Außenstellen (insbesondere etwa in Köln) einrichten.

Gegenüber der bisherigen Regelung in § 41 Absatz 6 des BND-Gesetzes wird demgegenüber darauf verzichtet, einen zweiten Dienstsitz (Pullach) vorzuschreiben. Die Entwicklung des Dienstsitzes in Pullach wurde durch den Unabhängigen Kontrollrat zugunsten des Behördenaufbaus bislang zurückgestellt, sodass die Aufgabe des Dienstsitzes in Pullach nicht mit einem Rückbau oder anderweitigen organisatorischen Fragen von Gewicht verbunden ist.

Zu § 5 (Aufbau)

Der Unabhängige Kontrollrat besteht aus einem gerichtsähnlichen und einem administrativen Kontrollorgan. Gegenüber der bisherigen Regelung des § 40 Absatz 1 des BND-Gesetzes erfolgt insoweit eine Klarstellung zur behördlichen Grundstruktur. Ähnlich wie in der Regelung des Bundesrechnungshofgesetzes wird eine zwingende Grundstruktur der Behörde vorgegeben, die freilich durch die Geschäftsordnung ergänzt wird (vgl. NomosBR/Erb BRHG/Horst Erb, 1. Aufl. 2012, BRHG § 2 Rn. 1-2).

Beide Kontrollorgane sind gleichermaßen Teil des Unabhängigen Kontrollrats, üben aber eine unterschiedliche Funktion aus. Dem gerichtsähnlichen Kontrollorgan obliegt die Vorabkontrolle eingriffsintensiver nachrichtendienstlicher Maßnahmen sowie eine (nachträgliche) Einzelfallkontrolle in gesetzlich bestimmten Fällen. Darüber hinaus bestimmt das gerichtsähnliche Kontrollorgan den Rahmen der strukturellen Kontrolle durch das administrative Kontrollorgan, indem der Senat des gerichtsähnlichen Kontrollorgans ein Prüfprogramm beschließt (vgl. § 26). Dem administrativen Kontrollorgan obliegt demgegenüber die Ausübung der strukturellen datenschutzrechtlichen Kontrolle, soweit diese zuvor im Zuständigkeitsbereich der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit lag. Entlang der Unterscheidung von gerichtsähnlichem und administrativem Kontrollorgan erfolgt die differenzierte Ausübung der Rechtskontrolle, die in den jeweiligen Zuständigkeitsregelungen konkretisiert wird.

In Absatz 2, der dem § 2 Absatz 2 des Bundesrechnungshofgesetzes nachgebildet ist, findet sich die Maßgabe, dass auch im Unabhängigen Kontrollrat eine Präsidialabteilung vorgesehen und mit den Angelegenheiten der Verwaltung betraut ist.

Zu § 6 (Prüfung der Haushalts- und Wirtschaftsführung)

Die Regelung entspricht dem bisherigen § 41 Absatz 4 des BND-Gesetzes und wurde um die Berücksichtigung von Geheimschutzbelangen ergänzt.

Zu § 7 (Leitung des Unabhängigen Kontrollrats)

Zu Absatz 1

Die Regelung bestimmt die Leitung des Unabhängigen Kontrollrat und wie die Präsidentin oder der Präsident im Falle seiner Verhinderung vertreten wird, wobei die untergesetzliche Ausgestaltung weiterer Stufen der Vertretung (z.B. durch das jeweils dienstälteste Mitglied

des Senats beim Unabhängigen Kontrollrat) unbenommen bleibt. Zudem wird der Begriff der Behördenleitung legaldefiniert.

Zu Absatz 2

Die Regelung ist unter Anpassung an die Systematik („Behördenleitung“) an den bisherigen § 41 Absatz 2 Satz 2 des BND-Gesetzes angelehnt. Der bisherige § 41 Absatz 2 Satz 3, der lediglich Selbstverständliches ausdrückte (dass die Behördenleitung auch die Verwaltung des Unabhängigen Kontrollrats leitet, bedarf keiner Regelung), konnte entfallen.

Zu Absatz 3

Absatz 3 ermöglicht, Verwaltungsaufgaben auf Mitglieder des Unabhängigen Kontrollrats zu delegieren, soweit diese damit einverstanden sind und sie dadurch nicht in ihrer Haupttätigkeit beeinträchtigt werden und ihre Unabhängigkeit gewährleistet ist. Die Regelung ist an § 6 Absatz 3 des Bundesrechnungshofgesetzes angelehnt. Die Unterstützung bezieht sich grundsätzlich auf Verwaltungsangelegenheiten, vgl. Nomos-BR/Erb BRHG, § 6 Rn. 2. Die Regelung ermöglich klarstellend eine Aufteilung der Verwaltungsaufgaben mit dem Ziel der Sicherstellung einer funktionalen Aufgabenteilung und -erfüllung. Hierunter kann z.B. die Bestimmung einer oder eines Verantwortlichen für den Haushalt fallen. Die Ausgestaltung dieser Möglichkeit bleibt der Selbstorganisation vorbehalten. Die Verantwortlichkeit der Präsidentin oder der Präsident für die Leitung der Verwaltung bleibt davon unberührt.

Zu Absatz 4

Der Behördenleitung wird in Absatz 4 auch die Möglichkeit eingeräumt, in Einzelfragen eine Entscheidung des Senates des gerichtsähnlichen Kontrollorgans auch zu Angelegenheiten der behördlichen Verwaltung zu befassen oder ihn hierzu anzuhören. Dabei bleibt es der Behördenleitung offen, ob sie den Senat „nur“ anhören möchte – ohne dass damit eine bindende Entscheidung verbunden wäre – oder der Senat eine verbindliche Entscheidung (im Rahmen einer „Befassung“) treffen soll. Letzteres kann insbesondere dann tunlich sein, wenn eine behördlich bedeutsame Frage mit größtmöglicher Akzeptanz entschieden werden soll.

Zu § 8 (Geschäftsordnung)

Zur verbesserten Nachvollziehbarkeit und Regelungsklarheit werden Geschäftsordnung und die Verfahrensordnung nun in einer jeweils eigenen Norm geregelt. Die Ausgestaltung von Geschäfts- und Verfahrensordnung durch den Senat selbst sichert – entsprechend den Vorgaben des Bundesverfassungsgerichts (BVerfGE 1 BvR 2835/17, Leitsatz 8) – die Unabhängigkeit der Behörde sowie dessen Verfahrensautonomie. Die bisherige Regelung zur Geschäftsordnung in § 41 Absatz 5 Nummer 1 des BND-Gesetzes hat sich in der Praxis als zu unspezifisch, insbesondere in Abgrenzung zur Verfahrensordnung, erwiesen und wird mithin konkretisiert (vgl. z.B. Hoch/Schmidt-Räntsch/Brunst, NVwZ 2023, 712 (714, 717).

Zu Absatz 1

Die Regelungsgegenstände aus § 41 Absatz 5 Satz 1 Nummer 1 und Satz 3 des BND-Gesetzes werden im Absatz 1 zusammengefasst. Zudem wird die Regelung unter Berücksichtigung der erweiterten Zuständigkeit um die Notwendigkeit einer Anhörung des Bundesministeriums des Innern sowie des Bundesministeriums der Verteidigung ergänzt. Die Regelung zum Verfahren bei Stimmengleichheit des § 41 Absatz 5 Satz 4 des BND-Gesetzes wurde wegen Redundanz mit Blick auf die allgemeine Regelung zu den Kollegialspruchkörpern des gerichtsähnlichen Kontrollorgans (§ 23 Absatz 5) gestrichen.

Zu Absatz 2

In Absatz 2 wird die bislang in § 41 Absatz 5 Satz 2 des BND-Gesetzes enthaltende Vorgabe zum Geheimschutz geregelt, sprachlich verbessert und aus Gründen der Rechtsklarheit in einem eigenen Absatz verankert.

Zu Absatz 3

Die bisherige Regelung des § 41 Absatz 5 Satz 5 des BND-Gesetzes wurde unverändert übernommen und aus Gründen der Rechtsklarheit in einem eigenen Absatz verankert.

Zu § 9 (Verfahrensordnung)

Die Regelungen zur Verfahrensordnung, die bisher gemeinsam mit den Regelungen zur Geschäftsordnung in § 41 Absatz 5 des BND-Gesetzes verankert war, werden nunmehr in einer eigenen Norm verortet.

Zu Absatz 1

Die Regelung zum Erlass einer Verfahrensordnung sowie zur Anhörung des Bundeskanzleramtes waren bislang in § 41 Absatz 5 Satz 1 und Satz 3 des BND-Gesetzes geregelt und werden im Absatz 1 nunmehr zusammengefasst. Die Regelung zum Verfahren bei Stimmengleichheit wurde wegen Redundanz mit Blick auf die allgemeine Regelung zu den Kollegialspruchkörpern des gerichtsähnlichen Kontrollorgans (§ 23 Absatz 5) gestrichen.

Zu Absatz 2

Eingeführt wird die Vorgabe, dass die Verfahrensordnung die Einzelheiten des Verfahrensablaufs bei der Durchführung der Rechtskontrolle vorsieht. Diese Klarstellung soll bisher bestehenden Abgrenzungserschwernissen gegenüber der Geschäftsordnung abhelfen und die Abläufe der konkreten Kontrolltätigkeit des Unabhängigen Kontrollrats festlegen.

Zu Absatz 3

In Absatz 3 wird die bislang in § 41 Absatz 5 Satz 2 des BND-Gesetzes enthaltende Vorgabe zum Geheimschutz geregelt und aus Gründen der Rechtsklarheit in einem eigenen Absatz verankert.

Zu Absatz 4

Absatz 4 übernimmt die Regelungsinhalte des bisherigen § 41 Absatz 5 Satz 6 des BND-Gesetzes, um nunmehr für die Kontrolle von Bundesnachrichtendienst und Bundesamt für Verfassungsschutz eine verbesserte Nachvollziehbarkeit der Kontrolle des Unabhängigen Kontrollrats für das Parlamentarische Kontrollgremium und somit eine Stärkung der parlamentarischen Kontrolle zu erreichen.

Zu § 10 (Geschäftsverteilung)

Zu Absatz 1

Nach Absatz 1 ist es Aufgabe des Senates, einen Geschäftsverteilungsplan zu erlassen. Das Kollegialorgan Senat wird so in die Grundentscheidung über die Arbeitsorganisation eingebunden. Die Mitglieder des gerichtsähnlichen Kontrollorgans, die den Senat bilden, stellen mithin ein Kollegium, welches sich auf die wesentlichen Auslegungsfragen verständigt. Die Rolle der oder des Mitglieds des gerichtsähnlichen Kontrollorgans erfährt hierdurch eine umfassendere Einbindung und somit eine Stärkung.

Zu Absatz 2

Die neu eingeführte Zuweisung von thematischen Schwerpunkten ermöglicht eine vertiefte Befassung mit den Themen z.B. der technischen Aufklärung durch einzelne Mitglieder des gerichtsähnlichen Kontrollorgans und wurde auch vor dem Hintergrund des Aufgabenzuwachs für den Unabhängigen Kontrollrat eingeführt. Für die konkrete Festlegung der jeweiligen Themen bestehen keine Vorgaben, der Unabhängige Kontrollrat kann insofern flexibel auf seinen Bedarf eingehen. Es können sowohl inhaltliche als auch z.B. regionale Schwerpunkte unterschiedlicher Reichweite gesetzt werden. Die Regelung soll weiterhin die Interaktion zwischen dem gerichtsähnlichen Kontrollorgan und dem administrativen Kontrollorgan befördern. Die Regelung ist unter Berücksichtigung der Besonderheiten des Unabhängigen Kontrollrats an die entsprechende Regelung des § 7 des Bundesrechnungshofgesetzes angelehnt.

Zu Unterabschnitt 2 (Rechte und Pflichten der Bediensteten des Unabhängigen Kontrollrats)

Zu § 11 (Deutsche Staatsangehörigkeit; Sicherheitsüberprüfung)

Zu Absatz 1

Die Regelung wählt gegenüber dem bisherigen § 53 erster Fall des BND-Gesetzes einheitlich den Begriff der Bediensteten des Unabhängigen Kontrollrats. Dieser umfasst sowohl die Mitglieder des gerichtsähnlichen Kontrollorgans als auch alle weiteren, im Unabhängigen Kontrollrat tätigen Personen. Letztere werden als Mitarbeiterinnen und Mitarbeiter des Unabhängigen Kontrollrats bezeichnet.

Zu Absatz 2

Die Regelung des bisherigen § 53 zweiter Fall des BND-Gesetzes zur Sicherheitsüberprüfung wurde mit der Regelung des bisherigen § 43 Absatz 2 des BND-Gesetzes zusammengeführt und gilt einheitlich für alle Bediensteten des Unabhängigen Kontrollrats. Dabei wird ergänzend klargestellt – dies entspricht insoweit ohnehin den Vorgaben des Sicherheitsüberprüfungsgesetzes, vgl. § 2 Absatz 1 Satz 1 SÜG –, dass die Sicherheitsüberprüfung vor Aufnahme der Tätigkeiten durchzuführen ist. Durch den in Satz 2 neu hinzugekommenen Verweis auf § 15 des Sicherheitsüberprüfungsgesetzes wird klargestellt, dass die dort enthaltene Ausnahme auch bei den Bediensteten des Unabhängigen Kontrollrats Anwendung findet.

Zu § 12 (Geheimhaltung; Aussagegenehmigung)

Zu Absatz 1

Die Regelung entspricht dem bisherigen § 54 Absatz 2 des BND-Gesetzes.

Als unabhängige oberste Bundesbehörde kommt dem Unabhängigen Kontrollrat neben seiner Funktion in der Rechtskontrolle auch eine Rolle beim öffentlichen sicherheitsrechtlichen Diskurs zu. Die Geheimhaltungspflicht wirkt hierauf zwar begrenzend, hindert diese jedoch nicht. Das Einbringen in sicherheitspolitische Diskurse stärkt die Sichtbarkeit der Rechtskontrolle und das gesellschaftliche Vertrauen in diese und steht der Regelung in Absatz 1 nicht entgegen.

Zu Absatz 2

Die Regelung entspricht weitgehend dem bisherigen § 54 Absatz 3 des BND-Gesetzes, wobei klargestellt wird, dass die Behördenleitung entscheidet (im bisherigen Recht war insoweit nur der Präsident bzw. die Präsidentin genannt. Über die Erteilung einer Aussagegenehmigung für die Präsidentin oder den Präsidenten entscheidet die Vizepräsidentin oder

der Vizepräsident. Für Verhinderungsfälle bleibt dem Unabhängigen Kontrollrat unbenommen, untergesetzliche Vertretungsregelungen zu statuieren. Die Ergänzung zum Einvernehmen im Falle der Beteiligung weiterer Stellen entspricht § 44d Absatz 2 des Abgeordnetengesetzes. Ergänzungen zum bisherigen § 54 Absatz 3 des BND-Gesetzes wurden eingefügt, um auch den Unabhängigen Kontrollrat in geheimhaltungsbedürftige Angelegenheiten einzubeziehen, an denen er beteiligt war. Zudem wurde der Maßstab klargestellt, anhand dessen das Einvernehmen zu erteilen ist. Schließlich wurde ein Erfordernis zur schriftlichen Begründung etabliert.

Zu Unterabschnitt 3 (Befugnisse im Zusammenhang mit der Rechtskontrolle)

Zu § 13 (Befugnisse des Unabhängigen Kontrollrats)

Die in § 13 explizit geregelten „Befugnisse des Unabhängigen Kontrollrats“ regeln lediglich besondere Befugnisse, welche über die im Rahmen einer kontrollierenden Tätigkeit bereits immanenten Rechte hinausgehen (zum Vergleich: Im Bundesrechnungshofgesetz ist eine gesonderte Regelung von Befugnissen nicht vorgesehen). Unabhängig davon bleibt es den Nachrichtendiensten des Bundes auch unbenommen, im Einzelfall über die Maßgaben des § 13 hinausgehende Informationsersuchen des Unabhängigen Kontrollrats zu erfüllen.

§ 13 greift die Regelung des bisherigen § 56 BND-Gesetz auf, bereinigt diese indes in mehrerer Hinsicht um normativen Ballast und unklaren Vorgaben. Eine Verminderung der Kontrolldichte geht von diesen Änderungen nicht aus.

Um Missverständnissen im Zusammenhang mit dem Begriff der „Unterstützung“ vorzubeugen, wurde auf die bisherige Regelung des § 56 Absatz 1 des BND-Gesetzes verzichtet. An der Verpflichtung, dem Unabhängigen Kontrollrat die Verwirklichung seiner Befugnisse zu ermöglichen, ändert sich nichts. Dies betrifft insoweit nicht nur die „Unterstützung bei der Kontrolltätigkeit im engeren Sinne“, sondern auch die notwendigen Maßnahmen (wie z.B. die verhältnismäßige zur Verfügung Stellung von Ausstattung und Räumlichkeiten), um die Aufgabenerfüllung des Unabhängigen Kontrollrats zu ermöglichen.

Entfallen ist der bisherige § 56 Absatz 1 Satz 3 des BND-Gesetzes. Nach diesem war „Verlangen des Unabhängigen Kontrollrats unverzüglich zu entsprechen“. Dabei war schon die Verortung in Absatz 4 missverständlich, da nicht hinreichend klar wurde, auf welches Verlangen sich diese Pflicht erstreckte (insbesondere, ob auch Absatz 2 und 3 hiervon erfasst waren). Darüber hinaus war die Regelung redundant, da ein Tätigwerden gegenüber der Kontrollbehörde „ohne schuldhaftes Zögern“ keinerlei gesetzlichen Anordnung bedarf, sondern bereits für sich genommen selbstverständlich ist. Die explizite gesetzliche Regelung führt demgegenüber lediglich zu dem (falschen) Schluss, dass eine unbedingte Priorisierung vor allen anderen Aufgaben zu erfolgen habe. Dies ist nicht intendiert; vielmehr hat eine sachgerechte Abwägung zu der Wahrnehmung der sonstigen gesetzlichen Behördenaufgaben zu erfolgen. Bei Kollisionslagen zwischen wirksamer Aufgabenwahrnehmung und wirksamer Kontrolle (etwa hinsichtlich der Ressourcensteuerung) ist ein sachgerechter Ausgleich im Einzelfall nötig.

Zudem ist das „individuelle Fragerecht“ des § 56 Absatz 4 Satz 1 des BND-Gesetzes weggefallen (hierzu näher bei der Begründung zu Absatz 3).

Zu Absatz 1

Die Regelung entspricht im Wesentlichen dem bisherigen § 56 Absatz 2 des BND-Gesetzes. Der Unabhängige Kontrollrat kann, soweit seine Kontrollzuständigkeit reicht, von dem jeweiligen Nachrichtendienst verlangen, Akten oder andere in amtlicher Verwahrung befindliche Schriftstücke, soweit im Einzelfall ein berechtigtes Interesse besteht auch im Original, und in Dateien gespeicherte Daten zur Verfügung zu stellen. Dieses zur Verfügung stellen erfolgt an einer Dienststelle des Nachrichtendienstes. Die geeignete Dienststelle wird vom jeweiligen Nachrichtendienst benannt. Diese Benennung darf nicht der Befugnis

des Unabhängigen Kontrollrats zuwiderlaufen. D.h. eine Benennung von Dienststellen, die missbräuchlich ist oder die Kontrolltätigkeit zu beeinträchtigen geeignet ist, ist ausgeschlossen. Unabhängig von einer Übersendungspflicht – welche nicht besteht – bleibt es den Nachrichtendiensten des Bundes aber unbenommen, Daten oder Schriftstücke dann an den Unabhängigen Kontrollrat zu übersenden, wenn aus Sicht des jeweiligen Nachrichtendienstes hiervon keine Sicherheitsrisiken ausgehen oder anderweitige Gründe entgegenstehen.

Zu Absatz 2

Hier findet sich der Regelungsinhalt des § 56 Absatz 3 des BND-Gesetzes. Die Einschränkung, dass Zutritt oder Zugang nur in dem die Ausübung der Kontrolle erforderlichen Rahmen zu gewähren ist, bezieht sich dabei nicht auf einen konkreten Vorgang, sondern auf die Kontrolltätigkeit insgesamt.

Die „Erforderlichkeit“ bezieht sich insoweit darauf, dass die Kontrolle nicht durch ein „milderes“, d.h. in (arbeits-)ökonomischer Hinsicht für die Verwaltung im Allgemeinen und die Nachrichtendienste des Bundes im Speziellen, weniger belastendes Mittel möglich ist. Hierbei wird im Rahmen der praktischen Anwendung insbesondere zu berücksichtigen sein, dass der Unabhängigen Kontrollrat zwar grundsätzlich auch befugt ist, Dienststellen der Nachrichtendienste des Bundes im Ausland in seine Kontrolle mit einzubeziehen. In diesem Fall ist indes in besonderem Maße sicherzustellen, dass eine solche Kontrolle „erforderlich“ – also insbesondere auch nicht in gleich geeigneter Weise vom Inland aus möglich – ist.

Zu Absatz 3

Die bisherige Regelung des § 56 Absatz 4 Satz 1 des BND-Gesetzes wurde übernommen, dabei indes insoweit geändert, dass nicht länger auf ein „individuelles“ Fragerecht gegenüber Mitarbeiterinnen und Mitarbeitern der Nachrichtendienste des Bundes abgestellt wird. Es ist Aufgabe des zu kontrollierenden Nachrichtendienstes, die Informationen auf geeignetem Wege (etwa auch durch Benennung entsprechend sachkundiger Mitarbeiter) zur Verfügung zu stellen.

Mit dieser Änderung geht keine Verminderung der Kontrolldichte einher: Der Kontrolle durch den Unabhängigen Kontrollrat unterliegt der jeweilige Nachrichtendienst. Entsprechend ist auch dessen Auskunft einzuholen. Eine Regelung individualisierter Befragungsrechte ist demgegenüber fehlgeleitet und schafft insbesondere auch keinen Mehrwert. Vielmehr ist es an der kontrollierten Behörde, sicherzustellen, dass ihrer Darlegungslast gegenüber dem Unabhängigen Kontrollrat genügt wird. Für die Vorabkontrolle folgt dies schon daraus, dass es dem beantragenden Dienst gelingen muss, die Anordnungsvoraussetzung zur Überzeugung des Unabhängigen Kontrollrats darzulegen, da die Anordnung anderenfalls nicht durchführbar ist. Dies bezieht auch den schwer vorstellbaren Fall mit ein, dass der Unabhängigen Kontrollrat für seine Überzeugungsbildung die Einlassung eines individuellen Mitarbeiters benötigt.

Der bisherige § 56 Absatz 4 Satz 1 des BND-Gesetz ist entfallen. Auch hiermit geht indes keine Rechtsänderung einher – vielmehr ist es eine Selbstverständlichkeit, dass eine kontrollierte Behörde auf Fragen der Kontrollinstanz vollständig und wahrheitsgemäß antworten muss. Dies gesondert zu regeln, wirft letztlich nur Fragen zur Rechtskonformität der Verwaltung auf.

Zu Absatz 4

Die Befugnisse des Unabhängigen Kontrollrats finden eine Grenze im Quellenschutz, wo die Arbeitsfähigkeit und Aufgabenerfüllung der Nachrichtendienste auch über den konkreten Einzelfall hinaus für die Zukunft generell beeinträchtigt werden kann. Dieser Schutz bezieht sich zum einen auf die Arbeitsweise und Funktionsfähigkeit der Nachrichtendienste im Verhältnis zu operativ eingesetzten Personen (Vorgehen der Behörden bei der

Anwerbung und Führung von sowie der Kommunikation mit V-Leuten bzw. nachrichtendienstlichen Verbindungen und sonstigen Quellen) und zum anderen auf die unverzichtbare und verbindliche Vertraulichkeitszusage gegenüber Quellen als Voraussetzung für die weitere Nutzung aktiver und die Gewinnung neuer Informationsquellen. Es kommt zentral darauf an, dass das Vertrauen in die Einhaltung gegebener Vertraulichkeitszusagen nicht erschüttert wird. Zu berücksichtigen ist, dass bereits der (subjektive) Eindruck, dass die Vertraulichkeit nicht gesichert sei ausreichen kann, um eine menschliche Quelle von dem weiteren Zusammenarbeiten mit einem Nachrichtendienst abzuhalten und die Gewinnung neuer Quellen zu erschweren (vgl. BVerfGE 146, 1, Rn. 114 auch mit Verweis auf Warg, NVwZ 2014, S. 1263, 1266).

Die Regelung ist insoweit restriktiver ausgestaltet als § 28 Absatz 3 Satz 2 des Bundesverfassungsschutzgesetzes, da sie auf einen speziellen Aspekt der Funktionssicherung nachrichtendienstlicher Aufgabenwahrnehmung beschränkt bleibt.

Besondere Zurückhaltung ist bei der Identität von nachrichtendienstlichen Verbindungen angezeigt, die oftmals als „Verräter“ gegenüber ihrer eigenen Staatsmacht oder möglicherweise militanten Umfeld gelten – verbunden mit Gefahren für ihre Freiheit, ihren Leib und ihr Leben. Dementsprechend besteht hier ein außerordentliches Bedürfnis zur Vertraulichkeit, insbesondere auch als Grundlage ihrer Zusammenarbeitsbereitschaft. Dabei schließt die gebotene Vertraulichkeit sowohl den Schutz direkter Informationen, welche Rückschlüsse auf die Identität zulassen, als auch sonstiger Angaben, welche eine Enttarnung mittelbar befördern können, ein. Letzteres umfasst etwa die Angabe eines Geburtsdatums oder anderer Merkmale, die erst bei Kombination mit weiteren Informationen (gleichsam einem „Puzzle“) zu einer Enttarnung führen könnten. Dieses Funktionserfordernis zum Schutz der herausragenden Rechtsgüter des Verfassungsschutzes geht selbst parlamentarischer Kontrolle vor (BVerfGE vom 14. Dezember 2022, 2 BvE 8/21 (146, 1). Auch die ständige Rechtsprechung des Bundesverwaltungsgerichts erkennt ausdrücklich an, dass für die Funktionsfähigkeit der Nachrichtendienste die verlässliche Vertraulichkeit betreffend die Identität seiner menschlichen Quellen, von essentieller Bedeutung ist – selbst über den Tod einer Quelle hinaus (vgl. BVerwG 20 F 15.16, Rn. 27ff.). Für das Anordnungskontrollverfahren sind die Umstände des Einsatzes und die Art des Einsatzmittels, grundsätzlich jedoch nicht seine Individualisierung bedeutsam. Demgemäß wird die Identität einer nachrichtendienstlichen Verbindung in den Anordnungen nicht genannt (dies entspricht sogar den Gepflogenheiten im polizeilichen Kontext, vgl. Anträge des Bundeskriminalamt nach § 45 Absatz 4 BKAG). Sofern der Unabhängige Kontrollrat in ganz besonderen Ausnahmesachverhalten allgemeine Informationen zur Person zwingend benötigt, bleibt im jeweiligen Verfahren zu klären, wie dem Informationsbedarf so schonend Rechnung getragen werden kann, dass die Identität der eingesetzten Person nicht – auch nicht mit zusätzlichen Informationen offenbart werden kann (abstrahierte Ergänzungsauskünfte).

Zu Unterabschnitt 4 (Gerichtsähnliches Kontrollorgan)

Zu § 14 (Besetzung des gerichtsähnlichen Kontrollorgans)

Zu Absatz 1

Die Vorschrift entspricht in ihrem Regelungsgehalt dem bisherigen § 43 Absatz 1 BND-Gesetz. Das gerichtsähnliche Kontrollorgan besteht künftig aus acht Mitgliedern. Die vormals im bisherigen § 48 Absatz 1 und Absatz 2 BND-Gesetz enthaltenen Regelungen zur „Amtsbezeichnung“ geht in Absatz 1 auf. Unverändert bleibt die Amtsbezeichnung insoweit „Präsidentin oder Präsident des Unabhängigen Kontrollrats“ bzw. „Vizepräsidentin oder Vizepräsident des Unabhängigen Kontrollrats“. Die bisherige Amtsbezeichnung der übrigen Mitglieder wird in die geschlechterneutrale Begrifflichkeit „Mitglied des Senats beim Unabhängigen Kontrollrat“ geändert.

Zu Absatz 2

Die Regelung entspricht dem bisherigen § 43 Absatz 1 2. Halbsatz BND-Gesetz. Zugunsten der Rechtsklarheit wurde sie in einen eigenen Absatz überführt. Das gerichtsähnliche Kontrollorgan wird aufgrund der Zunahme der Aufgaben des Unabhängigen Kontrollrates auf acht Mitglieder erweitert.

Sieben der Mitglieder des gerichtsähnlichen Kontrollorgans müssen zuvor Richterinnen oder Richter gewesen sein. Hier wird die Begrenzung auf Bundesgerichtshof und Bundesverwaltungsgericht zugunsten aller obersten Gerichtshöfe des Bundes aufgehoben.

Zudem wird die Möglichkeit eingeführt, dass nichtrichterliche Mitglieder in das gerichtsähnliche Kontrollorgan gewählt werden können. Bei diesen handelt es sich entweder um Bundesbeamte oder Bundesbeamtinnen einer obersten Bundesbehörde der Besoldungsgruppe B 6 oder höher mit der Befähigung zum Richteramt, die in ihrem beruflichen Werdegang mehrjährige Erfahrungen mit der Tätigkeit von Sicherheitsbehörden gesammelt haben, um Bundesanwältinnen oder Bundesanwälte beim Bundesgerichtshof oder um Mitglieder eines Kontrollgremiums, welches mit der Nachprüfung von (nachrichtendienstlichen) Eingriffen in das Fernmeldegeheimnis betraut war. Diese Ergänzung führt dazu, dass die Expertise des gerichtsähnlichen Kontrollorgans wächst, nicht nur richterliche Vorerfahrung wird berücksichtigt, sondern auch Facherfahrung, die in obersten Bundesbehörden gesammelt wurde.

Zu Absatz 3

Mit der Verteilung von sieben richterlichen und zwei nichtrichterlichen Mitgliedern werden die Vorgaben des Bundesverfassungsgerichts für Entscheidungen der Kollegialspruchkörper berücksichtigt. Für diese ist zwingend zu gewährleisten, „dass der richterlichen Perspektive ein maßgebliches Gewicht zukommt, die für eine maßgebliche Zahl der Mitglieder durch langjährige richterliche Erfahrung belegt sein muss.“ (BVerfG 1 BvR 2835/17, Rn. 286). Die grundsätzlich bereits damals vom Bundesverfassungsgericht aufgezeigte Öffnungsmöglichkeit wird nun mit den nichtrichterlichen Mitgliedern genutzt: „Erfahrung in anderen juristischen Berufen zu berücksichtigen“ sollte ebenfalls möglich sein (BVerfGE a.a.O., Rn. 286). Das gerichtsähnliche Kontrollorgan kann so von den unterschiedlichen Erfahrungen juristischer Perspektive insgesamt profitieren und die Spruchpraxis unter Berücksichtigung dieser entsprechend fortentwickeln. Die nichtrichterlichen Mitglieder sind den richterlichen Mitgliedern gleichgestellt. Insbesondere können auch nichtrichterliche Mitglieder auch als Einzelrichter tätig werden.

Zu § 15 (Unabhängigkeit der Mitglieder des gerichtsähnlichen Kontrollorgans)

Die bisherige Regelung des § 44 Absatz 1 Satz 3 des BND-Gesetzes wurde in einer eigenen Norm verortet. Dies hebt die Unabhängigkeit der Mitglieder des gerichtsähnlichen Kontrollorgans im Rahmen ihrer „gerichtsähnlichen Tätigkeit“ adäquat hervor.

Zu § 16 (Vakanzen im gerichtsähnlichen Kontrollorgan)

Zu Absatz 1

Um die Funktionsfähigkeit des Unabhängigen Kontrollrats zu gewährleisten, sollen auch bereits absehbare Vakanzen dem Parlamentarischen Kontrollgremium zum Zwecke der Ausschreibung vom Unabhängigen Kontrollrat mitgeteilt werden. Erst recht gilt dies für bereits eingetretene Vakanzen.

Das bisherige Vorschlagsrecht aus § 43 Absatz 3 des BND-Gesetzes entfällt. Das Parlamentarische Kontrollgremium übernimmt vielmehr die Administration des Bewerbungsverfahrens sowie die Wahl selbst. Eine Vorfilterung entfällt. Konkret erfolgt eine Ausschreibung bei den obersten Gerichten des Bundes für die richterlichen Mitglieder sowie öffentlich für

die nichtrichterlichen Mitglieder. Das Ausschreibungsverfahren und die Sichtung des Bewerbungseingangs, die Einbindung der Bundesregierung und des Unabhängigen Kontrollrats für die Anhörung potenzieller Kandidatinnen und Kandidaten und schließlich die Wahl obliegen zukünftig dem Parlamentarischen Kontrollgremium als Herrin des Verfahrens.

Da mindestens sechs richterliche Mitglieder vorgesehen sind, sind etwaige Vakanzen der richterlichen Stellen zunächst auch „nur“ durch richterliche Mitglieder nachzubesetzen, wenn nicht bereits zuvor mehr als sechs der Stellen mit richterlichen Mitgliedern besetzt war. In diesen Fällen erübrigt sich eine öffentliche Ausschreibung.

Im neu ausgestalteten Auswahlverfahren (öffentliche Ausschreibung und anschließende Wahl durch das Parlamentarische Kontrollgremium) kann weiterhin die Qualifikation und berufliche Erfahrung der Mitglieder berücksichtigt werden.

Zu Absatz 2

Die Bewerbungen der nichtrichterlichen und der richterlichen Mitglieder sind an das Parlamentarische Kontrollgremium zu richten.

Zu § 17 (Wahl und Ernennung der Mitglieder des gerichtsähnlichen Kontrollorgans; Wahl der Präsidentin oder des Präsidenten und der Vizepräsidentin oder des Vizepräsidenten des Unabhängigen Kontrollrats)

Zu Absatz 1

Das Parlamentarische Kontrollgremium wählt die Mitglieder des gerichtsähnlichen Kontrollorgans mit einfacher Stimmenmehrheit. Die Regelung entspricht dem bisherigen § 43 Absatz 4 Satz 1 des BND-Gesetzes. Die Regelung zur Vorstellung der Kandidatinnen und Kandidaten vor der Wahl beim Parlamentarischen Kontrollgremium war bisher in § 43 Absatz 3 Satz 3 des BND-Gesetzes enthalten.

Zu Absatz 2

Die Bundesregierung und der Unabhängige Kontrollrat werden vor der Wahl durch das Parlamentarische Kontrollgremium zu den Personen angehört, die zur Wahl stehen.

Zu Absatz 3

Wie bislang (§ 43 Absatz 4 des BND-Gesetzes) werden Präsidentin/Präsident und Vizepräsidentin/Vizepräsident ebenfalls durch das Parlamentarische Kontrollgremium aus den gewählten Mitgliedern des Unabhängigen Kontrollrats gewählt, wobei diese Wahl auch vor Ernennung zum Mitglied erfolgen kann.

Zu Absatz 4

Für die Mitglieder des Parlamentarischen Kontrollgremiums gilt – dem § 7 des Richterwahlgesetzes entsprechend – dass ein Mitglied des Parlamentarischen Kontrollgremiums von der Mitwirkung bei der Wahl eines Mitglieds des gerichtsähnlichen Kontrollorgans ausgeschlossen ist, wenn die Voraussetzungen des § 41 Nummer 3 der Zivilprozessordnung (Person, mit der sie oder er in gerader Linie verwandt oder verschwägert, in der Seitenlinie bis zum dritten Grad verwandt oder bis zum zweiten Grad verschwägert ist oder war) vorliegen.

Zu § 18 (Ernennung und Rechtsstellung der Mitglieder des gerichtsähnlichen Kontrollorgans)

Zu Absatz 1

Die Regelung entspricht § 44 Absatz 1 Satz 1 und Satz 2 in Verbindung mit § 44 Absatz 2 des BND-Gesetzes.

Zu Absatz 2

Die in Absatz 2 geschaffene Regelung soll dem möglichen Einzelfall Rechnung tragen, dass bei einem durch das Parlamentarische Kontrollgremium gewählten Mitglied des Unabhängigen Kontrollrats im Rahmen der nach § 11 Absatz 1 durchzuführenden Sicherheitsüberprüfung solche Sicherheitsrisiken festgestellt werden, welcher einer Ausübung der Tätigkeit als Mitglied des gerichtsähnlichen Kontrollorgans entgegenstehen. In diesen Fällen hat eine Ernennung zu unterbleiben und stattdessen ist eine neue Kandidatin ein neuer Kandidat zu wählen.

Zu Absatz 3

Die Regelung entspricht § 44 Absatz 3 des BND-Gesetzes.

Zu § 19 (Amtszeit der Mitglieder des gerichtsähnlichen Kontrollorgans)

Zu Absatz 1

Die bisher in § 45 Absatz 1 des BND-Gesetzes geregelte Vorschrift erfährt Anpassung aus Gründen der Normenklarheit. Ergänzt wird die Regelung dahingehend, dass die Amtszeit automatisch endet, wenn nach der Ernennung ein Sicherheitsrisiko im Sinne des § 5 Absatz 1 des Sicherheitsüberprüfungsgesetzes festgestellt wird. Gegen diese Feststellung steht der Rechtsweg offen.

Zu Absatz 2

Die Regelung des § 45 Absatz 2 des BND-Gesetzes wurde übernommen.

Zu Absatz 3

Wie bisher ruhen bei den Mitgliedern mit Ernennung in das Beamtenverhältnis auf Zeit für die Dauer der Amtszeit die Rechte und Pflichten aus dem im Richter- oder Beamtenverhältnis auf Lebenszeit übertragenen Amt. Für die Verschwiegenheitspflicht und das Verbot der Annahme von Belohnungen, Geschenken und sonstigen Vorteilen gilt dies freilich nicht.

Zu Absatz 4

Die bisherige Regelung des § 45 Absatz 5 des BND-Gesetzes wurde übernommen. Der § 30 des Bundesbeamtengesetzes bleibt unbeschadet: Selbstverständlich gehen die dort in den Nummern 1 bis 3 genannten Beendigungsgründe der Verlängerung vor.

Zu Absatz 5

Absatz 5 regelt in Ergänzung des Absatzes 4, dass im Falle der Verlängerung der Amtszeit eines Mitglieds des gerichtsähnlichen Kontrollorgans das Amt bis zum Ende des Kalendermonats übertragen wird, in dem die Geschäftsführung endet.

Zu § 20 (Ruhestand; Ruhegehalt der Mitglieder des gerichtsähnlichen Kontrollorgans)

Die bisherige Regelung des § 45 Absatz 4 des BND-Gesetzes wird in einer eigenen Norm verortet und auf drei Absätze aufgeteilt.

Zu Absatz 1

Die bisherige Regelung des § 45 Absatz 4 Satz 1 und Satz 2 des BND-Gesetzes wird übernommen. Die Wartezeit wird von vier auf fünf Jahre angehoben. Dies folgt daraus, dass mit der Öffnung des gerichtsähnlichen Kontrollorgans für nichtrichterlicher Mitglieder die Möglichkeit besteht, dass Personen ohne bestehendes Richter- oder Beamtenverhältnis in das gerichtsähnliche Kontrollorgan gewählt werden können. Auch für die Versetzung dieser Personen in den Ruhestand ist nach § 50 des Bundesbeamtengesetzes die Erfüllung einer versorgungsrechtlichen Wartezeit erforderlich. Diese ist nach § 4 Absatz 1 Satz 1 Nummer 1 des Beamtenversorgungsgesetzes auf fünf Jahre festgesetzt.

Zu Absatz 2

Die Regelung entspricht dem bisherigen § 45 Absatz 4 Satz 3 bis 5 des BND-Gesetzes und wird aufgrund der Öffnung für nichtrichterliche Mitglieder für die Personen ergänzt, die aus einem Beamtenverhältnis auf Lebenszeit in das gerichtsähnliche Kontrollorgan gewählt werden.

Zu Absatz 3

Die Regelung entspricht dem bisherigen § 45 Absatz 4 Satz 6 des BND-Gesetzes und wird aufgrund der Öffnung für nichtrichterliche Mitglieder für die Personen ergänzt, die aus einem Beamtenverhältnis auf Lebenszeit in das gerichtsähnliche Kontrollorgan gewählt werden.

Zu § 21 (Besoldung der Mitglieder des gerichtsähnlichen Kontrollorgans)

Die Regelung entspricht dem bisherigen § 46 des BND-Gesetz

Zu Absatz 1

Die Regelung des bisherigen § 46 Absatz 1 des BND-Gesetzes wird übernommen und lediglich aus Gründen der Normenklarheit angepasst.

Zu Absatz 2

Die Regelung des bisherigen § 46 Absatz 2 des BND-Gesetzes wird dahingehend ergänzt, dass der Vizepräsidentin oder dem Vizepräsidenten, die oder der Teil der Behördenleitung ist und insbesondere regelmäßig auch Leitungsaufgaben (wie z.B. die Leitung der Verwaltung) übernimmt, ein Amt der Besoldungsgruppe B 8 übertragen wird. Dies ist infolge der herausgehobenen Stellung im Vergleich zu den übrigen Mitgliedern des Senats des gerichtsähnlichen Kontrollorgans sachgerecht.

Zu § 22 (Weitere Rechte und Pflichten der Mitglieder des gerichtsähnlichen Kontrollorgans)

Zu Absatz 1

Die Regelung des Satz 1 ist gegenüber dem bisherigen § 47 Absatz 1 des BND-Gesetzes unverändert geblieben. Satz 2 trifft eine besondere Regelung zugunsten der für die Richterinnen und Richter des Bundesgerichtshofs geltenden Besetzung des Dienstgerichts. Dies ist dem Umstand geschuldet, dass die „reguläre“ Besetzungsvorschrift des § 61 Absatz 2

des Deutschen Richtergesetzes für die Mitglieder des gerichtsähnlichen Kontrollorgans, die gerade keinem besonderen Gerichtszweig mehr „angehören“, fehlgehen würde.

Zu Absatz 2

Die Regelung des bisherigen § 47 Absatz 2 des BND-Gesetzes wird übernommen und lediglich aus Gründen der Normenklarheit angepasst.

Zu § 23 (Kollegialspruchkörper und Entscheidungen des gerichtsähnlichen Kontrollorgans)

Zu Absatz 1

Entsprechend der Rechtsprechung des Bundesverfassungsgerichts (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, 275) sind für das gerichtsähnliche Kontrollorgan „Spruchkörper“ vorzusehen, bei denen richterliche Mitglieder die Mehrzahl bilden. Dies ist nur insoweit normativ abbildbar, als dass die diesbezüglichen Spruchkörper des gerichtsähnlichen Kontrollorgans auf „Kollegialspruchkörper“ begrenzt bleiben; also lediglich die Kammern und der Senat die vom Bundesverfassungsgericht genannten Entscheidungen (über strategische Aufklärungsmaßnahmen des Bundesnachrichtendienstes) treffen dürfen.

Zu Absatz 2

Die Regelung etabliert den Senat als Kollegium aus den Mitgliedern des gerichtsähnlichen Kontrollorgans. Zudem wird der Vorsitz im Senat bestimmt mitsamt der insoweit geltenden Vertretungsverhältnisse, wobei die untergesetzliche Ausgestaltung weiterer Stufen der Vertretung unbenommen bleibt. Der Senat ist das oberste Entscheidungsgremium des Unabhängigen Kontrollrats und daher von herausgehobener Bedeutung. Dem Senat obliegen zum einen die Entscheidungen bei seinen Aufgaben in der Rechtskontrolle. Zum anderen ist der Senat auch für die nach innen wirkenden Entscheidungen zuständig, wie z.B. den Beschluss von Geschäfts- und Verfahrensordnung sowie der Geschäftsverteilung. Er ist dergestalt in seinem Wesen mit dem Großen Senat des Bundesrechnungshofes vergleichbar, vgl. § 13 des Bundesrechnungshofgesetzes.

Zu Absatz 3

Bislang regelte § 49 Absatz 1 des BND-Gesetzes, dass zwei Kammern gebildet werden. Mit dem Zuwachs an zu kontrollierenden Stellen sowie einem breiteren Portfolio an materiellen Kontrollzuständigkeiten soll diese feste Vorgabe zugunsten der autonomen behördlichen Ausgestaltung entfallen. Das gerichtsähnliche Kontrollorgan bleibt verpflichtet, Kammern zu bilden.

Zu Absatz 4

In Absatz 3 ist geregelt, dass die Präsidentin oder der Präsident bzw. die Vizepräsidentin oder der Vizepräsident den Vorsitz in der Kammer führen, der sie oder er angehören. Hierdurch ist zugleich klargestellt, dass mindestens zwei Kammern gebildet werden müssen und dass die Präsidentin oder der Präsident bzw. die Vizepräsidentin oder der Vizepräsident nicht in der gleichen Kammer tätig sein können.

Vertretungsregelungen für den Vorsitz in den jeweiligen Kammern können untergesetzlich festgelegt werden.

Zu Absatz 5

Entscheidungen des gerichtsähnlichen Kontrollorgans ergehen als Beschluss. Im Übrigen entspricht Absatz 4 der Regelung des bisherigen § 49 Absatz 3 des BND-Gesetzes und wurde lediglich aus Gründen der Normenklarheit angepasst.

Zu Absatz 6

Stellt das gerichtsähnliche Kontrollorgan die Rechtswidrigkeit fest (Nummer 1), ist der Beschluss mit bestimmten Maßgaben oder Einschränkungen versehen oder weist ein Sachverhalt, welcher dem Unabhängigen Kontrollrat vorgelegt wird, Besonderheiten tatsächlicher oder rechtlicher Art auf oder ist von grundsätzlicher Bedeutung (Nummer 3), so ist der Beschluss schriftlich zu begründen. Wann ein Sachverhalt, welcher dem Unabhängigen Kontrollrat vorgelegt wird, Besonderheiten tatsächlicher oder rechtlicher Art aufweist oder von grundsätzlicher Bedeutung ist, kann dabei – soweit dies für erforderlich gehalten wird – vom Unabhängigen Kontrollrat auch innerhalb der Geschäftsordnung näher ausgeführt werden.

Die hier geregelte Schriftlichkeit ist für die Handlungsfähigkeit und -sicherheit der Nachrichtendienste von besonderer Bedeutung. Weiterhin trägt die Regelung, die aktuell bereits gelebte Praxis im gerichtsähnlichen Kontrollorgan ist, dazu bei, die Rolle des Unabhängigen Kontrollrats an der Auslegung des Nachrichtendienstrechts zu stärken. Denn unabhängig von dem jeweiligen geheimen Vorlagefall kann die abstrakte Rechtsfrage im öffentlichen Diskurs Relevanz haben.

Zu § 24 (Beratungsgeheimnis)

Die Regelung entspricht dem bisherigen § 54 Absatz 1 des BND-Gesetzes, klarstellend wird auf das gerichtsähnliche Kontrollorgan Bezug genommen.

Zu Unterabschnitt 5 (Administratives Kontrollorgan)

Zu § 25 (Leitung des administrativen Kontrollorgans; Weisungen)

Zu Absatz 1

Die Regelung des bisherigen § 50 Satz 1 bis Satz 4 des BND-Gesetzes wird unverändert übernommen.

Zu Absatz 2

Die Weisungsbefugnis der Behördenleitung gegenüber der Leiterin oder dem Leiter des administrativen Kontrollorgans wird klarstellend angepasst. Bereits mit der Novelle 2021 wurde festgelegt. „Durch die einheitliche Behördenstruktur ist zwischen beiden Säulen ein offener und unmittelbarer Austausch gewährleistet, um dem Gebot einer wirksamen und kohärenten Kontrolle nachkommen zu können.“ (BT Drs. 19/26103, S. 102) Sowie „Dabei bleibt es dem gerichtsähnlichen Kontrollorgan unbenommen, auf die Expertise des administrativen Kontrollorgans zuzugreifen, um z.B. seine Entscheidungen vorzubereiten.“ (BT Drs. 19/26103, S. 111).

Zu Absatz 3

Die in Absatz 2 geregelte Weisungsbefugnis der Behördenleitung wird in Absatz 3 durch eine allgemeine Pflicht des administrativen Kontrollorgans flankiert, die Mitglieder des Senats beim Unabhängigen Kontrollrat bei der Durchführung ihrer Kontrollbefugnisse zu unterstützen. Dies bedeutet einerseits eine institutionelle und umfassende Nachordnung im Rahmen der internen Behördenstruktur und zum anderen, dass auf faktischer Ebene das administrative Kontrollorgan den Mitgliedern des Senats beim Unabhängigen Kontrollrat jederzeit seine faktische Expertise zur Verfügung stellt.

Einzelheiten zu der konkreten behördlichen Organisation dieses Nachordnungsverhältnisses (also insbesondere etwa zu der Frage, in welchem Umfang einzelne Mitglieder des gerichtsähnlichen Kontrollorgans gegenüber dem Leiter des administrativen Kontrollorgans oder einzelnen Mitarbeitenden des administrativen Kontrollorgans weisungsbefugt sind und

auf welchem Wege der gesetzlich intendierte Vorrang der gerichtsähnlichen Vorabkontrolle im Falle konfligierender Weisungen umzusetzen ist – etwa, wenn Mitarbeitende des administrativen Kontrollorgans angewiesen werden, das gerichtsähnliche Kontrollorgan vorrangig im Rahmen der Vorabkontrolle zu unterstützen und konkrete administrative Prüfaufgaben insoweit zurückzustellen – bleibt der innerbehördlichen Organisation durch die Behördenleitung überlassen.

Zu § 26 (Prüfprogramm für das administrative Kontrollorgan; Prüfaufträge)

Zu Absatz 1

Unverändert zum geltenden Recht gibt das gerichtsähnliche Kontrollorgan den Prüfrahmen für die administrative Kontrolle (also die Einhaltung der Vorgaben der Bestimmungen für die Erhebung, Weiterverarbeitung und Übermittlung von personenbezogenen Daten in den nachrichtendienstlichen Fachgesetzen im Wege einer strukturellen datenschutzrechtlichen Kontrolle) durch das administrative Kontrollorgan vor. Die administrative Kontrolle erfolgt dabei grundsätzlich dergestalt, dass nicht einzelne Vorgänge in den Blick genommen werden, sondern die grundlegenden Strukturen der Datenverarbeitung. Dabei wird es in der Regel indes notwendig sein, stichprobenhaft Einzelvorgänge in die Kontrolle mit einzubeziehen und anhand dieser Einzelvorgänge die genannten Strukturen sichtbar zu machen und einer wirksamen Kontrolle zu unterziehen. Die administrative Kontrolle folgt dabei zwar dem Rahmen des Prüfprogramms, erfolgt aber innerhalb dieses Rahmens grundsätzlich eigeninitiativ (mit Ausnahme des Absatzes 3).

Das Prüfprogramm soll nunmehr für einen Zeitraum von bis zu 24 Monaten gelten, während bislang in § 51 Absatz 2 BND-Gesetz „regelmäßige Abstände“ vorgesehen waren. Dies soll einerseits dem Umstand Rechnung tragen, dass der Prüfrahmen des administrativen Kontrollorgans regelmäßig an die Entwicklung des Prüfgeschehens angepasst werden muss. Zugleich ist ein Ausgleich zwischen der „Aktualität“ des Prüfprogramms und der Langfristigkeit der Ressourcenplanung bei den Nachrichtendiensten des Bundes zu erreichen. Diesem Ausgleich ist sachgerecht mit einem Zeitraum von 24 Monaten entsprochen. Zuständig für den Erlass ist dabei der Senat.

Das Prüfprogramm des Unabhängigen Kontrollrats lenkt die Tätigkeit des administrativen Kontrollorgans. Sie schafft einerseits einen klaren Rahmen für die Prüftätigkeit – wobei dieser Rahmen in aller Regel abstrakt generelle Vorgaben zur Prüfung von Themenkomplexen, Aufklärungsarten, Erhebungsvoraussetzungen etc. enthalten wird – um auch für die Nachrichtendienste eine verlässliche Grundlage für die eine wirksame Prüfung begleitende Ressourcenallokation zu geben. Zudem sorgt das Prüfprogramm dafür, dass das gerichtsähnliche Kontrollorgan entscheidenden Einfluss auf die Grundpfeiler der Strukturprüfung ausüben kann. Dabei ist – dies folgt schon aus der Natur der Sache einer gemeinsamen Tätigkeit im Rahmen einer Behördenhierarchie – ein steter Austausch zwischen den Kontrollorganen entscheidend. Dieser Austausch kann und soll in der Praxis auch zur wechselseitigen Sensibilisierung hinsichtlich rechtlicher Fragestellungen beitragen. Es ist gerade der Vorteil der integralen Kontrolle, die im Rahmen der administrativen Kontrolle auch die datenschutzrechtliche Strukturprüfung beinhaltet, gegenüber der bisherigen Aufspaltung zwischen der datenschutzrechtlichen Kontrolle durch die Bundesbeauftragte für den Datenschutz sowie der Vorabkontrolle durch den Unabhängigen Kontrollrat bzw. der G10-Kommission. Bei der Ausgestaltung des Prüfprogrammes ist Sorge zu tragen, dass die Prüfung durch das administrative Kontrollorgan nicht dergestalt verengt wird, dass durch die Ausnahme einzelner Bereiche ein Prüfvakuum entsteht. Es ist insoweit Funktion des Prüfprogrammes, eine Priorisierung anhand thematischer oder vergleichbarer Schwerpunkte zu treffen und nicht einen verbindlichen „Prüfrand“ für das administrative Kontrollorgan zu definieren.

Den Nachrichtendiensten des Bundes, und infolge der Fachaufsicht auch den jeweiligen obersten Bundesbehörden, wird mit angemessener Frist Gelegenheit zur Stellungnahme

eingeräumt. Hierdurch ist keineswegs beabsichtigt, dass Einfluss auf das Prüfprogramm genommen wird, um die Kontrolle durch den Unabhängigen Kontrollrat zu schmälern. Vielmehr soll die Möglichkeit der Stellungnahme lediglich gewährleisten, dass z.B. Hinweise gegeben werden können, wenn ein vorgesehenes Kontrollthema etwa aus tatsächlichen Gründen wie einer Umstrukturierung oder anderen Art der Anpassung in dem vorgesehenen Zeitraum keiner effektiven Kontrolle zugeführt werden kann. Dem Unabhängigen Kontrollrat steht es frei, diese etwaigen Hinweise zu ignorieren und an dem beabsichtigten Prüfprogramm festzuhalten.

Abschließend ist in Satz 3 geregelt, dass der Senat auch Änderungen am laufenden Prüfprogramm vornehmen kann.

Zu Absatz 2

Die neue Regelung bindet die Rechtmäßigkeitskontrolle stärker als bisher an die parlamentarische Kontrolle an und soll so zu deren Stärkung beitragen.

Zu Absatz 3

In Absatz 3 findet sich die im bisherigen § 51 Absatz 2 Satz 2 des BND-Gesetzes vorgesehene Möglichkeit, konkrete und einzelfallbezogene Prüfaufträge zu vergeben. Prüfaufträge sind verbindliche Aufträge des gerichtsähnlichen Kontrollorgans an das administrative Kontrollorgan, welche einzelne strategische Aufklärungsmaßnahmen des Bundesnachrichtendienstes betreffen und diesem gegenüber Prüfwirkung entfalten. Nicht von dem Begriff umfasst sind damit solche „Prüfaufträge“ des gerichtsähnlichen Kontrollorgans an das administrative Kontrollorgan, welche auf eine behördeninterne Prüfung im Unabhängigen Kontrollrat beschränkt bleiben und bei denen keine direkte Kontaktaufnahme mit dem Bundesnachrichtendienst erforderlich ist. Das bisherige Verfahren der Befassung des gerichtsähnlichen Kontrollorgans mit den Prüfvorgängen des administrativen Kontrollorgans im Bereich der strategischen Fernmeldeaufklärung des Bundesnachrichtendienstes, welches sich bewährt hat, bleibt insoweit unverändert erhalten.

Dass die Möglichkeit der Prüfaufträge auf die strategische Aufklärung durch den Bundesnachrichtendienst begrenzt wird, folgt den verfassungsgerichtlichen Vorgaben dahingehend, dass dieser Bereich nachrichtendienstlichen Handelns in besonderem Maße einer (verschränkten) Kontrolle durch administrative und gerichtsähnliche Kontrolle unterliegt: „Im Zusammenwirken der Kontrollinstanzen muss gewährleistet sein, dass der gesamte Prozess der strategischen Überwachung [d.h. der strategischen Fernmeldeaufklärung im bisherigen Recht bzw. der strategischen Aufklärung im Rahmen der Novellierung des BND-Gesetzes] einschließlich der hieran anknüpfenden Datenverarbeitung und -übermittlung wie auch der Zusammenarbeit mit ausländischen Nachrichtendiensten potentiell umfassend der Kontrolle unterliegt. Soweit keine gerichtsähnliche Kontrolle vorgesehen ist, muss die Möglichkeit der administrativen Kontrolle eröffnet sein“ (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 279).

Diese Erwägungen gelten nicht in gleichem Maße für die übrigen nachrichtendienstlichen Maßnahmen, welche einer Vorabkontrolle unterliegen, da diese gerade nicht von einer solchen Streubreite sind wie die strategische Aufklärung. Insbesondere gelten diese Erwägungen auch nicht für die – im bisherigen Recht durch § 51 Absatz 1 Satz 2 des BND-Gesetzes der Zuständigkeit des administrativen Kontrollorgan zugewiesenen – Rechtskontrolle über Maßnahmen der technischen Aufklärung, welche über die strategische (Fernmelde-)Aufklärung hinausgehen (vgl. zu den verfassungsrechtlichen Anforderungen BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 273); im bisherigen Recht also insbesondere Maßnahmen nach § 34 des BND-Gesetzes.

Soweit der Bundesnachrichtendienst von einem Prüfauftrag betroffen ist, wird dieser gemeinsam mit dem Bundeskanzleramt darüber vom Unabhängigen Kontrollrat in Kenntnis gesetzt. Hiermit soll dem Bundesnachrichtendienst lediglich die Möglichkeit gegeben

werden, die organisatorischen Maßnahmen zu treffen, die für eine umfassende Ausführung der Prüfaufträge notwendig sind.

Zu Abschnitt 3 (Ausübung der Rechtskontrolle durch den Unabhängigen Kontrollrat)

Zu Unterabschnitt 1 (Rechtskontrolle durch das gerichtsähnliche Kontrollorgan; Gefahr im Verzug)

Zu § 27 (Vorabkontrolle durch das gerichtsähnliche Kontrollorgan)

Zu Absatz 1

Bei der Vorabkontrolle durch das gerichtsähnliche Kontrollorgan steht die Befugnisausübung (das heißt konkret die Durchführung der jeweiligen Maßnahme auf Grundlage der behördlichen Anordnung) durch den jeweiligen Nachrichtendienst unter dem Vorbehalt der Bestätigung der Rechtmäßigkeit durch das gerichtsähnliche Kontrollorgan. Je nach Eingriffsintensität der Maßnahmen ergibt sich aus dem Verhältnismäßigkeitsgrundsatz im engeren Sinne auch die Notwendigkeit, die Maßnahme vor ihrer Durchführung einer Kontrolle durch eine unabhängige Stelle zu unterziehen. Gerade wegen der Weite der nachrichtendienstlichen Eingriffsschwellen, die Überwachungsmaßnahmen im Vorfeld konkreter Gefahren im Sinne des Polizeirechts zulassen, kommt dem Erfordernis einer Vorabkontrolle besondere Bedeutung zu (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17 Rn. 213).

Zu Absatz 2

In den Fällen, in denen das gerichtsähnliche Kontrollorgan eine Vorabkontrolle durchzuführen hat, legt der jeweilige Nachrichtendienst die behördeninterne Anordnung zur vorgesehenen Befugnisausübung dem Unabhängigen Kontrollrat vor. Die Vorabkontrolle hat die Schutzaufgabe zu erfüllen, die sonst dem Richtervorbehalt sowie auch nachträglichen Rechtsschutzmöglichkeiten, insbesondere Feststellungsklagen, zukommt. Entsprechend muss mit ihr eine auf den Einzelfall bezogene Prüfung ermöglicht werden, die materiell und verfahrensmäßig einer gerichtlichen Kontrolle gleichwertig, insbesondere mindestens ebenso wirkungsvoll ist (BVerfG, a.a.O. Randnummer 275, dort auch mit Verweis auf BVerfGE 30, 1 <23>, dort zu Art. 10 Abs. 2 Satz 2 GG. Das gerichtsähnliche Kontrollorgan (bzw. der jeweils zuständige Kollegialspruchkörper dieses Organs) kann eine Anordnung bestätigen, durch Nichtbestätigung die Rechtswidrigkeit feststellen oder eine Bestätigung nur unter bestimmten, für die Nachrichtendienste verbindlichen Maßgaben und Einschränkungen aussprechen.

Zu Absatz 3

In Absatz 3 erfolgen in den Nummern 1 bis 3 die Verweise auf die in den jeweiligen Fachgesetzen enthaltenen Vorschriften, nach denen Anordnungen einer Vorabkontrolle durch den Unabhängigen Kontrollrat unterfallen.

Zu Nummer 1

Die Regelung spiegelt die im Bundesverfassungsschutzgesetz verankerten Anforderungen für eine Vorabkontrolle durch das gerichtsähnliche Kontrollorgan bei der Aufgabenwahrnehmung durch das Bundesamt für Verfassungsschutz.

Zu Nummer 2

Die Regelung spiegelt die im BND-Gesetz verankerten Anforderungen für eine Vorabkontrolle durch das gerichtsähnliche Kontrollorgan bei der Aufgabenwahrnehmung durch den Bundesnachrichtendienst. Ergänzt wurde dies um die – allein beim Senat liegende –

Zuständigkeit, die Rechtmäßigkeit von Grundanordnungen im Zusammenhang mit erweiterten nachrichtendienstlichen Maßnahmen des Bundesnachrichtendienstes zu prüfen.

Zu § 28 (Zuständigkeit für Entscheidungen in der Vorabkontrolle)

Zu Absatz 1

Anders als nach dem bisherigen BND-Gesetz wird mit dem UKRat-Gesetz die Einzelentscheidung eines Mitglieds des gerichtsähnlichen Kontrollorgans ermöglicht. Dabei entscheidet das einzelne Mitglied, welches sowohl ein nichtrichterliches als auch ein richterliches sein kann, für den Kollegialspruchkörper. Das Mitglied ist nicht originärer Einzelrichter, sondern – in der justiziellen Terminologie – ein fakultativer Einzelrichter.

Für die strategische Fernmeldeaufklärung waren nach den Vorgaben des Bundesverfassungsgerichts die Entscheidungsfindung durch „Spruchkörper“ (die insoweit, wenn die Vorgabe eines richterlichen Übergewichts nicht sinnentleert wird, nur aus Kollegialspruchkörpern bestehen können) zwingend vorzusehen (BVerfG, Urteil vom 19. Mail 2020, 1 BvR 2835/17, Rn. 275). Für die nunmehr der gerichtsähnlichen Vorabkontrolle zu unterwerfenden Ausübungen von Befugnissen wie die heimliche Informationsbeschaffung im Zusammenhang mit menschlichen Quellen oder eingriffsintensive Observationen kann die Entscheidung des einzelnen Mitglieds des jeweiligen zuständigen Kollegialspruchkörper des gerichtsähnlichen Kontrollorgans ausreichend und verfahrensökonomisch geboten sein.

Das gerichtsähnliche Kontrollorgan wird über die Geschäfts- und Verfahrensordnung Vorkehrungen zu treffen haben, die ermöglichen, dass insbesondere in Rechtsmaterien, die bislang keiner gerichtsähnlichen Vorabkontrolle unterlagen, eine einheitliche Spruchpraxis entwickelt werden kann, ohne die Unabhängigkeit des einzelnen Mitglieds des gerichtsähnlichen Kontrollorgans zu beeinträchtigen.

Zu Nummer 1

Den Nachrichtendiensten des Bundes steht es frei, eine Maßnahme mit der Vorgabe vorzulegen, dass eine Entscheidung eines „fakultativen Einzelrichters“ nicht erwünscht ist. Die Vorlage ist dann dem nach der Geschäftsverteilung zuständigen Kollegialspruchkörper zur Vorabkontrolle vorzulegen. Dies kann z.B. angezeigt sein, wenn die beantragte Maßnahme Ausstrahlungswirkung auf weitere oder sich anschließende Maßnahmen haben kann und es dem Nachrichtendienst deshalb darauf ankommt, dass eine spruchkörpergebilligte Praxis etabliert wird.

Zu Nummer 2

Eine Kollegialspruchkörperentscheidung ist entsprechend den Vorgaben des Bundesverfassungsgerichts für die strategische Fernmeldeaufklärung (BVerfG 1 BvR 2835/17, Randnummer 275) zwingend vorzusehen. Eine Einzelentscheidung kann hingegen erfolgen, wenn eine von einem Kollegialspruchkörper gebilligte Maßnahme zur Verlängerung vorgelegt wird oder eine solche erweitert werden soll. Grundsätzlich bleibt es dem Unabhängigen Kontrollrat vorbehalten außerhalb der gesetzlich geregelten Fälle, über eine Kasuistik zu Nummer 3 Vorgaben zu treffen.

Zu Nummer 3

Dem Unabhängigen Kontrollrat steht es frei, die Auslegung dieser gesetzlichen Bestimmung im Wege der Geschäfts- und Verfahrensordnung zu konkretisieren und dabei z.B. die bestehenden Erfahrungen und die sich aufbauende Spruchpraxis zu berücksichtigen. Von grundsätzlicher Bedeutung sind u.a. die Fälle, in denen von einer bestehenden Spruchpraxis abgewichen werden soll. Die grundsätzliche Bedeutung kann sowohl durch das zur Entscheidung aufgerufene Mitglied des Senats beim Unabhängigen Kontrollrat als auch von der zuständigen Kammer oder dem Senat festgestellt werden.

Zu Absatz 2

Mit Absatz 2 wird Sorge getragen, dass der Grundsatz der Einzelentscheidung nicht dazu führt, dass Mitglieder des gerichtsähnlichen Kontrollorgans – mit Ausnahme von Präsidentin/Präsident oder Vizepräsidentin/Vizepräsident – im ersten Jahr nach ihrem Eintritt in den Unabhängigen Kontrollrat bereits Einzelentscheidungen fällen können und müssen. Die Vorschrift ist an die Regelung für obligatorische Einzelrichter in der Zivilprozessordnung angelehnt.

Zu Absatz 3

Absatz 3 eröffnet es jedem Mitglied des gerichtsähnlichen Kontrollorgans, bei Angelegenheiten von grundsätzlicher Bedeutung eine Entscheidung des Senats zu beantragen.

Die Möglichkeit, den Senat zu befassen, ergänzt den neu eingeführten Grundsatz der Einzelentscheidung durch ein Mitglied des gerichtsähnlichen Kontrollorgans in strukturierter Art und Weise. Sie bietet die Möglichkeit, Fragen der Ablauforganisation zu adressieren, aber auch Rechtsfragen zur Anhörung zu bringen. Dieser Aspekt kann z.B. relevant werden, wenn sich aus der einzelnen Kontrollpraxis übergreifende Auslegungsfragen stellen. Dies kann u.a. bei der Bewertung der Auswirkung kumulativer Grundrechtseingriffe Relevanz entfalten.

Zu § 29 (Einzelfallkontrolle durch das gerichtsähnliche Kontrollorgan)

Zu Absatz 1

Die Nachrichtendienste des Bundes sind in bestimmten Fällen verpflichtet, einen konkreten Vorgang dem gerichtsähnlichen Kontrollorgan zur Prüfung vorzulegen. In diesen Fällen erfolgt die Vorlage im Wege eines Ersuchens, bei dem es nicht darum geht, dass die Ausübung einer Befugnis unter dem Vorbehalt der vorherigen Bestätigung der Rechtmäßigkeit durch das gerichtsähnliche Kontrollorgan steht. Vielmehr handelt es sich um „allgemeine“ Rechtsfragen oder abgegrenzte Aspekte innerhalb eines Vorgangs, die einer gerichtsähnlichen Rechtskontrolle zuzuführen sind.

Zu Absatz 2

Ist der Nachrichtendienst verpflichtet, einen Vorgang zur Durchführung der Einzelfallkontrolle beim gerichtsähnlichen Kontrollorgan vorzulegen, so erfolgt dies im Wege eines Ersuchens.

Zu Absatz 3

Zu Nummer 1

Die Regelung spiegelt die im Bundesverfassungsschutzgesetz verankerten Anforderungen für eine Einzelfallkontrolle durch das gerichtsähnliche Kontrollorgan bei der Aufgabenwahrnehmung durch das Bundesamt für Verfassungsschutz.

Zu Nummer 2

Die Regelung spiegelt die im BND-Gesetz verankerten Anforderungen für eine Einzelfallkontrolle durch das gerichtsähnliche Kontrollorgan bei der Aufgabenwahrnehmung durch den Bundesnachrichtendienst.

Zu § 30 (Antrag auf Überprüfung durch den Senat)

Den Nachrichtendiensten des Bundes wird die Möglichkeit eröffnet, eine Entscheidung des gerichtsähnlichen Kontrollorgans (eines einzelnen Mitglieds oder einer Kammer)

überprüfen zu lassen, wobei die Überprüfung in beiden Fällen durch den Senat erfolgt. Kommt der Senat zu dem Ergebnis, dass der Beschluss unzutreffend ergangen ist, so hilft es dem Antrag ab. In diesem Fall ersetz die Entscheidung des Senates den vorausgegangenen Beschluss.

Das Recht zur Überprüfung flankiert die Möglichkeit der Nachrichtendienste zur Vorlage direkt an einen Kollegialspruchkörper (abermals Senat oder Kammer) und sichert damit auch die Entwicklung einer einheitlichen Spruchpraxis. Ohne die Möglichkeit der Überprüfung wäre der Nachrichtendienst gezwungen, den Gegenstand der Vorabkontrolle neu abzufassen und zur Spruchkörperentscheidung vorzulegen. Dieser erhebliche Mehraufwand wird mit vermieden. Auch schützt dieser Mechanismus die Nachrichtendienste des Bundes vor einer zu großen Entscheidungsdivergenz.

Zu § 31 (Gefahr im Verzug)

Zu Absatz 1

Die Regelung zur Gefahr im Verzug wird gegenüber der bisherigen Regelung im BND-Gesetz neu gefasst und prozessual vereinfacht.

Gefahr im Verzug – dies ist nunmehr auch durch eine entsprechende Legaldefinition klargestellt – liegt vor, wenn der Erfolg der Maßnahme durch die Verzögerung, die die Erwirkung einer Entscheidung des Unabhängigen Kontrollrats mit sich bringen würde, gefährdet wäre. Liegt Gefahr im Verzug vor, kann der Nachrichtendienst – nach Maßgabe der Fachgesetze in aller Regel durch die Behördenleitung oder eine benannte Vertretung – eine Anordnung, die der Vorabkontrolle unterliegt, für sofort durchführbar erklären und entsprechend vollziehen.

Zu Absatz 2

Die sofortige Durchführbarkeit der Anordnung ist im Anschluss unverzüglich dem zuständigen Kollegialspruchkörper zur Bestätigung vorzulegen (Satz 1). Hierbei ist – den allgemeinen Grundsätzen folgend – eine Unverzüglichkeit gewahrt, wenn kein schuldhaftes Zögern vorliegt. In Satz 2 ist vorgesehen, dass die Bestätigung in einer (originären) Einzelentscheidung eines Mitglieds des gerichtsähnlichen Kontrollorganes ergeht. Im Geschäftsverteilungsplan ist insoweit eine entsprechende Eilzuständigkeit einzelner Mitglieder zu regeln. Eine anlassbezogene Übertragung auf Einzelmitglieder würde zu einem unnötigen Zeitverzug führen, sodass § 28 Absatz 1 Satz 1 hier einer Modifikation bedarf. Abweichend hiervon ist, wenn ein Fall des § 28 Absatz 1 Satz 2 vorliegt, in den dort genannten Fällen, in denen eine Übertragung der Entscheidung durch den Kollegialspruchkörper auf ein Einzelmitglied unzulässig wäre, eine Eilentscheidung durch den Kollegialspruchkörper erforderlich

Zu Absatz 3

Absatz 3 regelt, dass eine für sofort durchführbar erklärte Anordnung im Grundsatz außer Kraft tritt, wenn sie nicht innerhalb von drei Tagen durch den zuständigen Kollegialspruchkörper (bzw. „Einzelrichter“) des Unabhängigen Kontrollrats bestätigt wurde. Etwas anderes gilt nur dann, wenn der Unabhängige Kontrollrat die Fortgeltung der sofortigen Vollziehbarkeit explizit beschlossen. Sollte dies nicht der Fall sein, so ist die Maßnahme unverzüglich zu beenden. Dabei ist klarstellend aufgenommen, dass die „operative Sicherheit“ bei der Prüfung der Unverzüglichkeit zu berücksichtigen ist – es kann mit erheblichen Schwierigkeiten und Risiken verbunden sein, einen Einsatz sofort zu beenden, sodass ein geregelter Abbruch möglich und das Gebot sein muss.

Zu Absatz 4

Ist es dem Unabhängigen Kontrollrat aus Gründen, die in seinem Organisationsbereich liegen (also etwa bei besonders umfangreichen Vorgängen, dezidiert organisatorischen Gründen oder weil die Rechtssache eine besondere Schwierigkeit oder Bedeutung aufweist und deswegen zusätzliche Informationsbedarfe erkannt werden, die bei Vorlage an den Unabhängigen Kontrollrat noch nicht bekannt oder erwartbar waren) nicht möglich, innerhalb von drei Tagen eine Entscheidung herbeizuführen, so soll der zuständige Kollegialspruchkörper entscheiden, dass die Maßnahme (zunächst) weiter durchgeführt werden kann. In diesem Fall hat der Unabhängige Kontrollrat die Maßnahme unverzüglich – also ohne schuldhaftes Zögern – zu prüfen und ggf. zu bestätigen. Bei laufenden Maßnahmen gilt das zu Absatz 3 gesagte bezüglich ihrer Beendigung.

Zu Absatz 5

Wird die Anordnung nicht bestätigt, so dürfen die auf Grundlage der angeordneten sofortigen Durchführbarkeit erhobenen Daten nicht genutzt werden. Die Daten sind unverzüglich zu löschen, wenn kein Antrag nach Absatz 6 (Nachprüfung durch den Senat) gestellt wurde – Satz 2 Nummer 1 – oder wenn die Daten für eine Mitteilung an Betroffene oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Anordnung oder des Vorgangs von Bedeutung sein können – Satz 2 Nummer 2 –. In diesen Fällen ist die weitere Verarbeitung der Daten einzuschränken, im Falle von Satz 2 Nummer 1 endet diese Einschränkung mit einer (bestätigenden) Entscheidung des Senates.

Soweit ausnahmsweise bereits personenbezogene Daten übermittelt wurden, schließt die Löschpflicht insbesondere auch ein, dass die empfangende Stelle unverzüglich zur Löschung aufgefordert wird.

Zu Absatz 6

Der zuständige Nachrichtendienst hat die Möglichkeit, eine Entscheidung durch den Senat beantragen, wenn eine Anordnung außer Kraft getreten ist. Dieser hat, nachdem er den jeweiligen Nachrichtendienst unverzüglich angehört hat, gleichermaßen unverzüglich eine Entscheidung zu treffen.

Zu Unterabschnitt 2 (Rechtskontrolle durch das administrative Kontrollorgan)

Die administrative Kontrolle ist die datenschutzrechtliche Strukturkontrolle durch den Unabhängigen Kontrollrat. Sie ist geprägt von ihrer grundsätzlichen Anlassunabhängigkeit, wobei sie vom gerichtsähnlichen Kontrollorgan mit den Mitteln des Prüfprogramms und – bezogen auf den Bereich der strategischen Aufklärung für den Bundesnachrichtendienst – der Prüfaufträge gesteuert wird. Die Behördenleitung ist gegenüber dem administrativen Kontrollorgan weisungsbefugt. Diese Weisungsbefugnis wird um die materiellrechtlich erforderliche Weisungsbefugnis der einzelnen Mitglieder des gerichtsähnlichen Kontrollorgans sowie der Kollegialspruchkörper ergänzt, dies damit das administrative Kontrollorgan den Mitgliedern des gerichtsähnlichen Kontrollorgans seine fachliche Expertise zur Verfügung stellt.

Die Kontrolle ist prozessbegleitend ausgestaltet. Dabei kontrolliert das administrative Kontrollorgan sämtliche Verarbeitungen personenbezogener Datenverarbeitungen von Bundesnachrichtendienst und Bundesamt für Verfassungsschutz. Es ist somit insbesondere sichergestellt, dass keine Kontrolllücken entstehen, das gerichtsähnliche Kontrollorgan kontrolliert in der Vorabkontrolle den Einsatz besonders eingriffsintensiver nachrichtendienstlicher Mittel, das administrative Kontrollorgan kontrolliert – in der Strukturkontrolle – die Datenverarbeitung auch solcher Daten, die nicht mittels besonders eingriffsintensiver nachrichtendienstlicher Mittel erhoben wurden.

Die administrative Rechtmäßigkeitskontrolle hat über die für die Kontrolltätigkeit der Gesamtbehörde erforderliche besondere Expertise zu verfügen, da es sich – mit dem Ziel der Vermeidung geheimschutzbeeinträchtigender Schnittstellen – bei dem administrativen Kontrollorgan auch um das behördeneigene „Sachverständigenbüro“ handelt.

Wenngleich das administrative Kontrollorgan Beanstandungen und Anweisungen auf den Weg bringen kann, so kommen ihm doch keine abschließenden Entscheidungsbefugnisse zu. Das administrative Kontrollorgan agiert in seiner Kontrolltätigkeit nicht öffentlich. Begründet liegt dies nicht in der Art und Weise der Kontrolle, sondern in dem Kontrollgegenstand.

Im Bereich der oder des Ständigen Bevollmächtigten des Parlamentarischen Kontrollgremiums oder den integrierten Prüfstellen des Bundesrechnungshofes bestanden bereits ähnliche, administrative Kontrollfunktionen.

Stellt der Unabhängige Kontrollrat im Rahmen der administrativen Kontrolle einen Rechtsverstoß fest, so muss dieser der betroffenen Behörde oder auch der zuständigen Fachaufsicht mit dem Ziel der Abhilfe mitgeteilt werden. Die Feststellung eines rechtswidrigen Zustandes kann dabei einerseits einen Verstoß gegen die datenschutzrechtlichen Bestimmungen der nachrichtendienstlichen Bestimmungen betreffen. Zum anderen können auch qualifizierte Verstöße, etwa gegen das Erfordernis einer vorherigen Anordnung, in Betracht kommen. Im ersteren Fall kann der Unabhängige Kontrollrat, wie bisher der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, eine Beanstandung aussprechen. Im letzteren Fall kann eine bindende Anweisung erfolgen.

Zu § 32 (Administrative Kontrolle)

Zu Absatz 1

Die Zuständigkeit des administrativen Kontrollorgans ist einerseits datenschutzrechtlicher Natur (Nummer 1) und bezieht sich andererseits auf die erweiterten nachrichtendienstlichen Maßnahmen des Bundesnachrichtendienstes (Nummer 2).

Zu Nummer 1

Das administrative Kontrollorgan kontrolliert zuvorderst die datenschutzrechtliche Gesetzmäßigkeit der Aufgabenwahrnehmung der Nachrichtendienste des Bundes im Rahmen der Datenverarbeitung – also sowohl der Erhebung, der Weiterverarbeitung als auch der Übermittlung von personenbezogenen Daten durch die Nachrichtendienste. Kontrolllücken dürfen nicht entstehen, d.h. das administrative Kontrollorgang hat auch dort eine Zuständigkeit, wo das gerichtsähnliche Kontrollorgan nicht für die Vorabkontrolle zuständig ist. Die Kontrolltätigkeit des administrativen Kontrollorgans wird vom gerichtsähnlichen Kontrollorgan gesteuert. Dies erfolgt zentral über das Prüfprogramm sowie zum Teil über die Prüfaufträge (vgl. hierzu § 26). Bereits das Vorhandensein einer prozessbegleitenden administrativen Kontrolle ist geeignet, einer Überschreitung der gesetzlichen Befugnisse vorzubeugen (Alt, Kompensatorische Kontrolle heimlicher Grundrechtseingriffe, S. 209.)

Im Grundsatz erfolgt die datenschutzrechtliche Strukturkontrolle durch das administrative Kontrollorgan innerhalb des Prüfprogrammes dabei anlassunabhängig, d.h. eigeninitiativ. Dies verdeutlicht, dass gerade kein vorheriger Anlass für eine Prüfung – wie etwa im Rahmen einer Verlaufskontrolle – bestehen muss. Indes kann ein konkreter Anlass (etwa, weil ihm Rahmen der administrativen Kontrolle einer anderen Datenverarbeitungsstruktur, ein Kontrollbedürfnis indiziert wird) „erst recht“ eine administrative Kontrolle nach sich ziehen. Dem administrativen Kontrollorgan steht es insoweit frei, die Prozesse und Strukturen der Datenverarbeitung in den Nachrichtendiensten anhand von Stichproben auf ihre Rechtmäßigkeit zu überprüfen. Im Rahmen konkreter Prüfaufträge durch das gerichtsähnliche Kontrollorgan kann das administrative Kontrollorgan darüber hinaus auch gezielt die strategische Aufklärung des Bundesnachrichtendienstes überprüfen. Letzteres ist geboten, da die

strategische Aufklärung aufgrund ihrer großen Streubreite ein zusätzliches Korrektiv der Kontrolle benötigen (vgl. hierzu BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 272ff.), welches bei „gezielten“ Überwachungsmaßnahmen – insbesondere auch bei sog. CNE-Maßnahmen – nicht im gleichen Umfang erforderlich ist.

Zu Nummer 2

Neben der datenschutzrechtlichen Kontrolle kommt dem administrativen Kontrollorgan auch die Kontrolle über erfolgte erweiterte nachrichtendienstliche Maßnahmen des Bundesnachrichtendienstes zu. Dabei erstreckt sich die Kontrolltätigkeit hierbei primär darauf, ob der Bundesnachrichtendienst im Rahmen der Maßnahmen die gesetzlichen Bestimmungen des Abschnitt 4 des BND-Gesetzes eingehalten hat. Insbesondere eine Kontrolle der Zweckmäßigkeit einzelner Maßnahmen, der politischen Implikationen oder der etwaigen völkerrechtlichen Bedeutung erfolgt nicht.

Zu Absatz 2

Die administrative Kontrolle gewährleistet die Kontrolle der Datenverarbeitung im Rahmen der Aufgabenwahrnehmung der Nachrichtendienste und die nachträgliche Kontrolle erweiterter nachrichtendienstlicher Maßnahmen. Um dies zu gewährleisten, ist in Absatz 2 die Durchführung der Kontrolle als „anlassunabhängige“ und „strukturbezogene“ geregelt. Ersteres verdeutlicht, dass die Kontrolle nicht infolge konkreter Bezugspunkte erfolgen muss, sondern im Rahmen des Prüfprogrammes durch das gerichtsähnliche Kontrollorgans der administrativen Kontrolle selbst überantwortet bleibt, wie sie ihre Kontrolle ausübt. Letzteres (also der Strukturbezug) stellt klar, dass die Kontrolle nicht Einzelfälle in den Blick nimmt, sondern allgemeine Datenverarbeitungsprozesse und -strukturen kontrollieren soll. Dies schließt naturgemäß nicht aus, dass im Rahmen der Kontrolle auch Einzelvorgänge stichprobenartig in den Blick genommen werden können und müssen, da nur auf diese Weise eine umfängliche Kontrolle überhaupt möglich ist. Gleichwohl ist nicht Gegenstand der administrativen Kontrolle – und auch mit Blick auf die Kapazitäten des Kontrollorgans nicht erwartbar – dass eine einzelfallbezogene Verlaufskontrolle von Vorgängen erfolgt. Etwas anderes gilt insoweit nur dann, wenn ein konkreter Prüfauftrag nach Maßgabe des § 26 Absatz 3 vergeben wurde.

Zu § 33 (Beanstandungen; Unterrichtungen)

Die Vorschrift entspricht im Wesentlichen § 16 Absatz 2 des Bundesdatenschutzgesetzes, der für den oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit bislang das Beanstandungsrecht gegenüber öffentlichen Stellen des Bundes regelte. Neu ist nunmehr, dass der Unabhängige Kontrollrat im Geltungsbereich dieses Gesetzes an die Stelle der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit tritt. Dabei wird die Vorschrift moderat auf die Bedürfnisse des Unabhängigen Kontrollrats angepasst. Insbesondere ist die Beanstandung als „Kann-Vorschrift“ ausgestaltet. Die in § 16 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes vorgesehene Möglichkeit, von einer Beanstandung abzusehen, geht damit bereits in der Ermessensvorschrift selbst auf.

Wann von einer Beanstandung abzusehen ist, steht im pflichtgemäßen Ermessen des Unabhängigen Kontrollrats. Wie im Rahmen des § 16 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes kann ein Absehen in der Regel geboten sein, wenn und soweit es sich bei dem im Rahmen der administrativen Kontrolle festgestellten Verstoß um unerhebliche oder inzwischen beseitigte Mängel handelt.

Zu § 34 (Qualifizierter Verstoß; Anweisungen)

Die Regelung schafft für den Sachverhalt qualifizierter Rechtsverstöße einen Eskalationsmechanismus, welcher nach erfolgloser Durchlaufung eines Beanstandungsverfahrens nach § 33 Absatz 1 greift. Die Regelung stellt sicher, dass die integrale Kontrolle die Beachtung besonderer Schutzvorschriften final durch das gerichtsähnliche Kontrollorgan

durchsetzen kann. Dadurch kann insbesondere Auslegungsdivergenzen vorgebeugt oder abgeholfen werden.

Im bisherigen BND-Gesetz und bezogen auf die Rechtmäßigkeitskontrolle über die technische Aufklärung stand dem Unabhängigen Kontrollrat im dort noch als Beanstandungen genannten Verfahrensgang ebenfalls eine abschließende Entscheidungsbefugnis zu, vgl. § 52 des BND-Gesetzes. Das dort noch gestufte Verfahren wurde sachgerecht mit der Novellierung vereinfacht.

Zu Absatz 1

Das administrative Kontrollorgan übt im Rahmen seiner Zuständigkeit die Rechtskontrolle aus. Folgemaßnahmen knüpfen mithin an einen von dem administrativen Kontrollorgan festgestellten Verstoß gegen Rechtsvorschriften an. Wenn es sich bei der nach Auffassung des administrativen Kontrollorgans verletzten Vorschrift um eine der genannten besonderen Vorschriften (qualifizierter Verstoß) handelt, eröffnet dies die Vorlage zur rechtlich bindenden Folgeentscheidung des gerichtsähnlichen Kontrollorgans in Gestalt des Senats. Bei diesen Vorschriften handelt es sich grundsätzlich um Regelungen, die das Erfordernis einer unabhängigen Vorabkontrolle begründen oder spezielle Folgemaßgaben zu Eingriffen, die der Vorabkontrolle unterliegen, treffen.

Zu Nummer 1

Regelungen, die eine unabhängigen Vorabkontrolle oder Einzelfallkontrolle durch das gerichtsähnliche Kontrollorgan vorsehen, sind besondere Schutzvorschriften. Solche Schutzvorschriften sind mithin z.B. die Regelungen, die für längerfristige Observationen eine unabhängige Anordnungskontrolle vorsehen (wie § 9n Absatz 1 Nummer 3 BVerfSchG). Stellt das administrative Kontrollorgan bei seiner Kontrolle etwa fest, dass eine Observation durchgehend so lange durchgeführt worden ist, dass dazu eine unabhängige Anordnungskontrolle erforderlich war, ohne dass diese erfolgt ist, kann der Unabhängige Kontrollrat eine Anweisung dazu aussprechen, wie mit den gewonnenen Informationen umzugehen ist. Diese Anweisung ist für den Nachrichtendienst bindend. Im Unabhängigen Kontrollrat zuständig für rechtlich bindende Entscheidungen ist das gerichtsähnliche Kontrollorgan.

Zu Nummer 2

Im Rahmen der Vorabkontrolle kann das gerichtsähnliche Kontrollorgan seine Entscheidung zur Durchführbarkeit der Maßnahmenanordnung auch mit Maßgaben versehen, die die Rechtmäßigkeit der Durchführung sichern. Solche Maßgaben sind rechtlich bindend. Werden sie bei der Durchführung missachtet, verstößt der Nachrichtendienst gegen das gesetzliche Erfordernis der Vorabkontrolle, weil er insoweit aus dem gebilligten Rahmen ausbricht. Gleichermaßen kann das gerichtsähnliche Kontrollorgan auch bei seiner Prüfung im Rahmen der Einzelfallkontrolle Maßgaben treffen. Diese schließen insbesondere auch ein, dass das gerichtsähnliche Kontrollorgan zu dem Schluss kommt, dass ein rechtswidriger Zustand vorliegt. Der jeweilige Nachrichtendienst ist in diesen Fällen gehalten, den rechtswidrigen Zustand zu beseitigen. Kommt er dem nicht nach, liegt gleichermaßen ein Verstoß im Sinne der Nummer 2 vor.

Stellt das administrative Kontrollorgan bei seiner Kontrolle einen solchen Verstoß fest, ist ebenso die Möglichkeit einer bindenden Anweisung zu den Folgen dieses Fehlers bei der Datenweiterverarbeitung eröffnet.

Zu Nummer 3

Die Nummer 3 erfasst solche Bestimmungen, die spezielle Weiterverarbeitungsregelungen spezifisch für die Informationen treffen, die unter Eingriffen gewonnen worden sind, die der gerichtsähnlichen Vorabkontrolle oder der Einzelfallkontrolle unterliegen. Dies betrifft vornehmlich besondere Zweckbindungen (z.B. für Informationen aus Wohnraumüberwachung,

vgl. § 9h Absatz 5 BVerfSchG), aber auch besondere Verfahrensmaßgaben (vgl. § 9h Absatz 7 BVerfSchG), wobei sich der Kontroll- und Anweisungsrahmen des Unabhängigen Kontrollrats auf die Datenverarbeitung durch die Nachrichtendienste des Bundes beschränkt, diese mithin seine alleinigen Anweisungsadressaten sind.

Zu Absatz 2

Absatz 2 bestimmt den Senat als den Spruchkörper, der die Anweisung zur Abhilfe ausspricht; zudem finden sich dort Ausführungen zum Verfahren und zur Möglichkeit, eine unverzügliche Umsetzung oder eine Umsetzung innerhalb einer vom Senat bestimmten Frist anzuweisen.

Der Senat befasst sich mit der Anweisung in einem gestuften Verfahren. Zunächst hört der Senat den betroffenen Nachrichtendienst an. Sodann prüft er den mutmaßlichen Rechtsverstoß. Schließlich gewichtet der Senat den Sachverhalt z.B. im Hinblick auf die konkrete Art des Rechtsverstoßes.

Die mögliche Anweisung bezweckt, einem festgestellten Rechtsverstoß abzuhelfen. Dabei ist der Schutzzweck der verletzten Norm zu würdigen. Ist eine gerichtsähnliche Vorabkontrolle rechtswidrig unterblieben, war die durchgeführte Anordnung aber materiell rechtmäßig (d.h. hätte die Durchführung der gerichtsähnlichen Vorabkontrolle die Durchführbarkeit der Maßnahme bestätigt), ist eine Anweisung zur Löschung der erlangten Informationen zur Durchsetzung des materiellen Rechts nicht veranlasst. Der Unabhängige Kontrollrat kann aber eine bindende Feststellung der formellen Rechtswidrigkeit aussprechen. Dies ist insbesondere bedeutsam, wenn dadurch etwaige Auslegungsfragen zu den anzuwendenden Rechtsvorschriften geklärt werden. Damit schafft das gerichtsähnliche Kontrollorgan Rechtssicherheit für die künftige Verfahrensweise. Das gerichtsähnliche Kontrollorgan kann die Feststellungen aus dem Anweisungsverfahren dazu nutzen, Schwerpunkte der Kontrollsteuerung z.B. für das Prüfprogramm zu identifizieren. Hat der Senat eine Frist bestimmt, so hat der Nachrichtendienst die Anweisung innerhalb dieser Frist umzusetzen. Anderenfalls hat die Umsetzung ohne schuldhaftes Zögern zu erfolgen.

Zu Abschnitt 4 (Zusammenarbeit des Unabhängigen Kontrollrats mit dem Parlamentarischen Kontrollgremium)

Zu § 35 (Tätigkeitsbericht)

Mit den regelmäßigen Tätigkeitsberichten des Unabhängigen Kontrollrats an das Parlamentarische Kontrollgremium schließt sich der Kontrollkreislauf zwischen der integrierten Rechtmäßigkeitskontrolle über die Nachrichtendienste des Bundes und der parlamentarischen Kontrolle. Dabei kommt dem parlamentarischen Kontrollgremium als politischem Kontrollorgan, welches mit gewählten Abgeordneten über eine besondere demokratische Legitimität verfügt, eine besondere Bedeutung zu.

Zu Absatz 1

Der Tätigkeitsbericht umfasst einerseits die Kontrollzuständigkeiten des gerichtsähnlichen Kontrollorgans (Vorabkontrolle sowie Einzelfallkontrolle). Dem gerichtsähnlichen Kontrollorgan steht es, wie bisher, frei, bei dieser Gelegenheit auch grundsätzliche Stellungnahmen zu z.B. Rechtsfragen zu treffen oder über die behördliche Entwicklung zu berichten.

Andererseits hinaus wird im Tätigkeitsbericht über die Durchführung der administrativen Kontrolle berichtet. Diese entwickelt sich anhand der Vorgaben des Prüfprogramms. Dem Parlamentarischen Kontrollgremium wird so das strukturierte Nachvollziehen der konkreten Kontrolltätigkeit des administrativen Kontrollorgans möglich.

Zu Absatz 2

Absatz 2 überträgt die Regelung des bisherigen § 55 Absatz 2 Satz 1 bis 3 des BND-Gesetzes in das UKRat-Gesetz. Der Tätigkeitsbericht befasst sich mit allen Aspekten der Kontrollausübung. Der Bericht hat den Geheimschutz und die Grenzen der Verfügungsberechtigung der Nachrichtendienste des Bundes zu beachten. Dadurch ergeben sich vor allem Grenzen hinsichtlich Informationen, die von Nachrichtendiensten anderer Staaten geteilt wurden. Doch auch für solche Informationen regelt Absatz 2 ein Verfahren, um darüber möglichst auch das Parlamentarische Kontrollgremium zu unterrichten.

Ferner regelt Absatz 2 im letzten Satz, dass Angaben zur Kontrolltätigkeit mit Bezug zum Einsatz menschlicher Quellen, zu nachrichtendienstlicher Technik und nachrichtendienstlicher Methodik allgemein zu halten sind. Diese Vorgaben sollen die parlamentarische Kontrolle nicht begrenzen. Vielmehr muss es dem Unabhängigen Kontrollrat gelingen, so über seine Kontrolltätigkeit zu berichten, dass die parlamentarische Kontrolle ggf. erforderliche Ableitungen und gesetzgeberische Handlungsbedarfe erkennt. Zugleich muss der Schutz von Leib und Leben menschlicher Quellen gewährleistet sein und die damit direkt verbundene Funktionsfähigkeit der Nachrichtendienste des Bundes. Denn bereits der Anschein eines nicht absoluten Schutzes menschlicher Quellen wirkt abschreckend. Besonders schützenswert sind ebenfalls die nachrichtendienstliche Technik und nachrichtendienstliche Methodik, auch insoweit soll der Tätigkeitsbericht allenfalls und nur falls erforderlich allgemeine Angaben enthalten.

Zu Absatz 3

Absatz 3 übernimmt die Inhalte des bisherigen § 55 Absatz 2 Satz 4 und Satz 5 und verallgemeinert aufgrund der Zuständigkeitserweiterung des Unabhängigen Kontrollrats die Regelung mit dem Bezug auf die zuständige Aufsichtsbehörde. Die Vorschrift wurde zudem dahingehend erweitert, dass eine Ablehnung von „nur“ bestimmten Teilen eines Tätigkeitsberichts, einer Übermittlung der übrigen Teile nicht entgegensteht.

Zu Nummer 1

Die Übermittlung eines Berichts an das Parlamentarische Kotrollgremium nach Absatz 1 kann die zuständige Aufsichtsbehörde ablehnen, soweit dies aus Gründen des Wohls des Bundes oder eines Landes, insbesondere aus zwingenden Gründen des Nachrichtenzugangs oder aus Gründen des Schutzes von Persönlichkeitsrechten Dritter notwendig ist. Dieses Recht flankiert die Schutzgüter, die sich bereits im Absatz 3 niederschlagen, und wird ergänzt um den Schutz von Persönlichkeitsrechten Dritter.

Zu Nummer 2

Ergänzend ist der Aufsichtsbehörde ebenfalls möglich, die Übermittlung eines Berichtes unter Begründung abzulehnen, soweit der Kernbereich der exekutiven Eigenverantwortung betroffen ist.

Zu § 36 (Öffentlicher Bericht)

Es wird eine öffentliche Berichtslegung des Unabhängigen Kontrollrats eingeführt. Eine öffentliche Berichtslegung von Kontrollorganen über die Nachrichtendienste ist z.B. aus den Niederlanden bekannt, vgl. den „Annual report“ des Review Committee on the Intelligence and Security Services (CTIVD) oder aus dem Vereinigten Königreich, vgl. „Annual Report“ des Investigatory Powers Commissioner’s Office (IPCO).

Ein öffentlicher Bericht schafft Transparenz in die Rechtmäßigkeitskontrolle über die Nachrichtendienste des Bundes und bewirkt eine kontinuierliche Sichtbarkeit des Unabhängigen Kontrollrats in der Öffentlichkeit. Gewählt wird ein Zweijahresrhythmus. Die Art und Weise

der Veröffentlichung bleibt dem Unabhängigen Kontrollrat überlassen. Vorstellbar ist jedenfalls eine Bereitstellung im Internet.

Zu Absatz 1

Absatz 1 definiert den öffentlichen Bericht und sieht ihn in einem zweijährigen Turnus, erstmals für den Zeitraum 2024 bis 2025, vor. In Satz 2 wird dieser Bericht auch inhaltlich dahingehend vorgeprägt, dass er Ausführungen zu rechtlichen Bewertungen enthalten kann. Dadurch wird etwa auch die Veröffentlichung der vom Unabhängigen Kontrollrat entwickelten Leitsätze möglich.

Zu Absatz 2

Im weiteren Verfahren übermittelt der Unabhängige Kontrollrat den öffentlichen Bericht an den Deutschen Bundestag sowie die Bundesregierung und macht ihn der Öffentlichkeit zugänglich. Wie dies geschieht, steht dem Unabhängigen Kontrollrat frei. Der im Deutschen Bundestag federführende Ausschuss holt vor seiner Beratung eine Stellungnahme der Bundesregierung ein und beteiligt das Parlamentarische Kontrollgremium.

Zu § 37 (Austausch mit dem Parlamentarischen Kontrollgremium und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit)

Der Regelungsinhalt des bisherigen § 58 BND-Gesetz wird in § 37 aufgegriffen. Durch die Konsolidierung der Kontrolle beim Unabhängigen Kontrollrat konnte die Vorschrift dabei vereinfacht werden. Ergänzend sei an dieser Stelle darauf hingewiesen, dass es dem Unabhängigen Kontrollrat – schon aufgrund des Umstandes, dass seine Kontrolltätigkeit sich (primär) auf den Datenschutz (in seiner speziellen, nachrichtendienstrechtlichen Ausgestaltung) bezieht, unbenommen bleibt, den kontinuierlichen Austausch mit anderen Datenschutzbehörden (insbesondere der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit) zu suchen und zu pflegen, solange hierbei keine geheimhaltungsbedürftigen Informationen, sondern allgemeine datenschutzrechtliche Fragen und Erfahrungen in der Kontrolle geteilt werden.

Zu Absatz 1

Absatz 1 führt aus, dass die Rechte des Parlamentarischen Kontrollgremiums durch die Tätigkeit des Unabhängigen Kontrollrats unberührt bleiben. Die Vorschrift entspricht dem bisherigen § 58 Absatz 2 BND-Gesetz. Es gibt somit eine ergänzende, keine verdrängende Zuständigkeit des Unabhängigen Kontrollrats.

Zu Absatz 2

Absatz 2 eröffnet es dem Unabhängigen Kontrollrat sich regelmäßig mit dem Parlamentarischen Kontrollgremium über Angelegenheiten der Kontrolltätigkeit auszutauschen. Dies gilt im Rahmen der jeweiligen Kontrollzuständigkeit. Zudem sind weiterhin die geltenden Geheimhaltungsvorschriften zu wahren. Absatz 2 nimmt damit im Wesentlichen die Regelungsinhalte des bisherigen § 58 Absatz 1 des BND-Gesetzes auf.

Zu Absatz 3

In Absatz 3 wird dem Unabhängigen Kontrollrat die Möglichkeit eröffnet, sich mit der oder dem Bundesbeauftragten für Datenschutz und Informationsfreiheit auszutauschen. Dabei sind die geltenden Geheimhaltungsvorschriften auch hier zu wahren, ein Austausch zu konkreten operativen Einzelfällen/-fragen scheidet daher aus. Es besteht jedoch die Möglichkeit zur Erörterung der rechtlichen Bewertung eines typisierten Sachverhalts wie beispielsweise dem Ankauf von Daten durch Sicherheitsbehörden. Hintergrund für die Regelung ist, dass der Sachverstand der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Bezug auf den Datenschutz genutzt werden soll und eine einheitliche

Auslegung von datenschutzrechtlichen Fragestellungen dadurch sichergestellt werden soll. Die Third Party Rule gilt es stets zu beachten (Satz 2).

Zu Abschnitt 5 (Sonstige Vorschriften und Schlussvorschriften)

Zu § 38 (Individuelles Ersuchen beim Unabhängigen Kontrollrat)

Die Tätigkeiten der Nachrichtdienste des Bundes bleibt naturgemäß weitgehend im Verborgenen. Zwar hat der Einzelne gewisse Auskunftsrechte wie z.B. nach § 9 des BND-Gesetzes oder § 15 des Bundesverfassungsschutzgesetzes. Doch bereits die Auskünfte nach dem Informationsfreiheitsgesetz sind bezogen auf die Nachrichtendienste beschränkt. Die Einführung eines individuellen Petitionsrechts beim Unabhängigen Kontrollrat, welches dort eine Prüfung in Gestalt einer „objektivrechtlichen Kontrolle“ (BVerfG 1 BvR 2835/17 Rn. 280) auslöst, kompensiert die für eine effektive Aufgabenwahrnehmung erforderlichen Limitierungen. Sie findet sich in ähnlicher Form auch in § 15 Absatz 5 Satz 1 des Artikel 10-Gesetzes.

Jede Person kann beim Unabhängigen Kontrollrat eine Eingabe machen, wenn sie der Auffassung ist (und dies substantiiert vortragen kann), dass sie durch den jeweiligen Nachrichtendienst bei dessen Wahrnehmung der in § 2 Absatz 1 Nummer 1 bis 3 bezeichneten Aufgaben in ihren Rechten verletzt worden ist. Die eingebende Person hat einen substantiierten Sachverhalt sowie ein besonderes Interesse an der Prüfung darzulegen. Tut sie dies nicht, ist das Ersuchen bereits unstatthaft.

Der Unabhängige Kontrollrat prüft den Sachverhalt. Dabei obliegt es dem Unabhängigen Kontrollrat den für das Prüfvorhaben angezeigten behördeninternen Ablauf vorzusehen, z.B. mit der Prüfung das administrative Kontrollorgan zu befassen. Die Prüfung umfasst soweit aus Sicht des Unabhängigen Kontrollrat erforderlich z.B. das Einholen einer Stellungnahme beim jeweiligen Nachrichtdienst des Bundes oder eine Prüfung vor Ort. Dem Unabhängigen Kontrollrat steht es frei, die Entscheidung über Eingaben auch einem Mitglied des administrativen Kontrollorgans zuzuweisen. Sollte es zu einer Vielzahl von gleichgelagerten Eingaben kommen, insbesondere falls tatsächliche Anhaltspunkte dafür bestehen, dass diese Eingaben maschinell erstellt werden, lediglich pauschale Behauptungen einer Beeinträchtigung aufweisen, die Arbeit des Unabhängigen Kontrollrats behindern sollen oder offensichtlich missbräuchlich sind, kann der Unabhängige Kontrollrat die Ersuchen ohne inhaltliche Prüfung zurückweisen. Anderenfalls teilt der Unabhängige Kontrollrat der eingebenden Person mit, ob eine Verletzung ihrer Rechte festgestellt wurde. Bei seiner Antwort hat der Unabhängigen Kontrollrat an den Eingebenden Geheimschutzbelange umfassend zu berücksichtigten.

Zu § 39 (Schutz des Eigensicherungsbereichs)

Der Unabhängige Kontrollrat ist im Rahmen seiner Rechtskontrolle mit sehr sensiblen Vorgängen betraut. Dies folgt unmittelbar aus seiner Zuständigkeit für Kontrolle der Nachrichtendienste des Bundes, deren Arbeit in höchstem Maße geheimhaltungsbedürftig ist. Um diese Geheimhaltung (voll-)umfassend zu gewährleisten, muss auch die unabhängige oberste Bundesbehörde des Unabhängigen Kontrollrates in die Lage versetzt werden, seinen Eigensicherungsbereich abzusichern.

Die Vorschriften sind in weiten Teilen dem BVerfSchG und dem MAD-Gesetz nachempfunden, sodass allgemein auf die Begründung dieser Gesetze (BT-Drs. 20/8626 und BT-Drs. 21/1846) verwiesen wird.

Zu Absatz 1

In Absatz 1 findet sich die Grundregelung für die Maßnahmen der Eigensicherung. Dies beinhaltet zum einen die Legaldefinition des (räumlichen) Eigensicherungsbereiches, welche der Definition im bisherigen § 26b Absatz 1 des Bundesverfassungsschutzgesetzes

entspricht. Zum anderen werden die Schutzobjekte der Eigensicherung benannt, wobei abermals § 26b des Bundesverfassungsschutzgesetzes (mit Ausnahme der für den Unabhängigen Kontrollrat entbehrlichen „Quellen“) Pate stand. Im Übrigen verweist Absatz 1 auf die „folgenden Absätze“ für einzelne Maßnahmen. Ausdrücklich aufgenommen ist ein Bezug auf das (unangetastet) bleibende Hausrecht, was verdeutlicht, dass die spezialgesetzlichen Vorschriften das Hausrecht nicht abschließend verdrängen.

Zu Absatz 2

Absatz 2 entspricht dem bisherigen § 26b Absatz 2 des Bundesverfassungsschutzgesetzes, der um eine Befugnis zur Identitätsfeststellung (Satz 2) ergänzt wurde.

Zu Absatz 3

Absatz 3 entspricht dem bisherigen § 26b Absatz 3 des Bundesverfassungsschutzgesetzes, dessen Nummer 4 insoweit erweitert wird, also nunmehr auch solche Gegenstände durchsucht werden können, die verdeckt eingebracht werden, um ihrerseits sicherheitsgefährdende oder geheimdienstliche Gegenstände einzubringen.

Zu Absatz 4

In Absatz 4 findet sich neben der im bisherigen § 26b Absatz 6 des Bundesverfassungsschutzgesetzes enthaltene Raumüberwachung durch Videotechnik auch die dem § 65c des BND-Gesetzes nachempfundene – verdachtsunabhängige – Befugnis, Räume zu durchsuchen.

Zu Absatz 5

Absatz 5 entspricht dem bisherigen § 26b Absatz 4 des Bundesverfassungsschutzgesetzes, der um eine Nummer 2 ergänzt wird. Hiernach dürfen auch vorschriftswidrig eingebrachte Gegenstände – z.B. ein Smartphone – sichergestellt und untersucht werden.

Zu Absatz 6

In Absatz 6 ist neben der allgemeinen Duldungs- und Mitwirkungspflicht die Befugnis enthalten, dass der Unabhängige Kontrollrat Maßnahmen außerhalb des originären Eigensicherungsbereichs durchführen darf, wenn sich eine Person einer personengerichteten Maßnahme entziehen will (Nummer 1) oder wenn ein Gegenstand in der unmittelbaren Nähe zum Eigensicherungsbereich gefunden wird (Nummer 2).

Zu Absatz 7

In Absatz 7 ist geregelt, in welchen Situationen der Einsatz von Mitteln der Eigensicherung (die in Absatz 8 näher aufgeführt sind) statthaft ist. Dies betrifft neben den Fällen, in denen eine der in den Absätzen 2 und 5 (auch in Verbindung mit Absatz 6) genannten Maßnahmen durchgeführt werden soll (Nummer 3) zusätzlich auch Fälle, in denen ein unbefugter Zugriff „abgewehrt“ werden muss (Nummer 1) oder eine gegenwärtige Gefahr abgewehrt werde muss (Nummer 2).

Zu Absatz 8

In Absatz 8 finden sich die konkreten Mittel der Eigensicherung, welche dem Unabhängigen Kontrollrat im Rahmen der in Absatz 7 genannten Situationen offenstehen. Die Vorschrift entspricht § 26 Absatz 6 des MAD-Gesetzes.

Zu Absatz 9

Die Vorschrift entspricht dem § 26b Absatz 9 des Bundesverfassungsschutzgesetzes.

Zu § 40 (Verfahren im Eigensicherungsbereich)

Die Vorschrift enthält – flankierend zu § 39 – Verfahrensvorschriften für die besonderen Eigensicherungsbefugnisse des Unabhängigen Kontrollrates. Für die in weiten Teilen den bisherigen Fachgesetzen der Nachrichtendienste entnommenen Vorschriften wird abermals ergänzend auf die Begründungen dieser Vorschriften verwiesen (BT-Drs. 20/8626, BT-Drs. 20/8627 und BT-Drs. 21/1846).

Zu Absatz 1

In Absatz 1 findet sich die – vergleichbar zum bisherigen § 65e Absatz 1 des BND-Gesetzes, § 26c Absatz 1 des Bundesverfassungsschutzgesetzes sowie § 26 Absatz 1 des MAD-Gesetzes – Erfordernis einer Anordnung der Behördenleitung (oder einer von dieser bestimmten Vertretung) für bestimmte Eigensicherungsbefugnisse. Entsprechend dem BND-Gesetz wird dabei nicht zwischen Anordnungen von Abteilungsleitungen und der „Amtsleitung“ (so im MAD-Gesetz und im Bundesverfassungsschutzgesetz) unterschieden, sondern stets von einer Anordnung der Behördenleitung ausgegangen (die aber freilich an eine Vertretung „frei“ delegiert werden kann).

Zu Absatz 2

Absatz 2 entspricht dem bisherigen § 26c Absatz 2 des Bundesverfassungsschutzgesetzes bzw. § 26 Absatz 2 des MAD-Gesetzes und § 65e Absatz 2 des bisherigen BND-Gesetzes.

Zu Absatz 3

Absatz 3 entspricht dem bisherigen § 26c Absatz 3 des Bundesverfassungsschutzgesetzes bzw. § 26 Absatz 3 des MAD-Gesetzes.

Zu Absatz 4

Absatz 4 entspricht dem bisherigen § 26c Absatz 4 des Bundesverfassungsschutzgesetzes bzw. § 26 Absatz 4 des MAD-Gesetzes sowie § 65f Absatz 5 des BND-Gesetzes.

Zu Absatz 5

Absatz 5 entspricht dem bisherigen § 26c Absatz 5 des Bundesverfassungsschutzgesetzes bzw. § 26 Absatz 5 des MAD-Gesetzes.

Zu Absatz 6

Absatz 6 entspricht dem bisherigen § 26c Absatz 6 des Bundesverfassungsschutzgesetzes sowie § 65h des BND-Gesetzes.

Zu Absatz 7

Absatz 7 entspricht dem bisherigen § 26c Absatz 8 des Bundesverfassungsschutzgesetzes bzw. § 26 Absatz 7 des MAD-Gesetzes. Es wird eine Zuständigkeit des Bundesverwaltungsgericht für Klagen gegen Maßnahmen nach § 39 festgelegt.

Zu § 41 (Evaluationsbericht)

In § 41 wird die Regelung des bisherigen § 61 des BND-Gesetzes übernommen. Dabei erfolgt eine Modifikation dahingehend, dass nur eine einmalige Evaluation der Tätigkeit des Unabhängigen Kontrollrats (zum 1. Januar 2030) erfolgt. Die bislang in § 61 enthaltene Vorgabe einer Evaluation nach fünf Jahren ist durch Neufassung der Vorschrift obsolet.

Zu § 42 (Übergangsregelungen)

Zu Absatz 1

Die Regelung stellt sicher, dass der im Jahr 2021 entstandene Unabhängige Kontrollrat fortbesteht, so dass auch die laufenden Amtszeiten der Mitglieder des gerichtsähnlichen Kontrollorgans angerechnet werden können. Zudem wird sichergestellt, dass auch die bislang durch den Unabhängigen Kontrollrat getroffenen Entscheidungen fortbestehen.

Zu Absatz 2

Die Wartezeit von vier Jahren wird mit der Schaffung des UKRat-Gesetzes auf fünf Jahre angehoben, vgl. § 19 Absatz 1. Für die Mitglieder des gerichtsähnlichen Kontrollorgans, die bis zum 31. Dezember 2026 und somit nach alter Rechtslage in das gerichtsähnliche Kontrollorgan gewählt wurden, soll die vierjährige Wartezeit fortgelten.

Zu Absatz 3

Die in § 38 enthaltene Möglichkeit, individuelle Ersuchen zu stellen, beginnt zum 1. Januar 2029. Hierdurch soll dem Unabhängigen Kontrollrat die Möglichkeit eingeräumt werden, zunächst die Arbeitsprozesse auf die zusätzlichen Zuständigkeiten umzustellen.

Zu Artikel 4 (Änderung des Bundesverfassungsschutzgesetzes zum 1. Januar 2030)

Der Artikel dient in Verbindung mit der diesbetreffenden Inkrafttretensregelung der Rechtsbereinigung, weil die danach gestrichene Regelung ab dem 1. Januar 2030 gegenstandslos ist.

Zu Artikel 5 (Änderung des Gesetzes über die Kontrolle von Kriegswaffen)

In § 15 Absatz 1 war bereits eine vollständige Befreiung vom Erfordernis einer Genehmigung – sowie der hieran anschließenden Pflichten – für bestimmte Behörden vorgesehen. Eine solche wird jetzt durch die hier vorgenommene Änderung im Hinblick auf die herausgehobene Bedrohungslage für Bedienstete des Bundesnachrichtendienstes, die häufig in Kriegs- und Krisenregionen reisen müssen, ebenfalls geschaffen. Es bedarf einer den Bundespolizeien etc. vergleichbaren Möglichkeit für eine Ausstattung mit Waffen nach dem Kriegswaffenkontrollgesetz. Insoweit ist es unerheblich, dass der Bundesnachrichtendienst keine polizeilichen Befugnisse ausübt (vgl. Steindorf/ Heinrich, 11. Aufl. 2022, Gesetz über die Kontrolle von Kriegswaffen, § 15 Rn. 1). Entscheidend ist vielmehr, dass der Bundesnachrichtendienst in Krisenszenarien und -regionen den Objektschutz seiner Liegenschaften und Infrastrukturen effektiv selbst wahrnehmen können muss sowie für den Schutz seiner Bediensteten und eingesetzten Personen sorgen können muss. Die Gesetzesänderung dient dem Wegfall der kriegswaffenkontrollrechtlichen Genehmigungspflichten, auch um in Krisensituationen flexibel zu sein. Ziel ist es hierbei, auch den Bundesnachrichtendienst von – teilweise auch in operativ- sicherheitlicher Hinsicht bedenklichem – Verwaltungsaufwand zu befreien (vgl. zu diesem übergeordneten Ziel der Regelung in § 15 Absatz 1 schon BT-Drs. III/1589, S. 23). Ohne eine Aufnahme des Bundesnachrichtendienstes in die Regelung des § 15 Kriegswaffenkontrollgesetz wäre dieser weiterhin gezwungen, für den Umgang mit Kriegswaffen regelmäßig typen- und mengenspezifische Genehmigungen durch das Bundesministerium für Wirtschaft und Energie (BMWE) einzuholen und die regelmäßigen Berichtspflichten des § 12 Kriegswaffenkontrollgesetzes (u.a. zu den aktuellen Kriegswaffenbeständen des Bundesnachrichtendienstes) gegenüber dem Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) zu erfüllen. Derartige Genehmigungsvorbehalte und Berichtspflichten sind vor dem Hintergrund des Auftrages des Bundesnachrichtendienstes und der verschärften Bedrohungslage, denen der Bundesnachrichtendienst wirksam und verzugslos begegnen muss, nicht sachgerecht. Die Ausnahme von der Anwendung des Kriegswaffenkontrollgesetzes wird durch die Einrichtung eines adäquaten behördeninternen Kontroll- und Sicherungssystems kompensiert. Hierdurch wird sichergestellt, dass eine

Zweckbegrenzung erfolgt. Der Einsatz von Kriegswaffen durch den Bundesnachrichtendienst dient insbesondere dem Zweck der Einsatzsicherung und der Sicherung der Bediensteten und Dienststellen. Ein Kontroll- und Sicherungssystem wird intern im Rahmen einer Dienstvorschrift festgelegt. Darin werden Vorgaben zum Umgang mit Kriegswaffen festgelegt. Dies betrifft insbesondere den berechtigen Personenkreis, das Transportieren sowie lageabhängige Führen von Kriegswaffen. Darüber hinaus werden Belehrungs- und Dokumentationspflichten festgelegt. Es erfolgt eine jährliche Belehrung der trageberechtigten Mitarbeitenden des Bundesnachrichtendienstes. Die Dokumentationspflichten betreffen sämtliche Ausbildungs- und Einsatzwaffen im Bundesnachrichtendienst samt zugehöriger Munition, Anzahl, Typ, Verbleib sowie der verwendenden Dienststellen im In- und Ausland. Die Dienstvorschrift bedarf der Zustimmung des Bundeskanzleramtes.

Zu Artikel 6 (Änderung des Informationsfreiheitsgesetzes)

Klarstellend werden die für die Nachrichtendienste des Bundes Fachaufsicht ausübenden obersten Bundesbehörden (also das Bundeskanzleramt für den Bundesnachrichtendienst, das Bundesministerium des Innern für das Bundesamt für Verfassungsschutz und das Bundesministerium der Verteidigung für das Bundesamt für den Militärischen Abschirmdienst) in die Bereichsausnahme des § 3 Nummer 8 aufgenommen (vgl. BVerwG, Urteil vom 25. Februar 2016, 7 C 18.14, Rn. 22). Gleiches gilt für den Unabhängigen Kontrollrat als Kontrollbehörde der Nachrichtendienste. Alle Tätigkeiten der Nachrichtendienste sollen nach dem Willen des Gesetzgebers vom Anspruch auf Informationszugang ausgeschlossen sein (BT-Drs. 15/4493, S. 12). Der Informationszugang bezüglich aller Vorgänge und aller Tätigkeiten der Nachrichtendienste ist gesperrt (BVerwG, Urteil vom 25. Februar 2016, 7 C 18.14, Rn. 22). Zudem soll sichergestellt werden, dass der mit der Bearbeitung von Informationszugangsanträgen verbundene Verwaltungsaufwand – dem ein „nicht unbeträchtliches Gewicht“ zukommt – nicht nur Nachrichtendiensten zugutekommt, sondern auch Behörden oder Teilen von Behörden, die aufgrund ihrer Aufgabenstellung in einer besonders engen Beziehung zu den Nachrichtendiensten stehen (vgl. BVerwG, Urteil vom 25. Februar 2016, 7 C 18.14). Bereits im bisherigen Recht wird insoweit ein „funktionsbezogen erweitertes Verständnis der Bereichsausnahme [der Nummer 8 angewandt], das auch das Bundeskanzleramt in seiner Eigenschaft als Aufsichtsbehörde über den Bundesnachrichtendienst und Koordinierungsstelle für die Nachrichtendienste einbezieht“ (vgl. BVerwG, a.a.O.). Die Änderung durch ausdrückliche Aufnahme dient insoweit der Rechtssicherheit. So kann sich etwa das Bundeskanzleramt dabei, soweit es seine Stellung als Fachaufsicht über den Bundesnachrichtendienst, oder seine Rolle als Koordinierungsstelle für die Nachrichtendienste betrifft, auf die Bereichsausnahme, die den Anspruch entfallen lässt und eine einzelfallbezogene Recherche entbehrlich macht, berufen.

Zusätzlich zu Nummer 8, die sachgerecht eine Behördenausnahme für Informationsansprüche gegen die dort genannten Stellen regelt, regelt zudem Nummer 9 nunmehr den Schutz der Informationen bei anderen Stellen des Bundes. Nummer 8 greift hier zu kurz, weil in den Fällen der zu schützende Bereich ungeschützt bleibt, wenn die Informationen bei anderen Stellen des Bundes vorliegen. Selbst bei Aufsichtsbehörden können ungeschützte Bereiche entstehen, wenn zwar Informationen der Stellen nach Nummer 8 vorliegen, diese aber nicht im Rahmen einer Aufsichtstätigkeit (z.B. Vereinsverbotsverfahren) vorgelegt wurden oder entstanden sind. Das vom Gesetzgeber in der bisherigen Fassung verfolgte Regelungsziel kann daher nur durch ein hinzutretendes informationsbezogenes Verständnis der Bereichsausnahme erreicht werden. Dem trägt die neue Nummer 9 Rechnung.

Andere Ausschlussbegründe des Informationsfreiheitsgesetzes belassen insbesondere eine Darlegungslast bei der Bundesbehörde, die bereits die zu wahrenden Schutzerwägungen gefährdet. Dies gilt umso mehr, als künftig die Möglichkeiten einer systematischen Ausforschung durch fremde Mächte über Anfragen nach dem Informationsfreiheitsgesetz mittels eines durch künstliche Intelligenz gestützten Anfragesystems sowie einer mittels künstlicher Intelligenz vorgenommenen Auswertung der dabei generierten Daten zu befürchten ist. Es sollen keine Anknüpfungspunkte für die Ausforschung der Nachrichtendienste

entstehen, die Rückschlüsse zulassen können, zu welchen Themen Dokumente der Nachrichtendienste erstellt und verteilt wurden. Zudem soll sichergestellt werden, dass der mit der Bearbeitung von Informationszugangsanträgen verbundene Verwaltungsaufwand – dem ein „nicht unbeträchtliches Gewicht“ zukommt (BVerwG, NVwZ 2016, 940, Rn. 22) – nicht nur Nachrichtendiensten sowie Bundesbehörden und sonstigen öffentlichen Stellen des Bundes, soweit sie Aufgaben im Sinne des § 10 Nr. 3 des Sicherheitsüberprüfungsgesetzes wahrnehmen, zugutekommt, sondern auch Bundesbehörden und anderen öffentlichen Stellen des Bundes, bei denen derartige Informationen vorliegen. Eine tatsächliche Verschlechterung der Rechtsstellung der Bürgerinnen und Bürger geht damit im Wesentlichen nicht einher, da im Einzelfall bereits jetzt im Ergebnis die inhaltliche Auskunft zu nachrichtendienstlichen Informationen über die anderen Ausschlussgründe verwährt ist.

Zu Artikel 7 (Änderung des Beamtenversorgungsgesetzes)

Es handelt sich um eine redaktionelle Klarstellung, weil auch in § 56 Bundesbesoldungsgesetz die besondere Auslandsverwendung - und zwar zwecks Feststellung eines Anspruchs auf Auslandsverwendungszuschlag - definiert wird. § 31a hingegen regelt den Anspruch auf Einsatzversorgung, den nur jene Beamtinnen und Beamten haben, die ausschließlich bei den in § 31a aufgelisteten besonderen Verwendungen im Ausland einen Einsatzunfall erleiden.

Zu Artikel 8 (Änderung des Bundesbesoldungsgesetzes)

Der Bundesnachrichtendienst setzt zur Erfüllung seines gesetzlichen Auftrages, der nachrichtendienstlichen Auslandsaufklärung, weltweit Mitarbeiterinnen und Mitarbeiter ein, um Informationen zu beschaffen. Im Rahmen dieser Auslandsverwendungen ist der Bundesnachrichtendienst nicht offen als staatlicher Akteur erkennbar, sondern agiert in der Regel verdeckt, um seinen Aufklärungszweck nicht zu gefährden. Diese spezifischen Fallkonstellationen von Auslandsverwendungen des Bundesnachrichtendienstes sind mit außergewöhnlichen Risiken und Gefährdungen verbunden, werden jedoch vom Anwendungsbereich des § 56 bislang nicht abgedeckt. So sind zahlreiche Auslandsverwendungen des Bundesnachrichtendienstes nicht von der Legaldefinition der „besonderen Verwendung im Ausland“ nach § 56 Absatz 1 Satz 1 erfasst. Wird beispielsweise ein Angehöriger des Bundesnachrichtendienstes ohne Kenntnis des betreffenden Staates in einem Krisengebiet eingesetzt, besteht häufig kein Anspruch auf Auslandsverwendungszuschlag. Dies betrifft auch Ad-hoc-Einsätze, in denen die Bundesregierung darauf angewiesen ist, dass der Bundesnachrichtendienst kurzfristig mit nachrichtendienstlichen Mitteln Informationen im Ausland beschafft. In Bezug auf die durch den Auslandsverwendungszuschlag abzugeltenden Belastungen besteht kein Unterschied zwischen offen und verdeckt operierenden Mitarbeiterinnen und Mitarbeitern staatlicher Institutionen, der die nach bisheriger Gesetzeslage bestehende Differenzierung beim Auslandsverwendungszuschlag rechtfertigen würde. Zwar sind verdeckt tätige Mitarbeiterinnen und Mitarbeiter des Bundesnachrichtendienstes nicht offen als Hoheitsträger erkennbar. Wird jedoch die verdeckte Tätigkeit dieser Personen Dritten bekannt, drohen den Angehörigen des Bundesnachrichtendienstes deutlich schwerwiegendere Folgen (wie etwa langjährige Haftstrafen, Entführung, Verschleppung, Folter und Hinrichtung). Anders als offen tätige Mitarbeiterinnen und Mitarbeiter anderer staatlicher Institutionen können sich verdeckt operierende Angehörige des Bundesnachrichtendienstes grundsätzlich im Notfall nicht auf im Ausland vorhandene militärische Infrastruktur stützen. Weitere Schutzkomponenten wie militärische Bewaffnung, gepanzerte Fahrzeuge oder ein enger Kontakt zur deutschen Botschaft stehen den verdeckt operierenden Angehörigen des Bundesnachrichtendienstes regelmäßig nicht zur Verfügung, was die Gefahr für Leib und Leben durch Terrorakte und (para-)militärische Gewalt erheblich erhöht. Das hohe Risiko der verdeckt operierenden Angehörigen des Bundesnachrichtendienstes führt regelmäßig zu einer erheblichen psychischen Belastung, die durch die eingeschränkten Kontaktmöglichkeiten zu Angehörigen noch verstärkt wird.

Die Anpassung des § 56 gewährleistet auch bei verdeckten Operationen des Bundesnachrichtendienstes im Ausland eine Abgeltung der Belastungen.

Mit Blick auf das besondere Geheimhaltungsbedürfnis und eine Verwaltungsvereinfachung wird im Gleichklang zu den Spezialkräften der Bundeswehr (§ 56 Absatz 2 Satz 2 Nummer 1) und den Angehörigen der GSG 9 der Bundespolizei (§ 56 Absatz 2 Satz 2 Nummer 2) für die Angehörigen des Bundesnachrichtendienstes ein Tatbestand (§ 56 Absatz 2 Satz 2 Nummer 3 neu) innerhalb der bestehenden Regelungen zur besonderen Auslandsverwendung geschaffen. Es ist insofern in der Konstellation nach § 56 Absatz 2 Satz 2 Nummer 3 nicht erforderlich, dass kumulativ die tatbestandlichen Voraussetzungen des § 56 Absatz 1 Satz 1 vorliegen. Dies hat den Hintergrund, dass bei einer verdeckten Verwendung von Angehörigen des Bundesnachrichtendienstes im Ausland in der Regel kein Übereinkommen, kein Vertrag sowie keine Vereinbarung mit den dort genannten Einrichtungen oder Staaten im Sinne des § 56 Absatz 1 Satz 1 vorliegt.

Um die besonderen Anforderungen sowie außergewöhnlichen Risiken und Gefährdungen der Angehörigen des Bundesnachrichtendienstes bei der Erfüllung ihres anspruchsvollen Auftrags in allen Einsatzgebieten im Ausland angemessen abgelten zu können, sollen diese den Auslandsverwendungszuschlag der höchsten Stufe nach § 56 Absatz 3 erhalten.

Dem Bundeskanzleramt obliegt die Festlegung von Maßnahmen als besondere Verwendung der Angehörigen des Bundesnachrichtendienstes im Ausland im Sinne des § 56 Absatz 2 Satz 2 Nummer 3. In diesem Rahmen bedarf es keiner konkret-individuellen Regelung, vielmehr genügt bereits eine abstrakte Festlegung von typisierten besonderen Verwendungen der Angehörigen des Bundesnachrichtendienstes im Ausland.

Im Falle einer Auslandsverwendung von Angehörigen des Bundesnachrichtendienstes erfolgt keine Differenzierung zwischen der Verwendung in einem Verband, einer Einheit oder Gruppe einerseits und der Einzelverwendung andererseits. Der Auslandsverwendungszuschlag wird insofern gegenüber Angehörigen des Bundesnachrichtendienstes stets auch dann gezahlt, wenn diese sich im Rahmen einer Einzelverwendung im Ausland aufhalten und die Voraussetzungen des § 56 Absatz 2 Satz 2 Nummer 3 vorliegen.

Aufgrund der gesetzlichen Bestimmung des § 56 Absatz 3 Satz 6, aus dessen Verweisung sich ergibt, dass der Tagessatz für Mitarbeitende des Bundesnachrichtendienstes auf der Höchststufe geleistet wird, wird von einer Aufnahme des Bundeskanzleramtes in die Aufzählung des § 56 Absatz 6 abgesehen.

Zu Artikel 9 (Änderung des Bundespersonalvertretungsgesetzes)

Zu Nummer 1

Die Vorschrift des § 55 Absatz 2 soll Personalräte grundsätzlich davor schützen, gegen ihren Willen an eine andere Dienststelle umgesetzt zu werden, solange sie Mitglied im örtlichen Personalrat sind. Da im Geschäftsbereich des Bundesnachrichtendienstes auch Personalräte in Dienststellen im Ausland vertreten sein können, kann der Fall entstehen, dass ein Personalrat an einer Auslandsvertretung unter Verweis auf § 55 Absatz 2 BPersVG versucht, die – beim Bundesnachrichtendienst ähnlich wie im Auswärtigen Amt – nach dem Rotationsprinzip von vorneherein begrenzte Stehzeit zu verlängern. Die Änderung entspricht insoweit der Regelung des § 121 Absatz 5 BPersVG, in dem für das Auswärtige Amt der § 55 Absatz 2 BPersVG abbedungen ist, um der dort üblichen Rotation beim Personaleinsatz Rechnung zu tragen.

Zu Nummer 2

Die Ergänzung übernimmt die zum BND mit § 112 Absatz 2 und zum MAD mit § 117 Absatz 6 getroffenen Regelungen für das BfV, da die zugrunde liegenden Erwägungen zur

Funktionsfähigkeit der Personalvertretung und zur Gewährleistung von Geheimschutz bei einem Nachrichtendienst hier ebenso einschlägig sind.

Bei der Tätigkeit im BfV handelt es sich um eine sicherheitsempfindliche Tätigkeit. Für alle Bediensteten ist daher nach § 10 Nummer 3 des Sicherheitsüberprüfungsgesetzes grundsätzlich eine erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen durchzuführen. Eine solche ist nach § 14 Absatz 5 Satz 2 des Sicherheitsüberprüfungsgesetzes notwendig, um mit der Wahrnehmung einer sicherheitsempfindlichen Aufgabe betraut zu werden.

Die Aufgaben eines Mitglieds des Personalrats beim BfV bringen es zwangsläufig mit sich, dass Zugang zu geheimhaltungsbedürftigen Informationen besteht. Daher müssen auch die Mitglieder des Personalrats für eine sicherheitsempfindliche Tätigkeit zugelassen sein. Liegt in der betroffenen Person ein Sicherheitsrisiko vor, ist sie nicht mehr für eine sicherheitsempfindliche Tätigkeit zugelassen und damit auch nicht mehr für eine Tätigkeit im Personalrat. Dies wird nunmehr auch zum BfV im Bundespersonalvertretungsgesetz mit dem neuen Absatz 4 des § 113 speziell geregelt. Da das Personalratsmitglied in diesem Fall an der Ausübung seines Amtes gehindert ist, tritt nach § 33 Absatz 1 Satz 2 des Bundespersonalvertretungsgesetzes für die Dauer des Ruhens der Mitgliedschaft ein Ersatzmitglied ein.

Zu Artikel 10 (Änderung des Vereinsgesetzes)

Zu Nummer 1

Die Nummer gleicht die nebenstrafrechtliche Bestimmung an die Straftatbestände in § 86a StGB an und schließt dadurch Strafbarkeitslücken vor Bestands- bzw. Rechtskraft eines vollziehbaren Vereinsverbots. Zugleich wird damit auch die Strafbarkeit bei vereinsrechtlichen Betätigungsverboten entsprechend erweitert. Wegen der Komplementarität von § 20 VereinsG (vor Bestandskraft) und § 86a StGB (nach Bestandskraft) ist die inhaltliche Harmonisierung sachlich angezeigt. Mit der Angleichung können die verbotenen Kennzeichen - wie Fahnen, Abzeichen, Uniformstücke, Parolen und Grußformen - effektiver als bisher aus der Öffentlichkeit verbannt werden.

Zu Buchstabe a

Unter redaktioneller Anpassung der Nummer 4 (die Angabe „oder“ wird durch ein Komma ersetzt) wird in Nummer 5 die Tathandlung des Inhaltsverbreitens (§ 11 Absatz 3 StGB) ergänzt, wie bereits in § 86a Absatz 1 Nummer 1 StGB enthalten.

Die neue Nummer 6 übernimmt die Regelung des § 86a Absatz 1 Nummer 2 StGB.

Zu Buchstabe a

Zu Buchstabe b

Es handelt sich um eine redaktionelle Folgeänderung zu Buchstabe a.

Zu Nummer 2

Es handelt sich um eine redaktionelle Folgeänderung zu Nummer 1 Buchstabe a.

Zu Artikel 11 (Änderung des Bundeskriminalamtgesetzes)

Zu Nummer 1

Es handelt sich um eine Folgeänderung zur Ersetzung des früheren Bundesverfassungsschutzgesetzes durch die Neuverkündungen dieses Gesetzes, indem die Verweisung entsprechend angepasst wird.

Zu Nummer 2

Da es sich bei polizeilichen Ausschreibungen im Vergleich zu eingriffsintensiven nachrichtendienstlichen Mitteln um einen weniger gewichtigen Eingriff handelt (BVerfGE 165, 1 – Rn. 174), ist die bisherige Benachrichtigungsregelung für das Nachrichtendienstrecht sachwidrig. Im Sicherheitsrecht besteht eine materiespezifische Besonderheit des Nachrichtendienstrechts gegenüber dem Polizeirecht gerade darin, dass es von Transparenz- und Berichtspflichten gegenüber der betroffenen Person weithin freigestellt ist (s.o. Begründung zu Artikel 1 § 35). Die Benachrichtigung ist auch nicht unionsrechtlich determiniert, da Unionsrecht nach Artikel 4 Absatz 2 Satz 3 EUV auf die nachrichtendienstliche Aufgabenwahrnehmung im Bereich der nationalen Sicherheit nicht anzuwenden ist (BVerfG, Beschluss vom 8. Oktober 2024 - 1 BvR 1743/16 / 1 BvR 2539/16 – Rn. 77, 79).

Zu Artikel 12 (Änderung des Hochschulstatistikgesetzes)

Die Hochschulen und Prüfungsämter sind grundsätzlich dazu verpflichtet, semesterweise Daten über Studierendende, Prüfungsteilnehmende sowie Exmatrikulierte an die statistischen Landesämter zu melden. Vor dem Hintergrund der gesteigerten Bedrohungslage durch ausländische Nachrichtendienste wird im Rahmen der Novellierung in § 2 Absatz 2 Hochschulstatistikgesetz eine Bereichsausnahme geschaffen.

Die Bereichsausnahme betrifft die Erhebung statistischer Daten über das aktuelle und künftige Personal der Nachrichtendienste des Bundes und der Länder, soweit diese ein Studium oder eine Prüfung an einer Einrichtung im Sinne des § 2 Absatz 1 Hochschulstatistikgesetz absolvieren bzw. ablegen. Die Bereichsausnahme ist dabei auf diejenigen Studierenden, Prüfungsteilnehmenden sowie Exmatrikulierten begrenzt, die für die Nachrichtendienste des Bundes oder der Länder ausgebildet werde.

Dem in § 1 Absatz 1 Satz 2 Hochschulstatistikgesetz normierten Zweck, die statistischen Ergebnisse für Zwecke der Gesetzgebung und Planung im Hochschulbereich als Entscheidungsgrundlage nutzen zu können, steht das überragende Interesse der Nachrichtendienste des Bundes und der Länder am Schutz der Identität ihrer Mitarbeitenden sowie der Aufrechterhaltung ihrer jeweiligen Auftragserfüllung gegenüber.

Bei personenbezogenden Daten von Mitarbeitenden von Nachrichtendiensten des Bundes und der Länder handelt es sich um besonders schutzbedürftige Daten. Jede Übermittlung dieser sensiblen Daten stellt für sich ein Sicherheitsrisiko dar. Die Neuregelung zielt einerseits auf einen angemessenen Schutz der personenbezogenen Daten der Mitarbeitenden der Nachrichtendienste ab. Darüber hinaus sind bereits Aussagen zur Studierendenzahl der jeweiligen Nachrichtendienste an den Hochschulen, Prüfungsämter und Berufsakademien schutzbedürftig. Maßgeblich ist insoweit der Umstand, dass anhand dieser Daten weitere Aussagen zur gegenwärtigen Organisation, zu Personalbestand und -entwicklung sowie zu den damit korrespondierenden (auch perspektivischen) Aufklärungskapazitäten des jeweiligen Nachrichtendienstes abgeleitet werden können. Eine Weitergabe dieser Informationen an die Statistikämter muss daher auch zur Wahrung der Aufgabenerfüllung der Nachrichtendienste unterbleiben.

Zu Artikel 13 (Änderung des Aufenthaltsgesetzes)

Die Einfügung des Buchstaben b) in Nummer 2a, die insoweit rechtssystematisch umgestellt wurde, definiert für den Bereich der landesverräterischen und geheimdienstlichen Agententätigkeit ein besonders schwerwiegendes Ausweisungsinteresse. Damit wird die Gesetzeslage an die Regelung für Terrorismus in § 54 Absatz 1 Nummer 2 AufenthG angeglichen. Dies ist erforderlich, um die drohenden Gefahren seitens Agenten und Spionen fremder Mächte durch Ausweisung über die Versagung oder Entziehung des Aufenthaltstitels schnell begegnen zu können. Mit Blick auf die Veränderungen der Sicherheitslage in jüngerer Vergangenheit und die damit in Zusammenhang stehenden Tätigkeiten

ausländischer Nachrichtendienste ist die Änderung von großer Relevanz, was sich auch in der erfolgten Anhebung des Strafrahmens des § 99 des Strafgesetzbuches auf bis zu zehn Jahre Freiheitsstrafe niederschlägt

Zu Artikel 14 (Änderung der Verwaltungsgerichtsordnung)

Zu Nummer 1

Mit Nummer 1 wird die erstinstanzliche Zuständigkeit des Oberverwaltungsgerichts in Verfassungsschutz-Sachen begründet. Dies folgt der Zuständigkeitsentscheidung in § 99 Absatz 2 Satz 1 und bündelt damit auch gerichtliche Fachkompetenz, da im nachrichtendienstlichen Geschäftsbereich der Verfassungsschutzbehörden nach § 2 Absatz 1 und 4 BVerfSchG sowie des MAD nach § 2 Absatz 1 und 4 MADG naturgemäß Geheimschutzbelange regelmäßig berührt werden und dies nicht erst im Zwischenverfahren zu berücksichtigen ist. Eine spezielle gerichtliche Eingangszuständigkeit besteht mit § 50 Absatz 1 Nr. 4 bereits zum BND. Beim stärker im Inland tätigen BfV ist allerdings von einem Verfahrensaufkommen auszugehen, das eine erstinstanzliche Befassung des Bundesverwaltungsgerichts nicht gleichermaßen adäquat erscheinen lässt, so dass im Ergebnis die OVG-Ebene insgesamt sachgerecht ist.

Zu Nummer 2

Die neue Nummer 2a enthält einerseits eine Folgeänderung zu der im neuen § 34 Absatz 3 BVerfSchG (Artikel 1) aufgenommenen Zuständigkeitsregelung.

Korrespondierend zur Zuständigkeit nach der geltenden Nummer 2 zu Verbotsverfahren enthält die neue Nummer 2a zudem auch eine neue Eingangszuständigkeit zur vorlaufenden Öffentlichkeitsunterrichtung über extremistische Bestrebungen, sowohl über Verdachtsfälle als auch über eine Erkenntnislage, nach der die mitteilende Behörde (nach § 45 BVerfSchG das BfV oder das BMI) es als geklärt erachtet, dass extremistische Bestrebungen vorliegen (auch als „gesichert extremistisch“ bezeichnet).

Die bisherige Eingangszuständigkeit des Verwaltungsgerichts zu solchen Streitsachen der Öffentlichkeitsmitteilung führte über den Instanzenzug zu einer sehr langen Verfahrensdauer bis zum rechtskräftigen Abschluss. Dies ist gleichermaßen nachteilig für die von der negativen Etikettierung betroffene Vereinigung wie auch für öffentliche Interessen an verbindlicher Klärung, auch im Hinblick auf etwaige vereinsrechtliche Anschlussmaßnahmen. Deshalb ist hier eine Verfahrensbeschleunigung dringend geboten, die angemessen mit der Eingangszuständigkeit des Bundesverwaltungsgerichts erreicht wird. Dies ist auch sachlich naheliegend, weil das Bundesverwaltungsgericht bereits zu Verbotsverfahren zuständig ist, in denen sich inhaltlich zu großen Teilen gleiche Klärungsfragen stellen.

Die neue Nummer 2b legt eine neue Eingangszuständigkeit des Bundesverwaltungsgerichts für Klagen gegen Maßnahmen aus dem Eigensicherungsbereich des Unabhängigen Kontrollrates nach der § 39 des UKRat-Gesetzes fest.

Zu Artikel 15 (Änderung der Abgabenordnung)

Die Neufassung führt zu verbesserter Normenklarheit, indem nunmehr auch BfV, MAD und BND nicht lediglich in den Fachgesetzen, sondern auch überblicksmäßig in § 93 Absatz 8 Satz 1 Nummer 3 AO als abrufberechtigt aufgeführt werden. Eine besondere landesrechtliche Komplementärregelung speziell zum Kontostammdatenabruf (durch LfV) ist angesichts des geringen Eingriffsgewichts der Maßnahme nicht mehr vorausgesetzt, wie bereits aktuell nicht in Nummer 3 zum landespolizeilichen Abruf.

Zu Artikel 16 (Änderung des Zollverwaltungsgesetzes)

Zu Nummer 1

Für die Tätigkeit der Bediensteten des Bundesnachrichtendienstes ist bisweilen erforderlich, auch größere Summen von Barmitteln und gleichgestellten Zahlungsmitteln grenzüberschreitend zu transportieren. Dies betrifft Fälle, in denen die genannten Mittel aus dem Gebiet der Bundesrepublik Deutschland in Mitgliedstaaten der Europäischen Union ausgeführt bzw. aus Mitgliedstaaten der Europäischen Union in das Gebiet der Bundesrepublik Deutschland eingeführt werden sollen. Ebenso muss der Bundesnachrichtendienst auch Barmittel und gleichgestellte Zahlungsmittel von Deutschland aus dem Gebiet der Europäischen Union ausführen bzw. über Deutschland in das Gebiet der Europäischen Union einführen können.

Dabei gelten für die Bediensteten des Bundesnachrichtendienstes die Vorgaben der Verordnung (EU) 2018/1672 über die Überwachung von Barmitteln, die in die Union oder aus der Union verbracht werden, und zur Aufhebung der Verordnung (EG) Nr. 1889/2005 nicht. Diese Verordnung regelt (in unmittelbarer Anwendbarkeit) die Ein- und Ausfuhr von Barmitteln im Gesamtwert von 10 000 Euro in das bzw. aus dem Gebiet der Europäischen Union. Für den Bundesnachrichtendienst findet die Verordnungen indes aufgrund von Artikel 4 Absatz 2 Satz 3 EUV (vgl. BVerfG, Urteil vom 8. Oktober 2024, 1 BvR 1743/16 u.a., Rn. 77f.) keine Anwendung: Die Barmittelverbringung dient, wenn sie durch Bedienstete des Bundesnachrichtendienstes erfolgt, konkret operativ-sicherheitlichen Zwecken und im Allgemeinen der nationalen Sicherheit.

Die konkreten Fallkonstellationen, in denen Bedienstete des Bundesnachrichtendienstes im Rahmen ihrer dienstlichen Tätigkeit gehalten sind, derart große Mengen an Barmitteln zu transportieren, können hier nur angerissen werden: in Betracht kommen etwa die Ankäufe von Wehrmaterial ausländischer Staaten oder die Verbringung von Barmitteln zur Vergütung von hochwertigen nachrichtendienstlichen Verbindungen.

Für die praktische Handhabung ist erforderlich, dass den Zollbediensteten gegenüber angezeigt wird, dass es sich bei den Personen, um Bedienstete des Bundesnachrichtendienstes handelt. Hierbei kann eine Anzeige im Vorfeld der Reise – gegebenenfalls unter Angabe der Tarnidentität des Reisenden – erfolgen oder, wenn dies aus operativ-sicherheitlichen Aspekten möglich ist, eine Anzeige unmittelbar gegenüber den kontrollierenden Zollbediensteten sachdienlich sein. Die Implementierung weiterer Möglichkeiten, die Zugehörigkeit zum Bundesnachrichtendienst im Zweifelsfall belegen zu können, obliegt dem Bundesnachrichtendienst und bleibt der Praxis zugleich unbenommen.

Zu Nummer 2

Es handelt sich um eine Folgeänderung.

Zu Artikel 17 (Änderung des Geldwäschegesetzes)

Zu Nummer 1

Die Nachrichtendienste sind bei der Beschaffung von Informationen darauf angewiesen, menschliche Quellen zu entlohnen. Während dies in der Vergangenheit in erster Linie mit Bargeld erfolgte, birgt die Nutzung von Kryptowährungen erhebliche Vorteile bei der Durchführung nachrichtendienstlicher Operationen im In- und Ausland. Der Schutz der Identität der handelnden Personen kann aufgrund der im Rahmen der Nutzung von Kryptowerten gewährleisteten Anonymität oder Pseudonymität besser gewährleistet werden. Zudem wird durch einen digitalen Transfer das Risiko der Operateure und Kuriere der Nachrichtendienste beim Transfer von Zahlungen erheblich reduziert. Zugleich erweist sich die Zahlung von Kryptowerten als deutlich schneller gegenüber grenzüberschreitenden Überweisungen oder dem Bargeldtransfer. Grundsätzlich besteht nach § 8 Absatz 1 Satz 1 Nummer 1 eine

Verpflichtung des Finanzdienstleisters zur Aufzeichnung und Aufbewahrung der Daten über die Vertragspartner. Um den Erwerb von Kryptowerten zu vereinfachen, ist es erforderlich, eine Ausnahme für Konstellationen zu schaffen, in denen überwiegende Sicherheitsinteressen der Bundesrepublik Deutschland der Speicherung der Identität des Vertragspartners entgegenstehen. In diesen Fällen soll der verpflichtete Finanzdienstleister auch einen anderen Namen als den des Vertragspartners speichern dürfen. Da die Nachrichtendienste auf die Kooperationsbereitschaft des jeweiligen Finanzdienstleisters angewiesen sind, wird durch die Ausnahme von der Aufzeichnungs- und Aufbewahrungspflicht Rechtssicherheit für den verpflichteten Finanzdienstleister gewährleistet.

Zu Nummer 2

Es handelt sich um eine Folgeänderung.

Zu Artikel 18 (Änderung des Zehnten Buches Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz)

Die Änderung trägt einem erweiterten Informationsbedarf der berechtigten Stellen Rechnung, der sich insbesondere auf den Leistungsbezug bezieht. Dazu wird der Informationsumfang im Allgemeinen in Satz 1 sowie im neuen Satz 3 für bestimmte Fälle von erheblicher Bedeutung angepasst.

Es bleibt dabei, dass in Fällen der Gefahrenabwehr ein Auskunftsersuchen nur bezüglich der Daten, die übereinstimmend auch in § 68 Absatz 1 Satz 1 SGB X gelistet sind (derzeitiger Name, Vorname, Geburtsdatum, Geburtsort, derzeitige Anschrift der betroffenen Person sowie Namen und Anschriften ihrer derzeitigen Arbeitgeber), auch auf § 68 SGB X gestützt werden kann, sofern dessen tatbestandliche Voraussetzungen erfüllt sind.

Wie bisher gilt für die ersuchenden Stellen § 78 SGB X.

Zu Nummer 1

Zu Buchstabe a

In Absatz 1 Satz 2 wird der übermittlungsfähige Datenkranz erweitert auf derzeitige und frühere berufliche Tätigkeiten, auf schulische, akademische und berufliche Abschlüsse, Lichtbilder sowie die Angabe, welche Geldleistungen eine Person erhält. Wie sich bisher von Sinn und Zweck abgedeckte zulässige Zusatzinformationen der Zeiträume auf die sich frühere Anschriften des Betroffenen und früherer Arbeitgeber beziehen, gilt dies auch in Bezug auf die beruflichen Tätigkeiten. Das heißt, die Übermittlung von Beschäftigungszeiträumen ist ebenfalls zulässig.

Sowohl die beruflichen Tätigkeiten als auch der (Aus-)Bildungsweg können bei der Gefährdungsbewertung von Personen eine entscheidende Rolle spielen. Zudem können die im Rahmen des Bildungswegs erlangten Fertigkeiten bei der Bewertung des von einer Person ausgehenden Bedrohungspotentials von Relevanz sein. Die Abschlüsse zeigen das jeweilige Fähigkeitenpotenzial einer Person.

Durch die Aufnahme von Lichtbildern der Gesundheitskarte nach § 291a SGB V in Satz 2 wird eine Regelungslücke geschlossen, die bei nicht-deutschen EU-Bürgern besteht, da hier die Ermittlung eines Lichtbildes regelmäßig nicht möglich ist. Denn nicht-deutsche EU-Bürger müssen bei ihrer Anmeldung im Einwohnermeldeamt kein Lichtbild einreichen, sie benötigen als Nichtdeutsche ebenfalls keinen deutschen Reisepass oder Personalausweis. Auch bei der Ausländerbehörde müssen sie – anders als Nicht-EU-Ausländer – kein Lichtbild einreichen, da aufgrund der EU-Freizügigkeit keine Meldepflicht bei dieser Behörde besteht.

Die Übermittlung, ob eine Person Geldleistungen bezieht, ohne weitere Angaben zu Zahlungen oder Beträgen i.S.d. in Absatz 1 Satz 3, ermöglicht gestufte und zunächst niedrigschwellige Ermittlungen. Die Information, welche Sozialleistungen aktuell bezogen werden, hilft bei der Einschätzung des Bedrohungspotentials einer Person. Sie kann einen ersten Aufschluss darüber geben, welche Finanzmittel einer Person wahrscheinlich zur Verfügung stehen und in welchem sozialen Umfeld sie sich voraussichtlich bewegt. Sie kann zudem ein erster Anhaltspunkt sein, ob – ggf. an anderer Stelle – Abhängigkeiten bestehen können. Aus der Information über den Leistungsbezug können auch relevante Rückschlüsse für die Möglichkeit der Anwerbung von Personen gezogen werden.

Zu Buchstabe b

Durch Absatz 1 Satz 3 wird der übermittlungsfähige Datenkranz für Fälle von erheblicher Bedeutung erweitert. Für diese Fälle ermöglicht Absatz 1 Satz 3 die Übermittlung von Angaben zur Staatsangehörigkeit und Angaben über Geldleistungen, die an betroffene Personen erbracht worden oder zu erbringen sind.

Zu Nummer 2

Der Absatz orientiert sich an der Verantwortungsregelung des § 69 Absatz 3 Satz 2 und 3, die gleichermaßen in § 73 sachgerecht ist. Die Zulässigkeit nationaler Regelungen zur Konkretisierung des Verantwortlichen soweit es um Datenverarbeitung auf Grundlage mitgliedstaatlicher Regelungen geht, ergibt sich aus Artikel 4 Nummer 7 der Verordnung (EU) 2016/679.

Das Übermittlungsersuchen ist grundsätzlich so zu stellen, dass die ersuchte Stelle die Prüfung nach Absatz 3 Satz 2 durchführen kann. Die ersuchende Stelle hat deswegen bei ihrem Ersuchen insbesondere anzugeben, für welche ihrer gesetzlichen Aufgaben die Übermittlung der Daten erforderlich ist. Für die ersuchte Stelle muss dadurch insbesondere deutlich werden, wenn es sich um eine Aufgabe nach Absatz 1 Satz 3 handelt, bei der die Übermittlung von weiteren Daten zulässig ist. Die ersuchte Stelle prüft nicht, ob die Voraussetzungen der gesetzlich geregelten Aufgaben der ersuchenden Stelle im Einzelnen vorliegen. Hintergrund ist, dass aufgrund der spezifischen Aufgabenstellung der Sicherheitsbehörden zu beachten ist, dass diese nicht gezwungen sein können, sicherheitsrelevante Informationen zur Einschätzung der Erforderlichkeit an den ersuchten Leistungsträger übermitteln zu müssen.

Zu Artikel 20 (Außerkrafttreten)

Der Artikel regelt das Außerkrafttreten der von diesem Gesetz abgelösten Gesetze. Dies sind das bisherige Bundesverfassungsschutzgesetz und BND-Gesetz, die in Artikel 1 und 2 neu verkündet werden, und das Artikel 10-Gesetz, das in den Fachgesetzen (Artikel 1 und 2) und dem neuen Gesetz über den Unabhängigen Kontrollrat (Artikel 3) aufgeht. Absatz 2 trifft dabei für die Länder zu den bisherigen G 10-Sachen eine Übergangsregelung.

Zu Artikel 21 (Inkrafttreten)

Der Artikel regelt das Inkrafttreten.

Zu Anlage 1 (zu § 48 Absatz 2 Nummer 2 BVerfSchG)

Zu Nummer 1 (Aufstacheln zum Verbrechen der Aggression - § 80a StGB)

Die Vorschrift schützt den „Weltfrieden“. Ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft liegt vor, da die Rechtsgemeinschaft ein sehr hohes

Interesse am friedlichen Zusammenleben der Bundesrepublik Deutschland mit anderen Völkern hat.

Die besondere Schwere der Straftat ergibt sich zum einen aus der Tathandlung und zum anderen aus der Zielrichtung der Tathandlung. Tathandlung ist das Aufstacheln, also das Aufhetzen, durch das in bestimmter, zielgerichteter Weise zu einer emotional gesteigerten Haltung angereizt wird, also eine auf die Gefühle der Adressaten abzielende Propaganda. Zielrichtung der Tathandlung ist zum Verbrechen der Aggression aufzustacheln, d.h. zur Vorbereitung eines Angriffskrieges gegen ein anderes Land.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Schließlich kommt eine Radikalisierung größerer Bevölkerungsteile in Betracht, da der Täter darauf abzielt einen größeren Personenkreis zu erreichen (Öffentlich, Versammlung, Verbreiten). Dadurch wird ein gesellschaftliches Klima befeuert, dass die Vorbereitung eines Angriffkrieges begünstigt und damit eine erhebliche Gefahr für das o.g. Schutzgut „Weltfrieden“ darstellt.

Zu Nummer 2 (Vorbereitung eines hochverräterischen Unternehmens - § 83 Absatz 2 StGB)

Die Vorschrift schützt die dem Föderalismusprinzip zu Grunde liegende territoriale und konstitutionelle Eigenständigkeit der Länder. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist die Vorbereitung eines bestimmten hochverräterischen Unternehmens gegen ein Land, d.h. die Vorbereitung eines Umsturzes unter Anwendung von Gewalt oder einer entsprechenden Drohung, siehe § 82 StGB. Folglich liegt ein besonderes Gewaltpotential vor. „Bestimmt“ heißt, dass das Unternehmen nach der Vorstellung des Täters in seinen wesentlichen Grundzügen (Angriffsziel und Angriffsgegenstand, sowie grobe Umrisse von Zeit, Ort und Art und Weise der Durchführung) bereits feststehen muss. Vorbereitung sind alle Handlungen, die das hochverräterische Unternehmen mittelbar oder unmittelbar fördern und geeignet sind die verfassungsmäßige Ordnung eines Landes zu beeinträchtigen oder zu ändern.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge, da der Hochverrat gegen ein Land Ziel der vorbereitenden Handlungen ist. Beim Hochverrat handelt es sich um das schwerste Verbrechen gegen die Existenz eines Staates. Das o.g. Schutzgut wird dadurch gefährdet.

Zu Nummer 3 (Fortführung einer für verfassungswidrig erklärten Partei - § 84 Absatz 1 Satz 1, Absatz 2 und 3 StGB)

Die Vorschrift schützt die freiheitlich demokratische Grundordnung. Ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft liegt damit vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Als Tathandlung wird das Handeln als Rädelsführer oder Hintermann einer vom BVerfG für verfassungswidrig erklärten Partei (Nr. 1) oder einer Partei, von der das BVerfG festgestellt hat, dass sie Ersatzorganisation ist (Nr. 2) erfasst. Rädelsführer ist, wer in einer Organisation dadurch eine führende Rolle spielt, dass er sich in besonders maßgebender Weise für sie betätigt. Hintermann ist, wer geistig oder wirtschaftlich Wesentliches für die Partei leistet, dabei jedoch im Hintergrund bleibt. In beiden Fällen handeln Personen mit wesentlichem Einfluss auf die Organisation.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Diese ist die Aufrechterhaltung des organisatorischen Zusammenhalts einer verbotenen Partei bzw. Ersatzorganisation, sodass deren verfassungsfeindliche Ziele im Geltungsbereich des

Grundgesetzes organisiert weiterverfolgt werden können. Gerade in der Aufrechterhaltung eines Zusammenschlusses mehrerer Personen wohnt eine Eigendynamik inne, die zu einer Steigerung der Gefährlichkeit für wichtige Rechtsgüter der Gemeinschaft führt. Diese für größere Personenzusammenschlüsse typische Eigendynamik hat ihre besondere Gefährlichkeit darin, dass sie geeignet ist, dem einzelnen Beteiligten die Begehung von Straftaten zu erleichtern und bei ihm das Gefühl persönlicher Verantwortung zurückzudrängen. Damit geht ein erhebliches Gefährdungspotential für das o.g. Schutzgut „freiheitlich demokratische Grundordnung“ einher.

Zu Nummer 4 (Verstoß gegen ein Vereinigungsverbot - § 85 Absatz 1 StGB)

Die Vorschrift schützt die freiheitlich demokratische Grundordnung und den Gedanken der Völkerverständigung. Besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft liegen damit vor.

Dass es sich bei § 85 Absatz 1 StGB um eine besonders schwere Straftat handelt, ergibt sich bereits aus der besonderen Begehungsform, die im Tatbestand objektiviert ist. Als Tathandlung erfasst wird das Handeln als Rädelsführer oder Hintermann einer Partei oder Vereinigung von der unanfechtbar festgestellt ist, dass sie Ersatzorganisation einer verbotenen Partei ist (Nr. 1) oder einer Vereinigung, die unanfechtbar verboten ist, oder von der unanfechtbar festgestellt ist, dass sie Ersatzorganisation einer solchen verbotenen Vereinigung ist (Nr. 2). Rädelsführer ist, wer in einer Organisation dadurch eine führende Rolle spielt, dass er sich in besonders maßgebender Weise für sie betätigt. Hintermann ist, wer geistig oder wirtschaftlich Wesentliches für die Partei leistet, dabei jedoch im Hintergrund bleibt. In beiden Fällen handeln Personen mit wesentlichem Einfluss auf die Organisation.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Diese ist die Aufrechterhaltung des organisatorischen Zusammenhalts der o.g. Partei oder Vereinigung, sodass sie weiter gegen Strafgesetze, die verfassungsmäßige Ordnung bzw. den Gedanken der Völkerverständigung verstoßen. Gerade in der Aufrechterhaltung eines Zusammenschlusses mehrerer Personen wohnt eine Eigendynamik inne, die zu einer Steigerung der Gefährlichkeit für wichtige Rechtsgüter der Gemeinschaft führt. Diese für größere Personenzusammenschlüsse typische Eigendynamik hat ihre besondere Gefährlichkeit darin, dass sie geeignet ist, dem einzelnen Beteiligten die Begehung von Straftaten zu erleichtern und bei ihm das Gefühl persönlicher Verantwortung zurückzudrängen. Darüber hinaus werden durch die Aufrechterhaltung möglicherweise auch etwaige Radikalisierungen vorangetrieben, die mitunter in abgeschlossenen Räumen stattfinden.

Zu Nummer 5 (Agententätigkeit zu Sabotagezwecken - § 87 StGB)

Die Vorschrift schützt den Bestand und die Sicherheit der Bundesrepublik Deutschland. Damit liegt ein besonderes gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich bereits aus der besonderen Begehungsform, die im Tatbestand objektiviert ist, nämlich dem Tätigwerden auf einen Auftrag einer „Regierung, Vereinigung oder Einrichtung außerhalb des räumlichen Geltungsbereichs dieses Gesetzes“ hin. Dieses Tatbestandsmerkmal beschreibt typischerweise besonderes Gefährdungspotenzial, sei es durch die besonderen Gefährdungsfähigkeiten eines Staates in der Tatbegehung oder durch die Einbettung in ein über das einzelne Delikt hinausweisendes Gesamtgeschehen.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge sind Vorbereitungshandlungen für konkret und abschließend beschriebene Sabotagehandlungen (s. Absatz 2, u.a. schwere Brandstiftungsdelikte und Herbeiführung einer Sprengstoffexplosion) mit dem Ziel des Zerstörens, Beschädigens, Beseitigens etc. eines für die Landesverteidigung, für den Schutz der Zivilbevölkerung gegen Kriegsgefahren oder für die Gesamtwirtschaft wichtigen Unternehmens bzw. Betriebes.

Zu Nummer 6 (Ausübung fremder Einflussnahme und darauf gerichtete Agententätigkeit - § 87a StGB)

Die Vorschrift schützt die Souveränität und Sicherheit der Bundesrepublik Deutschland. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Die besonders schwere Straftat ergibt sich bereits aus der besonderen Begehungsform, die im Tatbestand objektiviert ist, da die Tatbegehung hier für eine fremde Macht erfolgt. Dieser Tatbestand beschreibt typischerweise besonderes Gefährdungspotenzial, sei es durch die besonderen Gefährdungsfähigkeiten eines Staates in der Tatbegehung oder durch die Einbettung in ein über das einzelne Delikt hinausweisendes Gesamtgeschehen (bei staatlichem Vorgehen ist generell von planvollem Handeln und systematischem Vorgehen auszugehen).

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist neben der Begehung der eigentlichen Straftat die hinzutretende Verletzung der Souveränität der Bundesrepublik Deutschland, da die Straftat auf Weisung einer fremden Macht auf deutschem Boden erfolgt. Die Souveränität ist auch dann verletzt, wenn es sich um weniger schwere Straftaten handelt, weil sich auch diese destabilisierend auf die freiheitlich-demokratische Grundordnung auswirken können, was von der ausländischen staatlichen Stelle regelmäßig auch bezweckt sein wird. Durch das Erteilen eines Auftrags zur Begehung von Straftaten auf deutschem Boden oder Handeln im Auftrag einer fremden Macht ergibt sich daher ein besonderes Bedrohungspotential für die Sicherheit der Bundesrepublik Deutschland.

Zu Nummer 7 (Verfassungsfeindliche Sabotage - § 88 StGB)

Die Vorschrift schützt den Bestand und die Sicherheit der Bundesrepublik Deutschland sowie die verfassungsmäßige Ordnung. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Der Tatbestand beschreibt die erfolgreiche (Abs. 1) bzw. versuchte (Abs. 2) Durchführung von Sabotagehandlungen an Anlagen von wesentlicher Bedeutung. Geschützt werden Unternehmen oder Anlagen, die der öffentlichen Versorgung mit Postdienstleistungen oder dem öffentlichen Verkehr dienen, Telekommunikationsanlagen, bestimmte Versorgungseinrichtungen, sowie der öffentlichen Sicherheit und Ordnung dienende Einrichtungen. Da es sich um Anlagen handelt, die öffentlichen Zwecken dienen, geht dies mit einer Betroffenheit großer Teile der Bevölkerung einher (Bsp.: Brandanschläge auf kritische Infrastruktur und hybride Bedrohungen durch staatliche Akteure (Stichwort: Unterseekabel)).

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist, dass die geschützte Einrichtung ganz oder teilweise stillgelegt oder ihren bestimmungsmäßigen Zwecken entzogen wird.

Zu Nummer 8 (Verunglimpfung des Bundespräsidenten - § 90 Absatz 1 und 3 StGB)

Die Vorschrift dient dem Schutz der Person und des Amtes des Bundespräsidenten iS seiner Funktionen während der jeweiligen Amtszeit; dahinter steht der beabsichtigte Schutz des Staates und seiner verfassungsmäßigen Ordnung. Hierbei handelt es sich um besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist eine Verunglimpfung, d. h. erheblichere Ehrenkränkung (Abs. 1, vgl. Fischer/Anstötz, StGB, 72. Aufl. 2025, § 90 Rn. 2), bzw. eine Verleumdung gemäß § 187 StGB (Absatz 3). Der erhöhte Strafrahmen des Absatzes 3 kommt auch dann zur Anwendung, wenn der Täter sich durch die Tat nach Absatz 1 absichtlich für Bestrebungen gegen den Bestand

der Bundesrepublik Deutschland oder gegen Verfassungsgrundsätze einsetzt. Vorausgesetzt ist jeweils, dass die Tat öffentlich, in einer Versammlung oder durch Verbreiten eines Inhalts (§ 11 Absatz 3 StGB) begangen wird. Ein Anwendungsfall sind etwa Maßnahmen Dritter im Bereich der Desinformation (Bsp.: Fake-News).

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die bewirkte Verunglimpfung. Darüber hinaus ist aufgrund des Öffentlichkeitsbezugs eine Förderung der gesellschaftlichen Radikalisierung möglich. Die Tatfolgen beeinträchtigen die o.g. Schutzgüter.

Zu Nummer 9 (Verunglimpfung des Staates und seiner Symbole für extremistische Bestrebungen - § 90a Absatz 3 StGB)

Die Vorschrift schützt den Bestand und die verfassungsmäßige Ordnung der Bundesrepublik Deutschland und ihrer Länder in ihrer konkreten Verfassungsordnung (vgl. Fischer/Anstötz, StGB, 72. Aufl. 2025, § 90a Rn. 2). Hierbei handelt es sich um besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist zum einen „beschimpfen“ oder „böswillig verächtlich machen“ des Bundes oder der Länder bzw. ein Verunglimpfen der wichtigsten Staatssymbole (Abs. 1). Zum anderen u.a. das Zerstören, Beschädigen und Unbrauchbarmachen von Hoheitszeichen (Abs. 2). Beides mit der Absicht sich für Bestrebungen gegen den Bestand der Bundesrepublik Deutschland oder gegen Verfassungsgrundsätze einzusetzen und jeweils verbunden mit einem gewissen Öffentlichkeitsbezug, konkret öffentlich, in einer Versammlung oder durch Verbreiten eines Inhalts (§ 11 Absatz 3 StGB). Dies kann insbesondere Teil hybrider Maßnahmen Dritter im Bereich der Desinformation sein (Bsp.: Fake-News).

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die bewirkte Verunglimpfung. Aufgrund des Öffentlichkeitsbezugs ist darüber hinaus die Förderung der gesellschaftlichen Radikalisierung eine mögliche Tatfolge, Damit beeinträchtigen die Tatfolgen die o.g. Schutzgüter.

Zu Nummer 10 (Verfassungsfeindliche Verunglimpfung von Verfassungsorganen - § 90b Absatz 1 StGB)

Die Vorschrift schützt die bezeichneten Verfassungsorgane. Hierbei handelt es sich um besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist die das Ansehen des Staates gefährdende Verunglimpfung von Verfassungsorganen (Gesetzgebungsorgan, Regierung, Verfassungsgerichte bzw. deren Mitglieder) in der Öffentlichkeit, in einer Versammlung oder durch Verbreiten eines Inhalts (§ 11 Absatz 3 StGB). Der Täter muss sich absichtlich für verfassungswidrige Bestrebungen einsetzen. Dies kann insbesondere Teil hybrider Maßnahmen Dritter im Bereich der Desinformation sein (Bsp.: Fake-News).

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die bewirkte Verunglimpfung, d.h. die Herabwürdigung. Aufgrund des Öffentlichkeitsbezugs ist darüber hinaus die Förderung der gesellschaftlichen Radikalisierung eine mögliche Tatfolge, Damit beeinträchtigen die Tatfolgen die o.g. Schutzgüter.

Zu Nummer 11 (Offenbaren von Staatsgeheimnissen - § 95 Absatz 1 StGB)

Die Vorschrift schützt die äußere Sicherheit der Bundesrepublik Deutschland. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist einem Unbefugten oder der Öffentlichkeit die Möglichkeit zu verschaffen, von einem Staatsgeheimnis im Sinne des § 93 Absatz 1 StGB Kenntnis zu nehmen.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die konkrete Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland aufgrund der möglichen Kenntnisnahme von einem Staatsgeheimnis durch Unbefugte oder der Öffentlichkeit und damit auch durch eine fremde Macht. Insbesondere durch die mögliche Folgeverwendung des Staatsgeheimnisses drohen gemeinwohlschädliche Auswirkungen zulasten des o.g. Schutzgutes (vgl. § 4 Absatz 2 SÜG).

Zu Nummer 12 (Landesverräterische Ausspähung; Auskundschaften von Staatsgeheimnissen - § 96 Absatz 2 Satz 1 StGB)

Die Vorschrift schützt die äußere Sicherheit der Bundesrepublik Deutschland. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist das Sich-Verschaffen von Staatsgeheimnissen, das von einer amtlichen Stelle oder auf deren Veranlassung geheim gehalten wird, um einem Unbefugten oder der Öffentlichkeit die Möglichkeit zu verschaffen, von diesen Kenntnis zu nehmen. Staatsgeheimnisse sind Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht geheim gehalten werden müssen, um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden (§ 93 Absatz 1 StGB).

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die Vorbereitungshandlung zum Offenbaren von Staatsgeheimnissen, womit eine konkrete Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland einhergeht. Insbesondere durch die mögliche Folgeverwendung des Staatsgeheimnisses (z.B. durch fremde Mächte) drohen gemeinwohlschädliche Auswirkungen zulasten des o.g. Schutzgutes (vgl. § 4 Absatz 2 SÜG).

Zu Nummer 13 (Preisgabe von Staatsgeheimnissen - § 97 Absatz 1 StGB)

Die Vorschrift schützt die äußere Sicherheit der Bundesrepublik Deutschland. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist die Preisgabe von Staatsgeheimnissen im Sinne des § 93 Absatz 1 StGB.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die durch die Preisgabe des Staatsgeheimnisses (mindestens) fahrlässige Herbeiführung eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland. Insbesondere durch die mögliche Folgeverwendung des Staatsgeheimnisses drohen gemeinwohlschädliche Auswirkungen zulasten des o.g. Schutzgutes (vgl. § 4 Absatz 2 SÜG).

Zu Nummer 14 (Landesverräterische Agententätigkeit (§ 98 Absatz 1 Satz 1 StGB))

Die Vorschrift schützt die äußere Sicherheit der Bundesrepublik Deutschland. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand, da die Tatbegehung in Nr. 1 für eine fremde Macht erfolgt. Dieser Tatbestand beschreibt typischerweise besonderes Gefährdungspotenzial, sei es durch die besonderen Gefährdungsfähigkeiten eines Staates in der Tatbegehung oder durch die Einbettung in ein über das einzelne Delikt hinausweisendes Gesamtgeschehen (bei staatlichem Vorgehen ist generell von planvollem Handeln und systematischem Vorgehen auszugehen). Bzgl. Nr. 2 bezieht sich die

Tathandlung auf ein zweifelsfreies und ernst gemeintes Bereiterklären für eine fremde Macht Staatsgeheimnisse zu Erlangen bzw. diese mitzuteilen.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die Ausübung der Tätigkeit bzw. das Bereiterklären, verbunden mit der abstrakten Gefahr, die regelmäßig durch die Involvierung einer „fremden Macht“ im Zusammenhang mit Staatsgeheimnissen besteht. Das Schutzgut der äußeren Sicherheit ist damit gefährdet.

Zu Nummer 15 (Landesverräterische Fälschung - § 100a Absatz 1 und 2 StGB)

Die Vorschrift schützt die äußere Sicherheit der Bundesrepublik Deutschland. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung sind gezielte Falschmeldungen, die den Staat diffamieren und geeignet sind, das Vertrauen anderer Länder in die außenpolitische Verlässlichkeit der Bundesrepublik Deutschland zu erschüttern.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland oder ihre Beziehungen zu einer fremden Macht. Im Informationszeitalter werden Nachrichten ohne Verzug über die ganze Welt verbreitet, d.h. es ist so gut wie unmöglich, sie wieder „einzufangen“ und ihre Unrichtigkeit klarzustellen. Es kann dadurch ein unabsehbarer außenpolitischer Schaden entstehen.

Zu Nummer 16 (Angriff gegen Organe und Vertreter ausländischer Staaten - § 102 Absatz 1 erste Alternative StGB)

Die Vorschrift schützt neben Leib und Leben, konkret von ausländischen Staatsoberhäuptern und Regierungsvertretern, welche sich in amtlicher Eigenschaft im Inland aufhalten, auch das Interesse der Bundesrepublik Deutschland an guten und ungestörten Beziehungen zu anderen Staaten. Hierbei handelt es sich um besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist ein Angriff auf Leib oder Leben, der sich gezielt auch auf den auslandsstaatlichen Status der betroffenen Personen beziehen muss.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist neben der möglichen Tötung oder Körperverletzung auch eine Belastung funktionierender bzw. diplomatischer Beziehungen zwischen dem ausländischen Staat und der Bundesrepublik Deutschland.

Zu Nummer 17 (Nötigung des Bundespräsidenten und von Mitgliedern eines Verfassungsorgans - § 106 Absatz 1 StGB)

Die Vorschrift schützt den Bundespräsidenten und die Funktionsfähigkeit und -freiheit der Mitglieder der genannten Verfassungsorgane. Hierbei handelt es sich um besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist die rechtswidrige Nötigung von Verfassungsorganen mit Gewalt oder durch Drohung mit einem empfindlichen Übel.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die Manipulation des Verfassungsorgans dahingehend, seine aus der Organstellung folgenden Befugnisse in einem bestimmten Sinne auszuüben bzw. davon Abstand zu nehmen. Das o.g. Schutzgut wird damit verletzt.

Zu Nummer 18 (Wahlbehinderung - § 107 Absatz 1 StGB)

Das Rechtsgut „Schutz der Wahlen“, konkret des ordnungsgemäßen Gesamtablaufs sowie die Richtigkeit des Wahlergebnisses und damit die Volkssouveränität als Teil der freiheitlichen, demokratischen Grundordnung, ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist der Einsatz von Gewalt oder die Drohung mit Gewalt, um eine Wahl oder die Feststellung ihres Ergebnisses zu verhindern oder zu stören, d.h. nicht unerheblich zu erschweren bzw. zu verzögern.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die Verhinderung oder Störung einer Wahl oder der Feststellung ihres Ergebnisses und damit die Wahlbehinderung einer Vielzahl von Personen. Dies führt zu einer erheblichen Beeinträchtigung der Kernfunktionen der Demokratie und bedroht das Vertrauen der Bevölkerung in deren Funktionsfähigkeit und damit das o.g. Rechtsgut.

Zu Nummer 19 (Wahlfälschung - § 107a Absatz 2 StGB)

Die Vorschrift schützt das unverfälschte Wahlergebnis und somit mittelbar die demokratische Entscheidungsfindung und damit die Volkssouveränität als Teil der freiheitlichen, demokratischen Grundordnung. Ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft liegt damit vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist die unrichtige Verkündung des Ergebnisses einer Wahl.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist eine unrichtige Wahlverkündung. Dies führt zu einer erheblichen Beeinträchtigung der Kernfunktionen der Demokratie und bedroht das Vertrauen der Bevölkerung in deren Funktionsfähigkeit.

Zu Nummer 20 (Wählernötigung - § 108 Absatz 1 StGB)

Die Vorschrift schützt die freie Stimmabgabe, d.h. die Entscheidung des einzelnen Wahlberechtigten über das Ob und das Wie seiner Stimmabgabe. Damit wird mittelbar der ordnungsgemäße Ablauf der Wahl und damit die Volkssouveränität als Teil der freiheitlichen, demokratischen Grundordnung geschützt. Ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft liegt somit vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist der Einsatz von Gewalt, Drohung mit einem empfindlichen Übel, Missbrauch eines beruflichen oder wirtschaftlichen Abhängigkeitsverhältnisses oder sonstiger wirtschaftlicher Druck, um einen Wahlberechtigten zu nötigen bzw. daran zu hindern zu wählen oder von seinem Wahlrecht in einem bestimmten Sinne Gebrauch zu machen.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Taterfolg ist, dass der Wahlberechtigte entgegen seinem Willen gezwungen wird, überhaupt oder in einem bestimmten Sinn zu wählen oder seine Stimmabgabe zu unterlassen, obwohl er zur Wahl bereit ist. Das o.g. Schutzgut wird dadurch massiv beeinträchtigt. Die Tathandlung führt folglich zu einer Beeinträchtigung der Kernfunktionen der Demokratie und bedroht das Vertrauen der Bevölkerung in deren Funktionsfähigkeit.

Zu Nummer 21 (Störpropaganda gegen die Bundeswehr - § 109d Absatz 1 StGB)

Die Vorschrift schützt die Funktionsfähigkeit der Bundeswehr und damit mittelbar die Landesverteidigung, die der Gewährleistung des Bestandes und der Sicherheit des Bundes

dient. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung sind unwahre oder gröblich entstellte Behauptungen tatsächlicher Art, deren Verbreitung geeignet ist, die Tätigkeit der Bundeswehr zu stören, wider besseres Wissen zum Zwecke der Verbreitung aufstellt oder solche Behauptungen in Kenntnis ihrer Unwahrheit verbreitet, um die Bundeswehr in der Erfüllung ihrer Aufgabe der Landesverteidigung zu behindern.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist eine potentielle Störung der Tätigkeit der Bundeswehr bzw. eine Behinderung in der Erfüllung ihrer Aufgabe der Landesverteidigung. Die damit verbundene Schwächung der äußeren Sicherheit stellt eine erhebliche Gefährdung des o.g. Schutzgutes dar.

Zu Nummer 22 (Sabotagehandlungen an Verteidigungsmitteln - § 109e Absatz 1 und 2 StGB)

Die Vorschrift schützt die Funktionsfähigkeit von Verteidigungsmitteln und dient damit mittelbar der Verteidigungsfähigkeit zur Gewährleistung des Bestandes und der Sicherheit des Bundes. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung sind Sabotagehandlungen, die die Funktionsfähigkeit von Wehrmitteln sowie Einrichtungen und Anlagen der Verteidigung der Bundesrepublik Deutschland sowie des Zivilschutzes gegen Kriegsgefahren betreffen.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die konkrete Gefährdung der Sicherheit der Bundesrepublik Deutschland, der Schlagkraft der Truppe oder Menschenleben und damit insbesondere eine Schwächung der äußeren Sicherheit, was eine erhebliche Gefährdung des o.g. Schutzgutes darstellt.

Zu Nummer 23 (Sicherheitsgefährdender Nachrichtendienst - § 109f Absatz 1 StGB)

Die Vorschrift schützt die Sicherheit der Bundesrepublik Deutschland und die Schlagkraft der Truppe. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Als Tathandlung wird vorausgesetzt, dass jemand für eine Dienststelle, eine Partei oder eine andere Vereinigung außerhalb des räumlichen Geltungsbereichs des Strafgesetzbuchs oder für eine verbotene Vereinigung oder für einen ihrer Mittelsmänner Nachrichten über Angelegenheiten der Landesverteidigung sammelt, diesbezüglich einen Nachrichtendienst betreibt oder für diese Tätigkeiten anwirbt bzw. sie unterstützt und dadurch Bestrebungen dient, die gegen die Sicherheit der Bundesrepublik Deutschland oder die Schlagkraft der Truppe gerichtet sind.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist, dass Bestrebungen gedient wird, die sich gegen die Sicherheit der Bundesrepublik Deutschland oder die Schlagkraft der Truppe richten.

Zu Nummer 24 (Sicherheitsgefährdendes Abbilden - § 109g Absatz 1 StGB)

Die Vorschrift schützt die Sicherheit der Bundesrepublik Deutschland und die Schlagkraft der Truppe. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist das Abbilden und Beschreiben militärischer Gegenstände bzw. das Gelangen lassen einer solchen Abbildung oder Beschreibung an andere, in dem Wissen, dass dadurch die Sicherheit der Bundesrepublik Deutschland oder die Schlagkraft der Truppe gefährdet wird.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die wissentliche Gefährdung der Sicherheit der Bundesrepublik Deutschland oder der Schlagkraft der Truppe.

Zu Nummer 25 (Anwerben für fremden Wehrdienst - § 109h Absatz 1 StGB)

Die Rechtsgüter „Schutz des Wehrpotentials“ und „Wahrung der politischen Neutralität“ dienen dem Bestand und der Sicherheit des Bundes sowie bestimmten auf das Verhältnis zum Ausland gerichteten Interessen der Bundesrepublik Deutschland. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist das Anwerben zum Wehrdienst und das Zuführen zu Werbern oder zum Wehrdienst und dessen Einrichtungen zugunsten einer ausländischen Macht.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Taterfolg ist eine erfolgte Verpflichtung bzw. die Zuführung des Opfers in den Einflussbereich einer ausländischen Macht bzw. von Werbern oder einer militärischen Einrichtung. Damit einher geht eine Entziehung des Opfers aus dem Einflussbereich der Bundesrepublik Deutschland, sodass die Opfer nicht mehr als „Wehrpotential“ bzw. personelle Ressource für die Bundesrepublik Deutschland zur Verfügung stehen, was eine Schwächung der Sicherheit der Bundesrepublik Deutschland zur Folge hat.

Zu Nummer 26 (Öffentliche Aufforderung zu Straftaten - § 111 Absatz 1 StGB, sofern die rechtswidrige Tat, zu der aufgefordert wird, eine besonders schwere Straftat im Sinne dieser Vorschrift ist)

Die Vorschrift schützt das Rechtsgut der jeweils angesonnenen Vorschrift und den inneren Gemeinschaftsfrieden. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Vorausgesetzt wird, dass öffentlich, in einer Versammlung oder durch Verbreiten eines Inhalts zu einer bestimmten besonders schweren Straftat aufgefordert wird, also jedenfalls dann, wenn diese eine Höchstfreiheitsstrafe von fünf Jahren aufweist.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist ein Angriff sowohl gegen die Rechtsgüter der Bezugstaten als auch gegen das überindividuelle Rechtsgut des inneren Gemeinschaftsfrieden, aufgrund der mit der öffentlichen Aufforderung verbundenen Gefahr des „aus dem Rudern Laufens“ eines durch den Auffordernden in Gang gesetzten Kausalverlaufs. Die o.g. Rechtsgüter sind dadurch unmittelbar betroffen.

Zu Nummer 27 (Betreiben krimineller Handelsplattformen im Internet - § 127 Absatz 1 StGB, sofern die rechtswidrige Tat im Sinne des § 127 Absatz 1 Satz 2 eine besonders schwere Straftat im Sinne dieser Vorschrift ist)

Die Vorschrift schützt die öffentliche Sicherheit und Ordnung und zugleich die Rechtsgüter der in Bezug genommen Straftaten (damit u.a. Leib und Leben). Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand, sofern jemand eine Handelsplattform im Internet betreibt, deren Zweck darauf gerichtet ist, die Begehung von besonders schweren Straftaten nach § 127 Absatz 1 Satz 2 Nummer 2 StGB zu ermöglichen oder zu fördern. Dies betrifft vor allem solche Plattformen, auf denen professionell illegale Güter und Dienstleistungen („Cybercrime-as-a-Service“) sowie der Austausch von kriminalitätsbezogenen Informationen angeboten werden.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist, dass durch die aktive Bereitstellung der virtuellen Infrastruktur einem unbegrenzten Adressatenkreis inkriminierte Angebote zugänglich gemacht werden und damit breitflächig, mitunter anonym, schwere Kriminalität gefördert wird, wie z.B. Menschenhandel im Internet, wodurch die Gemeinschaft geschädigt wird. Die o.g. Schutzgüter werden dadurch stark gefährdet.

Zu Nummer 28 (Bildung krimineller Vereinigungen - § 129 Absatz 1 Satz 1 in Verbindung mit Absatz 5 Satz 1 und 2 StGB)

Die Rechtsgüter „Öffentliche Sicherheit“, „Staatliche Ordnung“ und „Öffentlicher Frieden“ sind besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft, da die öffentliche Sicherheit und Ordnung fundamentale Basis für ein funktionierendes Zusammenleben und die Wahrnehmung von Grundrechten in einer Gemeinschaft bildet.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Ein besonders schwerer Fall liegt vor, wenn der Täter Rädelsführer oder Hintermann einer Vereinigung ist, deren Zweck oder Tätigkeit auf die Begehung von Straftaten gerichtet ist. Rädelsführer ist, wer in der Vereinigung dadurch eine führende Rolle spielt, dass er sich in besonders maßgebender Weise für sie betätigt. Hintermann ist, wer – im Unterschied zum Rädelsführer – zwar nicht Mitglied der Vereinigung ist, gleichwohl aber die Vereinigung als Außenstehender dadurch wesentlich fördert, dass er geistig oder wirtschaftlich maßgebenden Einfluss auf die Führung der Vereinigung hat. Rädelsführer und Hintermann haben somit maßgeblichen Einfluss auf die Vereinigung.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Diesbezüglich ist festzuhalten, dass bereits durch die bloße Existenz krimineller Vereinigungen auf Grund ihrer inneren Struktur, spezifischen Organisation und Zielsetzung das Sicherheitsgefühl der Allgemeinheit beeinträchtigt und unter dem Aspekt der öffentlichen Sicherheit und Ordnung als massive Bedrohung anzusehen ist (Bsp.: Organisierte Kriminalität oder politisch/ideologisch-extremistische Organisationen, insb. aus dem extremen linken und rechten Spektrum). Der kriminellen Vereinigung wohnt eine Eigendynamik inne, die zu einer Steigerung der Gefährlichkeit für wichtige Rechtsgüter der Gemeinschaft führt. Diese für größere Personenzusammenschlüsse typische Eigendynamik hat ihre besondere Gefährlichkeit darin, dass sie geeignet ist, dem einzelnen Beteiligten die Begehung von Straftaten zu erleichtern und bei ihm das Gefühl persönlicher Verantwortung zurückzudrängen. Tatfolge des Handelns als Rädelsführer bzw. Hintermann ist, dass durch deren Mitwirken die Vereinigung maßgeblich in ihrem kriminellen Tun unterstützt wird und somit entscheidend zu einer Steigerung der Gefährlichkeit für wichtige Rechtsgüter der Gemeinschaft beigetragen wird. Dadurch werden die o.g. Rechtsgüter stark gefährdet.

Zu Nummer 29 (Bildung terroristischer Vereinigungen - § 129a Absatz 3 und 5 Satz 1 zweite Alternative sowie Satz 2 StGB)

Die Vorschrift schützt die innere öffentliche Sicherheit, da sie auf den Schutz vor besonders gefährlichen Vereinigungen gerichtet ist und der Bildung und dem Fortbestand derartiger schwerkrimineller Gruppierungen entgegenwirken soll. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Absatz 3 setzt als Tathandlung das Gründen oder das Sichbeteiligen als Mitglied an einer

Vereinigung voraus, deren Tätigkeit bzw. Zweck auf die Androhung von Straftaten nach § 129a Absatz 1 und 2 StGB gerichtet ist. D.h. es wird eine künftige Straftat nach § 129a Absatz 1 und 2 StGB in Aussicht gestellt, auf deren Begehung die Vereinigung Einfluss hat oder zumindest zu haben vorgibt. Absatz 5 setzt als Tathandlung das Unterstützen bzw. das Werben um Mitglieder oder Unterstützer voraus. Die Unterstützungshandlung bezieht sich dabei auf terroristische Vereinigungen, die besonders schwere Strafen androhen. Das Werben bezieht sich hingegen auf terroristische Vereinigungen, deren Zwecke oder deren Tätigkeiten auf die tatsächliche Begehung von besonders schweren Straftaten gerichtet sind.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Diesbezüglich ist festzuhalten, dass bereits durch die bloße Existenz terroristischer Vereinigungen auf Grund ihrer inneren Struktur, spezifischen Organisation und insbesondere ihrer Zielsetzung das Sicherheitsgefühl der Allgemeinheit beeinträchtigt und unter dem Aspekt der inneren öffentlichen Sicherheit als massive Bedrohung anzusehen ist (Bsp.: Politisch/ideologisch-extremistische Organisationen, die die Abschaffung der freiheitlich-demokratischen Grundordnung der Bundesrepublik Deutschland sowie die Schaffung eines neuen deutschen Staatswesens zum Ziel haben). Der terroristischen Vereinigung wohnt eine Eigendynamik inne, die zu einer Steigerung der Gefährlichkeit für wichtige Rechtsgüter der Gemeinschaft führt. Diese für größere Personenzusammenschlüsse typische Eigendynamik hat ihre besondere Gefährlichkeit darin, dass sie geeignet ist, dem einzelnen Beteiligten die Begehung von Straftaten zu erleichtern und bei ihm das Gefühl persönlicher Verantwortung zurückzudrängen. Durch die o.g. Tathandlungen wird die Gefährlichkeit der Vereinigung weiter gefestigt. Das o.g. Rechtsgut wird dadurch stark gefährdet.

Zu Nummer 30 (Sexueller Missbrauch von Schutzbefohlenen - § 174 Absatz 1 und 2 StGB)

Das Rechtsgut „Sexuelle Selbstbestimmung von Schutzbefohlenen“ ist ein besonders gewichtiges Rechtsguter mit hoher Bedeutung für die Rechtsgemeinschaft. Die besondere Gewichtigkeit ergibt sich daraus, dass sich die Schutzbefohlenen in einem besonderen Vertrauensverhältnis befinden. Dieses schützenswerte Verhältnis ergibt sich z.B. aufgrund staatlicher Anordnung (z.B. Schulpflicht, staatliche Betreuungsverhältnis), aufgrund von Arbeitsverhältnissen oder aufgrund der familiären Stellung. Für die Rechtsgemeinschaft ist es von hoher Bedeutung, dass sich Schutzbefohlene, die sich, u.U. auch zwangsweise, in einem solchen Rechtsverhältnis befinden, sich dabei auf den Schutz der Rechtsordnung verlassen können. Anderenfalls führt es zu gesellschaftlichem Misstrauen gegenüber staatlicher Anordnung.

Die in der Strafnorm objektivierte besondere Begehungsform ergibt sich daraus, dass eine Autoritätsperson, die zum Vertrauen verpflichtet ist, gerade dieses Vertrauen missbraucht.

Die besonderen Tatfolgen ergeben sich aus der entwicklungspsychologisch nachhaltigen Schädigung des Schutzbefohlenen, der ggf. erhebliche Schwierigkeiten hat sich wieder in die Gesellschaft zu integrieren, was wiederum nicht im Sinne der Rechtsgemeinschaft ist.

Zu Nummer 31 (Sexueller Missbrauch von Gefangenen, behördlich Verwahrten oder Kranken und Hilfsbedürftigen in Einrichtungen - § 174a Absatz 1 und Absatz 2 StGB)

Die Rechtsgüter „Sexuelle Selbstbestimmung von Gefangenen, behördlich Verwahrten oder Kranken und Hilfsbedürftigen in Einrichtungen sowie die Integrität dieser Institutionen“ sind besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft. Die besondere Gewichtigkeit ergibt sich daraus, dass die Rechtsgemeinschaft ein hohes Interesse an der Integrität der Institutionen, sowie ein hohes Interesse an dem Schutz des Zwecks der Verwahrung hat (z.B. Strafvollzug), als auch ein Vertrauen in die Objektivität der für Gefangene (u.s.w.) verantwortlichen Personen besteht. Ebenso besteht dieses hohe Interesse in dem Schutz der sexuellen Selbstbestimmung der in Absatz 1 und Absatz 2

genannten Personen. Dies gilt umso mehr, als bei Absatz 1 eine staatliche Zwangsmaßnahme vorausgeht und der Staat daher eine besondere Pflicht hat, bei deren Vollstreckung für deren Ordnungsmäßigkeit zu sorgen. Bei Absatz 2 ergibt sich die besondere Schutzbedürftigkeit aus der Würde des (hilflosen) Menschen.

Die in der Strafnorm objektivierte besondere Begehungsform ergibt sich aus dem Obhutsverhältnis (Opfer muss Täter der konkreten Ausgestaltung nach anvertraut gewesen sein) bzw. bei Absatz 2 aus dem Ausnutzen (Tatbegehung aufgrund geschwächter Widerstandskraft des Opfers).

Bei Absatz 1 sind die Tatfolgen für den Betroffenen erheblich, der das Vertrauen in den Staat durch derartige Tathandlungen verlieren kann und somit in die Gesellschaft schwer (wieder) einzugliedern ist. Bei Absatz 2 kommen als Tatfolge gemeinwohlschädliche Auswirkungen hinzu (Vertrauen der Allgemeinheit in den Staat, Kranke und Hilflose besonders zu schützen).

Zu Nummer 32 (Sexueller Missbrauch unter Ausnutzung einer Amtsstellung - § 174b Absatz 1 StGB)

Die Rechtsgüter „Sexuelle Selbstbestimmung sowie Integrität bei der Ausübung staatlicher Macht“ sind besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft. Die besondere Gewichtung zusammen mit der hohen Bedeutung ergibt sich aus dem hohen Vertrauen der Rechtsgemeinschaft in die Ordnungsmäßigkeit der Amtsführung und auch das hohe Vertrauen in eine umfassende Schutzwürdigkeit von Personen, denen freiheitsentziehenden Maßnahmen drohen können.

Die qualifizierte Anforderung besteht darin, dass Täter nur sein kann, wer an einem Straf- oder Unterbringungsverfahren als entscheidungserheblicher Amtsträger mitwirkt. Es reicht, dass der Täter das Verfahren nur zum Schein einleitet, um das Opfer unter Druck zu setzen, was besonders verwerflich ist und das Vertrauen der Rechtsgemeinschaft in einen funktionierenden Staat erschüttern kann.

Die Tatfolgen sind für den Betroffenen erheblich, da er das Vertrauen in den Staat durch eine solche Tathandlung verlieren kann und somit in die Gesellschaft schwerer eingliederbar ist.

Zu Nummer 33 (Sexueller Missbrauch unter Ausnutzung eines Beratungs-, Behandlungs- oder Betreuungsverhältnisses - § 174c Absatz 1 und 2 StGB)

Das Rechtsgut „Sexuelle Selbstbestimmung von Personen, die wegen einer psychischen oder körperlichen Beeinträchtigung oder einer Suchtkrankheit auf die sie beratenden, behandelnden oder betreuenden Personen angewiesen sind“ ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft. Die Gewichtung ergibt sich aus der Vertraulichkeit und Störungsfreiheit der angesprochenen Abhängigkeitsverhältnisse, an der die Rechtsgemeinschaft ein hohes Interesse hat. Gleichzeitig besteht ein hohes Interesse an dem Schutz der erkrankten Personen, die auf ein solches Abhängigkeitsverhältnis angewiesen sind. Das große Hilfsbedürfnis kranker bzw. labiler Personen, verbunden mit deren deutlich reduzierten Kritik- und Widerstandsfähigkeit hat besondere gesellschaftliche Relevanz und bedarf des Schutzes vor sexueller Ausbeutung.

Die Tatfolgen sind sowohl für das Vertrauen des Opfers, als auch der Bevölkerung in ein derartiges Verhältnis erheblich.

Zu Nummer 34 (Sexueller Übergriff; sexuelle Nötigung; Vergewaltigung - § 177 Absatz 1 und 2 StGB)

Das Rechtsgut „Sexuelle Selbstbestimmung einer Person“ ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft. Die Gewichtung ergibt sich

aus der hohen Bedeutung des Schutzguts für die Rechtsgemeinschaft: Der Schutz vor der Verletzung der sexuellen Selbstbestimmung ist ein gewichtiger Teilaspekt der Menschenwürde.

Die Tatbegehung ist aufgrund des damit verbundenen Gewalt- und Aggressionspotential, das vorrangig auf die Unterwerfung und Demütigung des Opfers abzielt, besonders qualifiziert.

Tatfolgenqualifiziert sind die mit der Tat verbundenen gravierenderen Langzeitfolgen für das Opfer.

Zu Nummer 35 (Förderung sexueller Handlungen Minderjähriger - § 180 Absatz 2 StGB)

Das Rechtsgut „Sexuelles Selbstbestimmungsrecht Minderjähriger“ ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft. Die Entwicklung der sexuellen Selbstbestimmung in einer sensiblen Entwicklungsphase frei von störenden Einflussnahmen Dritter, ist ein Rechtsgut von besonders hoher Bedeutung für die Rechtsgemeinschaft.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Die Tathandlung betrifft ein minderjähriges Opfer, auf das unmittelbar eingewirkt wird, auch und gerade unter Zwang, damit es gegen Entgelt sexuelle Handlungen an Dritten vornimmt bzw. von Dritten an sich vornehmen lässt bzw. das zur Durchführung solcher Sexualkontakte vermittelt wird.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist das Erleben von Sexualität als „käuflicher Ware“ und ein erster Schritt in die Kinderprostitution. Besonders gravierende Aspekte der Tatfolgen sind dabei die psychischen Langzeitfolgen mit ggf. Depressionen, Traumata und Verhaltensauffälligkeiten, die von Rückzug bis hin zu risikoreichem Verhalten reichen sowie der (ggf. dauerhaften) Erschütterung des Vertrauens in zwischenmenschliche Beziehungen.

Zu Nummer 36 (Zuhälterei - § 181a Absatz 1 StGB)

Das Rechtsgut „Sexuelle Selbstbestimmung, verstanden als die Freiheit, über die Bedingungen und Umstände der eigenen Sexualkontakte zu entscheiden“ ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft. Das bereits besonders gewichtige Rechtsgut enthält durch den implizierten Schutz der Würde der Prostituierten eine zusätzliche Verstärkung. Bei der Zuhälterei handelt es sich um ein ausbeuterisches oder dirigistisches Verhalten, das darauf abzielt, eine andere Person, die der Prostitution nachgeht, zu kontrollieren oder ihr Einkommen weitgehend an sich zu ziehen. Die besonders verwerfliche Tatbegehung liegt in der Ausbeutung/Missbrauch des in der Regel vorausgehenden Näheverhältnis. Daraus folgt auch die hohe Bedeutung für die Rechtsgemeinschaft.

Die besondere Tatbegehung (und damit die besondere Verwerflichkeit) liegt darin, dass i.d.R. mehrere Täter an der Zuhälterei beteiligt sind und somit Täternetzwerke bestehen, was die Hilflosigkeit und Ohnmacht der Opfer verstärken.

Die Tatfolgen sind für die Prostituierten durch massive psychische Schäden, Vorenthaltung finanzieller Mittel zur Lebensgestaltung sowie Alterssicherung, damit einhergehender totalen Kontrolle und Abhängigkeit sowie damit einhergehender körperlicher und/oder psychischer Gewalt gravierend.

Zu Nummer 37 (Sexueller Missbrauch von Jugendlichen - § 182 Absatz 1 und 2 StGB)

Das Rechtsgut „Sexuelle Selbstbestimmung“ ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft. Die ordnungsgemäße Entwicklung der sexuellen Selbstbestimmung in einer sensiblen Entwicklungsphase ist ein Rechtsgut von besonders hoher Bedeutung für die Rechtsgemeinschaft. Es gilt, diese Entwicklung auch vor Ausnutzung mittels materieller Anreize besonders zu schützen.

Die Tatfolgen bei einem nach § 182 strafbaren sexuellen Missbrauch von Jugendlichen sind als besonders gravierend einzustufen. Besonders gravierende Aspekte der Tatfolgen sind dabei die psychischen Langzeitfolgen mit ggf. Angststörungen, Depressionen, Traumata und einem erhöhten Suizidrisiko, Verhaltensauffälligkeiten, die von Rückzug bis hin zu risikoreichem Verhalten reichen sowie der (ggf. dauerhaften) Erschütterung des Vertrauens in zwischenmenschliche Beziehungen.

Zu Nummer 38 (Aussetzung - § 221 Absatz 1 StGB)

Der Schutz der physischen Existenz und Gesundheit eines Menschen in hilfloser Lage ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft. Dies ergibt sich daraus, dass der Schutz des Lebens und der Gesundheit bereits per se ein Rechtsgut von besonders gewichtiger Bedeutung ist.

Erschwerend kommt hier die herbeigeführte oder ausgenutzte hilflose Lage hinzu. Qualifizierend wirkt dabei eine Garantenstellung.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist der konkrete Gefährdungserfolg des Todes oder einer schweren Gesundheitsschädigung. Die Tatfolgen für das Opfer sind gravierend vor dem Hintergrund der enttäuschten (und von der Gesellschaft erwarteten) Solidaritäts- und Schutzpflicht.

Zu Nummer 39 (Menschenhandel - § 232 Absatz 1 StGB)

Der Schutz der persönlichen Freiheit einschließlich seiner sexuellen Selbstbestimmung vor Ausbeutung und seiner persönlichen Freiheit, über die Arbeitskraft zu verfügen sind Unterfälle der Menschenwürde und damit besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft. Menschenhandel ist eine schwere Verletzung der Menschenwürde und des Selbstbestimmungsrechts. Das Opfer befindet sich in einer Ausbeutungssituation, in denen die persönliche oder wirtschaftliche Zwangslage ausgenutzt wird (wie Zwangsarbeit, Prostitution, Bettelei oder Organentnahme). Im Kern geht es hier um ein Delikt, dass den Menschen als handelndes Subjekt gegen seine Instrumentalisierung und Ausbeutung schützt. Daher hat das Delikt eine hohe Bedeutung für die Rechtsgemeinschaft.

Die besondere Tatbegehung (und damit die besondere Verwerflichkeit) liegt in dem mehrstufigen Täternetzwerk, das die Nachschubebene (Rekrutierung der Opfer), die Logistikebene (Weitergabe der Opfer) sowie die eigentliche Ausbeutung (Basisebene) betrifft. Das Zusammenwirken von mehreren Tätern gegenüber einem Opfer erhöht dessen Hilflosigkeit und Ohnmacht und damit den Unrechtsgehalt.

Die Tatfolgen haben schwerwiegende Auswirkungen für die persönliche Freiheit der Opfer, verbunden mit tiefgehenden psychischen Störungen und sind damit besonders gravierend.

Zu Nummer 40 (Verschleppung - § 234a Absatz 3 StGB)

Der Schutz der persönlichen Freiheit und das Recht auf Verbleib im räumlichen Geltungsbereich des Gesetzes sind Unterfälle der Menschenwürde und damit besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft. Aufgrund der hohen kriminellen Energie sowie die Gefährlichkeit für das Opfer gilt dies auch für die Vorbereitung einer Verschleppung. Durch eine Verschleppung wird eines der zentralen Grundrechte (die Freiheit) massiv verletzt. Das Delikt führt zu einer hohen Beeinträchtigung des

Sicherheitsgefühls der Bevölkerung und kann daher von der Rechtsgemeinschaft nicht hingenommen werden.

Die Tatfolgen sind auch bereits bei Vorbereitungshandlungen besonders gravierend, da damit bereits ernsthaft das Recht auf Freiheit sowie auf Verbleib im räumlichen Geltungsbereich des Gesetzes gefährdet wird.

Zu Nummer 41 (Zerstörung wichtiger Arbeitsmittel - § 305 a Absatz 1 StGB)

Die Vorschrift dient neben dem Schutz des Eigentums an den in § 305a Absatz 1 StGB aufgeführten Arbeitsmitteln und Kfz auch dem öffentlichen Interesse an der Funktionsfähigkeit der in § 316b Absatz 1 Nummer 1 und 2 StGB aufgezählten Anlagen und Betriebe (BeckOK StGB/Weidemann, 67. Ed. 1.11.2025, StGB § 305a Rn. 2 f). Geschützt werden Arbeitsmittel zur Errichtung von Anlagen, die für die Allgemeinheit wichtig sind, so wie z.B. Einsatzfahrzeuge der Sicherheits- und Rettungskräfte. Insofern wird von § 305 Absatz 1 StGB die Funktionsfähigkeit von besonders wichtigen Arbeitsmitteln geschützt, die von hoher Bedeutung für die Rechtsgemeinschaft sind.

Die Schwere der Straftat ergibt sich zudem aus der besonderen Begehungsform, die in Absatz 1 objektiviert ist. Der Tatbestand beschreibt die vollständige oder teilweise Zerstörung der besonders schutzwürdigen Arbeitsmittel. Anders als bei § 303 StGB reicht eine bloße Beschädigung nicht aus.

Taterfolg ist, dass ein besonders schutzwürdiges Arbeitsmittel, das von besonderer Bedeutung für die Rechtsgemeinschaft ist, nicht mehr zweckentsprechend genutzt werden kann. Das § 305a StGB auch im Katalog des § 129a Absatz 2 Nummer 2 StGB enthalten ist, unterstreicht strafrechtsimmanent das besondere Folgenpotential dieser Tat zur Verunsicherung der Bevölkerung.

Zu Nummer 42 (Gefährliche Eingriffe in den Straßenverkehr - § 315b Absatz 1 und 2 StGB)

Die Vorschrift schützt die allgemeine Sicherheit des Straßenverkehrs sowie Leib, Leben und Eigentum. Insbesondere Leben und Gesundheit sind besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft.

Die Schwere der Straftat ergibt sich aus der besonderen Begehungsform, die in § 315b Absatz 1 StGB objektiviert ist. Der Tatbestand beschreibt bestimmte Tathandlungen durch die die Sicherheit des Straßenverkehrs beeinträchtigt wird. Es reicht daher keine irgendwie geartete Straßenverkehrsgefährdung, sondern nur die in der Vorschrift näher umschriebenen Eingriffe (BeckOK StGB/Kudlich, 67. Ed. 1.11.2025, StGB § 315b Rn. 5). Diese müssen zudem zu einer Gefährdung von Leib oder Leben eines anderen Menschen oder fremden Sachen von bedeutendem Wert führen.

Taterfolg ist eine Beeinträchtigung der Sicherheit des Straßenverkehrs. Die normale Betriebsgefahr wird gesteigert und der Verkehr in seinem ungestörten Ablauf gefährdet. In dieser Gefährdung kann bereits zugleich auch eine Gefahr für ein besonders gewichtiges Rechtsgut liegen. Das Ausbleiben eines Schadens hängt nur noch vom Zufall ab. Weiterer Bestandteil des Taterfolgs ist eine Gefährdung eines der benannten besonders gewichtigen Rechtsgüter. Gerade mit Blick auf die hohe Anzahl von Verkehrsteilnehmern kann hier oft eine hohe Anzahl an Menschenleben betroffen sein.

Zu Nummer 43 (Störung öffentlicher Betriebe - § 316b Absatz 1 und 2 StGB)

Der Betrieb bestimmter, gemeinschaftswichtigen Zwecken dienender Unternehmen, Einrichtungen und Anlagen gegen störende Eingriffe ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft. Die besondere Gewichtigkeit sowie die hohe Bedeutung für die Rechtsgemeinschaft ergeben sich aus der Bedeutung der

Versorgung der Bevölkerung mit lebenswichtigen Gütern (u.a. Wasser, Strom) sowie die Bedeutung der Funktionsfähigkeit aller der öffentlichen Ordnung oder Sicherheit dienenden Einrichtungen oder Anlagen.

Die besondere Tatfolgen sind geprägt durch die tiefgreifende Verunsicherung der Allgemeinheit und die Destabilisierung des Vertrauens in die staatliche Integrität.

Zu Nummer 44 (Störung von Telekommunikationsanlagen - § 317 Absatz 1 und 2 StGB)

Die Funktionsfähigkeit des öffentlichen Telekommunikationsverkehrs ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft. Die besondere Gewichtigkeit sowie die hohe Bedeutung für die Rechtsgemeinschaft ergeben sich daraus, dass die Funktionalität von Telefon, Internet und Mobilfunk für das moderne Leben, die Wirtschaft und die öffentliche Sicherheit essenziell ist. Verstärkend kommt die zunehmende Digitalisierung hinzu. Ausfälle von elektronisch verfügbaren Nachrichten, Zugänge zu Banken, Versicherungen, Gesundheitswesen etc. haben schwerwiegende Auswirkungen auf Gesellschaft, Staat und Wirtschaft.

Die besonderen Tatfolgen manifestieren sich im Ausfall einer lebensnotwendigen Infrastruktur mit massiven Störungen für sämtliche Bereiche der Bundesrepublik Deutschland.

Zu Nummer 45 (Beschädigung wichtiger Anlagen - § 318 Absatz 1 StGB)

Der Schutz gewisser Anlagen der öffentlichen Daseinsvorsorge einhergehend mit der Gefährdung von Leib und Leben der von ihrer Beeinträchtigung betroffenen Personen sind besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft. Die besondere Gewichtigkeit sowie die hohe Bedeutung für die Rechtsgemeinschaft ergeben sich daraus, dass hier Leib, Leben sowie die Funktionsfähigkeit wesentlicher Infrastruktur (Wasser, Verkehr, Bergbau) für die Allgemeinheit geschützt wird.

Die aufgeführten Anlagen (wie z.B. Wasserleitungen, Brücken, Fähren oder Dämme) sind für die Wasserversorgung, aber auch für die Fortbewegung oder dem Schutz der Bevölkerung insbesondere vor Hochwasser essentiell. Sofern ein entsprechender Schutz dieser Anlagen nicht gewährleistet werden kann, kommt es als besondere Tatfolge zu einem Vertrauensverlust der Bevölkerung in die staatliche Ordnung.

Zu Nummer 46 (Bestechlichkeit - § 332 Absatz 1 Satz 1; auch in Verbindung mit § 336 - Unterlassen der Diensthandlung)

Die Vorschrift schützt die generelle Gefährdung der Funktionsfähigkeit des Staatsapparates, die sich aus der verbotenen Beziehung zwischen Bestechendem und Bestochenem ergibt. Ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft liegt damit vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Nach Absatz 1 ist erforderlich, dass ein Amtsträger oder für den öffentlichen Dienst besonders Verpflichteter für eine vergangene, gleichzeitig vorgenommene oder künftige pflichtwidrige Diensthandlung einen Vorteil für sich oder einen Dritten fordert, sich versprechen lässt oder annimmt.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Diesbezüglich ist festzuhalten, dass bereits der Anschein von Käuflichkeit von Trägern staatlicher Funktionen das Vertrauen der Öffentlichkeit in die Sachlichkeit bzw. Lauterkeit staatlicher Tätigkeit nachhaltig beeinträchtigt. Ein Amtsträger, der eine Abwendung von Kernanforderungen seiner Dienstpflichten sogar in der Begehung von Straftaten betätigt, lässt darüber hinaus Wiederholungen erwarten. Dies hat eine breite Schädigung öffentlicher Funktionen

wie letztlich auch des Vertrauens der Bevölkerung in die Funktionsfähigkeit der staatlichen Einrichtungen zur Folge. Das o.g. Rechtsgut wird dadurch stark gefährdet.

Zu Nummer 47 (§ 18 Absätze 1 bis 5 jeweils in Verbindung mit Absatz 9 AWG)

Die Vorschrift schützt die Sicherheit der Bundesrepublik Deutschland, den Völkerfrieden, die auswärtigen Beziehungen der Bundesrepublik Deutschland, die übergeordneten Interessen des Gemeinwohls und das Allgemeinwohl. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung sind alle vorsätzlichen Verstöße gegen die wesentlichen Verbote und Genehmigungserfordernisse des europäischen und nationalen Außenwirtschaftsrecht. Neben den Verstößen gegen Embargos (Absatz 1) betrifft dies auch Verstöße gegen die maßgeblichen Genehmigungserfordernisse für die Ausfuhr und Verbringung kritischer Güter, für Handlungs- und Vermittlungsgeschäfte und für technische Hilfeleistung. Dabei handelt es sich um Tathandlungen, die mit hoher krimineller Energie ausgeführt werden müssen, um die beabsichtigten (Ausfuhr-)Geschäfte trotz Verboten und fehlender Genehmigungserfordernisse realisieren zu können. Dies gilt auch in den Fällen das Absatzes 9. Die besondere Schwere folgt im Falle des Absatzes 9 daraus, dass nicht nur das Erfolgsunwert identisch mit dem der dort genannten Tatbestandsverwirklichungen (Absatz 1 Nummer 4, Absatz 1a, Absatz 2 Nummer 1, 3, 4 oder Nummer 6, Absatz 4 Satz 1 Nummer 5 oder Absatz 5 Satz 1) ist, sondern das Handlungsunwert durch die Art der Begehung noch darüber hinaus geht. Dies ist tatbestandlich objektiviert darin angelegt, dass hier eine Ausfuhrgenehmigung nicht nur fehlt, sondern durch eine aktive Handlung „erwirkt oder erschlichen“ wird. Besonders augenscheinlich wird dies, wenn eine solche Genehmigung durch eine Drohung oder Bestechung erwirkt wird, aber auch das täuschende Erschleichen verkörpert eine – im Vergleich zu der „bloß fehlenden“ Genehmigung – besonders schwere Begehungsform.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist, dass u.a. Güter in Umlauf kommen, die zur Vollstreckung der Todesstrafe, zur Folter oder zu anderen grausamen, unmenschlichen oder erniedrigenden Behandlungen oder Strafe genutzt werden können oder sog. Dual-Use-Güter, die sowohl für zivile als auch für militärische Zwecke verwendet werden können. Darin eingeschlossen sind Güter, die zur Konstruktion, Entwicklung, Herstellung oder zum Einsatz von nuklearen, chemischen und biologischen Waffen oder ihren Trägersystemen genutzt werden können. Das gilt auch für Güter, die sowohl für nicht explosive Zwecke als auch für jedwede Form der Unterstützung bei der Herstellung von Kernwaffen oder sonstigen Kernsprengkörpern verwendet werden können. Dies bedroht die o.g. Rechtsgüter, insbesondere die Sicherheit der Bundesrepublik Deutschland und den Völkerfrieden.

Zu Nummer 48 (§ 19 Absatz 1 KrWaffKontrG)

Die Vorschrift dient der Verhinderung der Beteiligung Deutscher an der Errichtung von Anlagen zur Herstellung von Atomwaffen und schützt damit mittelbar den Weltfrieden. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist die Ausübung der tatsächlichen Gewalt über eine Atomwaffe, d.h. einer Massenvernichtungswaffe, bei deren Einsatz Hunderttausende von Menschen in kurzer Zeit sterben können. Erfasst ist sowohl der unerlaubte täterschaftliche Umgang mit Atomwaffen (Nr. 1), als auch eine diesbezügliche Verleitung (Nr. 2) bzw. Förderung (Nr. 2a).

Die besondere Schwere der Tat ergibt sich aus der Tatfolge. Durch die Tathandlung wird die Herstellung und Ausbreitung von Massenvernichtungswaffen gefördert. Dies befeuert den Nuklearterrorismus und ist damit eine ernsthafte Bedrohung für das o.g. Schutzgut.

Zu Nummer 49 (§ 20a Absatz 1 KrWaffKontrG)

Die Vorschrift schützt mittelbar Leib und Leben und den Weltfrieden. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist die verbotene Tätigkeit des Einsetzens, Entwickeln, Herstellen, Handel treiben, Erwerben, Überlassen, Einführen, Ausführen, Durchführen oder sonstige Ausübung der tatsächlichen Gewalt über Antipersonenminen oder Streumunition und damit gemeingefährlichen Kriegswaffen, die ein großes Schadenspotential aufweisen.

Die besondere Schwere der Tat ergibt sich aus der Tatfolge. Durch die Tathandlung wird die Herstellung und Ausbreitung von Antipersonenminen oder Streumunition gefördert, womit eine ernsthafte Bedrohung für die o.g. Schutzgüter einhergeht.

Zu Nummer 50 (§ 22a Absatz 1 KrWaffKontrG)

Die Vorschrift schützt mittelbar den Weltfrieden. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist der unerlaubte Umgang mit Kriegswaffen, d.h. ohne die entsprechende Genehmigung. Kriegswaffen sind solche Waffen, die explizit zur Kriegsführung bestimmt sind (§ 1 Absatz 1 KrWaffKontrG), d.h. ein großes Schadenspotential aufweisen.

Die besondere Schwere der Tat ergibt sich aus der Tatfolge. Durch die Tathandlung wird die Herstellung und Ausbreitung von Kriegswaffen gefördert, womit eine ernsthafte Bedrohung für das o.g. Schutzgut einhergeht.

Zu Nummer 51 (§ 51 Absatz 1 WaffG)

Die Vorschrift schützt die öffentliche Sicherheit und Ordnung und Leib und Leben durch die Begrenzung der Verbreitung und Nutzung von Waffen. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist der Erwerb, Besitz, Überlassung, Führen, Verbringen, Mitnehmen, Herstellen, Bearbeiten, Instandsetzen oder Handel treiben mit verbotenen Schusswaffen zum Verschießen von Patronenmunition. Damit handelt es sich bei den verbotenen Schusswaffen um sog. „scharfe“ Schusswaffen, da nur diese Patronenmunition verschießt (u.a. vollautomatische Schusswaffen und Pumpguns).

Die besondere Schwere der Tat ergibt sich aus der Tatfolge. Durch die Tathandlung wird die Herstellung, Nutzung und Verbreitung von verbotenen scharfen Schusswaffen gefördert, was eine ernsthafte Bedrohung für die o.g. Schutzgüter bedeutet.

Zu Nummer 52 (§ 52 Absatz 1 WaffG)

Die Vorschrift schützt die öffentliche Sicherheit und Ordnung und Leib und Leben durch die Begrenzung der Verbreitung und Nutzung von Waffen. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist das unerlaubte Ausüben der tatsächlichen Gewalt über Waffen oder Waffenteile bzw. Munition, u.a. ehemalige Kriegswaffen und Molotow-Cocktails.

Die besondere Schwere der Tat ergibt sich aus der Tatfolge. Durch die Tathandlung wird die Herstellung und Verbreitung der o.g. Waffen gefördert, was eine ernsthafte Bedrohung für die o.g. Schutzgüter bedeutet.

Zu Nummer 53 (§16 Absatz 1 CWÜAG)

Die Vorschrift schützt die Sicherheit der Bundesrepublik und den Völkerfrieden. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

§ 16 Abs. 1 CWÜAG beinhaltet Strafvorschriften im Zusammenhang mit der Zuwiderhandlung von u.a. Ausfuhrbeschränkungen, die sich aus den Verpflichtungen des sog. „Chemiewaffenübereinkommens“ ergeben. Die besondere Schwere dieser Straftat ergibt sich aus der Gefahr, welche aus ihrer Verwirklichung entstehen kann. Tatbestandlich ist diese Gefahr – und folglich auch die besondere Schwere eines Verstoßes – darin angelegt, dass der Straftatbestand letztlich einer Verbreitung von chemischen Waffen, welche aufgrund ihrer verheerenden Wirkungen und perfiden Natur völkerrechtlich geächtet sind, entgegenwirkt. Ein Verstoß gegen dieses Verbot ist somit in objektivierter Weise mit einem besonderen Tatunrecht verbunden. Überdies ist ein Verstoß für Beteiligte auch aufgrund des Gepräges der Tatbestandsverwirklichung, welche gerade mit Blick auf die historische Verwendung dieser Waffen betrachtet werden muss, als besonders schwere Straftat zu erkennen. Da ein Vertrieb der entsprechenden Chemikalien nur von spezialisierten Händlern mit hoher chemischer Sachkenntnis in Betracht kommt, ist zudem davon auszugehen, dass diese Kenntnis von der (möglichen) Verwendung in Chemiewaffen haben. Nur vorsätzliche Taten werden von der Übermittlungsbefugnis erfasst, da das besondere Tatunrecht einer aktiven Mitwirkung an der Verbreitung von Chemiewaffen nur bei vorsätzlicher Begehung anzunehmen ist.

Ein praktisches Beispiel für einen solchen Fall wäre der vorsätzliche Export einer Chemikalie, welche Nordkorea die Produktion von Chemiewaffen ermöglicht. Insbesondere vor dem Hintergrund der nordkoreanischen Unterstützung Russlands in seinem Angriffskrieg gegen die Ukraine kann eine solche CWÜ-widrige Aktivität zu einer erheblichen Gefährdung außen- und sicherheitspolitischer Interessen der Bundesrepublik Deutschland und seiner Verbündeten führen.

Zu Anlage 2 (zu § 81 Absatz 2 Nummer 2 BNDG)

Zu Nummer 1 (Aufstacheln zum Verbrechen der Aggression, § 80a StGB)

Die Vorschrift schützt den „Weltfrieden“. Ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft liegt damit vor.

Die Gewichtigkeit ergibt sich daraus, dass die Rechtsgemeinschaft ein hohes Interesse am friedlichen Zusammenleben der Bundesrepublik Deutschland mit anderen Völkern hat.

Die besondere Schwere der Straftat ergibt sich zum einen aus der Tathandlung und zum anderen aus der Zielrichtung der Tathandlung. Tathandlung ist das Aufstacheln, also das Aufhetzen, durch das in bestimmter, zielgerichteter Weise zu einer emotional gesteigerten Haltung angereizt wird, also eine auf die Gefühle der Adressaten abzielende Propaganda. Zielrichtung der Tathandlung ist zum Verbrechen der Aggression aufzustacheln, d.h. zur Vorbereitung eines Angriffskrieges gegen ein anderes Land.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Schließlich kommt eine Radikalisierung größerer Bevölkerungsteile in Betracht, da der Täter darauf abzielt einen größeren Personenkreis zu erreichen (Öffentlich, Versammlung, Verbreiten). Dadurch wird ein gesellschaftliches Klima befeuert, dass die Vorbereitung eines Angriffskrieges begünstigt und damit eine erhebliche Gefahr für das o.g. Schutzgut „Weltfrieden“ darstellt.

Zu Nummer 2 (Vorbereitung eines hochverräterischen Unternehmens, § 83 Absatz 2 StGB)

Die Vorschrift schützt die dem Föderalismusprinzip zu Grunde liegende territoriale und konstitutionelle Eigenständigkeit der Länder. Damit liegt ein besonderes gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Die besondere Schwere der Straftat ist im Tatbestand objektiviert. Tathandlung ist die Vorbereitung eines bestimmten hochverräterischen Unternehmens gegen ein Land, d.h. die Vorbereitung eines Umsturzes unter Anwendung von Gewalt oder einer entsprechenden Drohung, siehe § 82 StGB. Folglich liegt ein besonderes Gewaltpotential vor. „Bestimmt“ heißt, dass das Unternehmen nach der Vorstellung des Täters in seinen wesentlichen Grundzügen (Angriffsziel und Angriffsgegenstand, sowie grobe Umrisse von Zeit, Ort und Art und Weise der Durchführung) bereits feststehen muss. Vorbereitung sind alle Handlungen, die das hochverräterische Unternehmen mittelbar oder unmittelbar fördern und geeignet sind die verfassungsmäßige Ordnung eines Landes zu beeinträchtigen oder zu ändern.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge, da der Hochverrat gegen ein Land Ziel der vorbereitenden Handlungen ist. Beim Hochverrat handelt es sich um das schwerste Verbrechen gegen die Existenz eines Staates. Das o.g. Schutzgut wird dadurch gefährdet.

Zu Nummer 3 (Fortführung einer für verfassungswidrig erklärten Partei, § 84 Absatz 1 Satz 1, Absatz 2 und 3 StGB)

Die Vorschrift schützt die freiheitlich demokratische Grundordnung. Ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft liegt damit vor.

Die besonders schwere Straftat ist im Tatbestand objektiviert. Als Tathandlung wird das Handeln als Rädelsführer oder Hintermann einer vom BVerfG für verfassungswidrig erklärten Partei (Nr. 1) oder einer Partei, von der das BVerfG festgestellt hat, dass sie Ersatzorganisation ist (Nr. 2) erfasst. Rädelsführer ist, wer in einer Organisation dadurch eine führende Rolle spielt, dass er sich in besonders maßgebender Weise für sie betätigt. Hintermann ist, wer geistig oder wirtschaftlich Wesentliches für die Partei leistet, dabei jedoch im Hintergrund bleibt. In beiden Fällen handeln Personen mit wesentlichem Einfluss auf die Organisation.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Diese ist die Aufrechterhaltung des organisatorischen Zusammenhalts einer verbotenen Partei bzw. Ersatzorganisation, sodass deren verfassungsfeindliche Ziele im Geltungsbereich des Grundgesetzes organisiert weiterverfolgt werden können. Gerade in der Aufrechterhaltung eines Zusammenschlusses mehrerer Personen wohnt eine Eigendynamik inne, die zu einer Steigerung der Gefährlichkeit für wichtige Rechtsgüter der Gemeinschaft führt. Diese für größere Personenzusammenschlüsse typische Eigendynamik hat ihre besondere Gefährlichkeit darin, dass sie geeignet ist, dem einzelnen Beteiligten die Begehung von Straftaten zu erleichtern und bei ihm das Gefühl persönlicher Verantwortung zurückzudrängen. Damit geht ein erhebliches Gefährdungspotential für das o.g. Schutzgut „freiheitlich demokratische Grundordnung“ einher.

Zu Nummer 4 (Verstoß gegen ein Vereinigungsverbot, § 85 Absatz 1 StGB)

Die Vorschrift schützt die freiheitlich demokratische Grundordnung und den Gedanken der Völkerverständigung. Besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft liegen damit vor.

Dass es sich bei § 85 Absatz 1 StGB um eine besonders schwere Straftat handelt, ergibt sich bereits aus der besonderen Begehungsform, die im Tatbestand objektiviert ist. Als Tathandlung erfasst wird das Handeln als Rädelsführer oder Hintermann einer Partei oder

Vereinigung von der unanfechtbar festgestellt ist, dass sie Ersatzorganisation einer verbotenen Partei ist (Nr. 1) oder einer Vereinigung, die unanfechtbar verboten ist, oder von der unanfechtbar festgestellt ist, dass sie Ersatzorganisation einer solchen verbotenen Vereinigung ist (Nr. 2). Rädelsführer ist, wer in einer Organisation dadurch eine führende Rolle spielt, dass er sich in besonders maßgebender Weise für sie betätigt. Hintermann ist, wer geistig oder wirtschaftlich Wesentliches für die Partei leistet, dabei jedoch im Hintergrund bleibt. In beiden Fällen handeln Personen mit wesentlichem Einfluss auf die Organisation.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Diese ist die Aufrechterhaltung des organisatorischen Zusammenhalts der o.g. Partei oder Vereinigung, sodass sie weiter gegen Strafgesetze, die verfassungsmäßige Ordnung bzw. den Gedanken der Völkerverständigung verstoßen. Gerade in der Aufrechterhaltung eines Zusammenschlusses mehrerer Personen wohnt eine Eigendynamik inne, die zu einer Steigerung der Gefährlichkeit für wichtige Rechtsgüter der Gemeinschaft führt. Diese für größere Personenzusammenschlüsse typische Eigendynamik hat ihre besondere Gefährlichkeit darin, dass sie geeignet ist, dem einzelnen Beteiligten die Begehung von Straftaten zu erleichtern und bei ihm das Gefühl persönlicher Verantwortung zurückzudrängen. Darüber hinaus werden durch die Aufrechterhaltung möglicherweise auch etwaige Radikalisierungen vorangetrieben, die mitunter in abgeschlossenen Räumen stattfinden.

Zu Nummer 5 (Agententätigkeit zu Sabotagezwecken, § 87 Absatz 1 StGB)

Die Vorschrift schützt den Bestand und die Sicherheit der Bundesrepublik Deutschland. Damit liegt ein besonderes gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich bereits aus der besonderen Begehungsform, die im Tatbestand objektiviert ist, nämlich dem Tätigwerden auf einen Auftrag einer „Regierung, Vereinigung oder Einrichtung außerhalb des räumlichen Geltungsbereichs dieses Gesetzes“ hin. Dieses Tatbestandsmerkmal beschreibt typischerweise besonderes Gefährdungspotenzial, sei es durch die besonderen Gefährdungsfähigkeiten eines Staates in der Tatbegehung oder durch die Einbettung in ein über das einzelne Delikt hinausweisendes Gesamtgeschehen.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge sind Vorbereitungshandlungen für konkret und abschließend beschriebene Sabotagehandlungen (s. Absatz 2, u.a. schwere Brandstiftungsdelikte und Herbeiführung einer Sprengstoffexplosion) mit dem Ziel des Zerstörens, Beschädigens, Beseitigens etc. eines für die Landesverteidigung, für den Schutz der Zivilbevölkerung gegen Kriegsgefahren oder für die Gesamtwirtschaft wichtigen Unternehmens bzw. Betriebes.

Zu Nummer 6 (Ausübung fremder Einflussnahme und darauf gerichtete Agententätigkeit, § 87a StGB)

Die Vorschrift schützt die Souveränität und Sicherheit der Bundesrepublik Deutschland. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Die besonders schwere Straftat ergibt sich bereits aus der besonderen Begehungsform, die im Tatbestand objektiviert ist, da die Tatbegehung hier für eine fremde Macht erfolgt. Dieser Tatbestand beschreibt typischerweise besonderes Gefährdungspotenzial, sei es durch die besonderen Gefährdungsfähigkeiten eines Staates in der Tatbegehung oder durch die Einbettung in ein über das einzelne Delikt hinausweisendes Gesamtgeschehen (bei staatlichem Vorgehen ist generell von planvollem Handeln und systematischem Vorgehen auszugehen).

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist neben der Begehung der eigentlichen Straftat die hinzutretende Verletzung der

Souveränität der Bundesrepublik Deutschland, da die Straftat auf Weisung einer fremden Macht auf deutschem Boden erfolgt. Die Souveränität ist auch dann verletzt, wenn es sich um weniger schwere Straftaten handelt, weil sich auch diese destabilisierend auf die freiheitlich-demokratische Grundordnung auswirken können, was von der ausländischen staatlichen Stelle regelmäßig auch bezweckt sein wird. Durch das Erteilen eines Auftrags zur Begehung von Straftaten auf deutschem Boden oder Handeln im Auftrag einer fremden Macht ergibt sich daher ein besonderes Bedrohungspotential für die Sicherheit der Bundesrepublik Deutschland.

Zu Nummer 7 (Verfassungsfeindliche Sabotage, § 88 StGB)

Die Vorschrift schützt den Bestand und die Sicherheit der Bundesrepublik Deutschland sowie die verfassungsmäßige Ordnung. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Der Tatbestand beschreibt die erfolgreiche (Abs. 1) bzw. versuchte (Abs. 2) Durchführung von Sabotagehandlungen an Anlagen von wesentlicher Bedeutung. Geschützt werden Unternehmen oder Anlagen, die der öffentlichen Versorgung mit Postdienstleistungen oder dem öffentlichen Verkehr dienen, Telekommunikationsanlagen, bestimmte Versorgungseinrichtungen, sowie der öffentlichen Sicherheit und Ordnung dienende Einrichtungen. Da es sich um Anlagen handelt, die öffentlichen Zwecken dienen, geht dies mit einer Betroffenheit großer Teile der Bevölkerung einher (Bsp.: Brandanschläge auf kritische Infrastruktur und hybride Bedrohungen durch staatliche Akteure (Stichwort: Unterseekabel)).

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist, dass die geschützte Einrichtung ganz oder teilweise stillgelegt oder ihren bestimmungsmäßigen Zwecken entzogen wird.

Zu Nummer 8 (Verunglimpfung des Bundespräsidenten, § 90 Absatz 1 und 3 StGB)

Die Vorschrift dient dem Schutz der Person und des Amtes des Bundespräsidenten iS seiner Funktionen während der jeweiligen Amtszeit; dahinter steht der beabsichtigte Schutz des Staates und seiner verfassungsmäßigen Ordnung. Hierbei handelt es sich um besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist eine Verunglimpfung, d. h. erheblichere Ehrenkränkung (Abs. 1, vgl. Fischer/Anstötz, StGB, 72. Aufl. 2025, § 90 Rn. 2), bzw. eine Verleumdung gemäß § 187 StGB (Absatz 3). Der erhöhte Strafrahmen des Absatzes 3 kommt auch dann zur Anwendung, wenn der Täter sich durch die Tat nach Absatz 1 absichtlich für Bestrebungen gegen den Bestand der Bundesrepublik Deutschland oder gegen Verfassungsgrundsätze einsetzt. Vorausgesetzt ist jeweils, dass die Tat öffentlich, in einer Versammlung oder durch Verbreiten eines Inhalts (§ 11 Absatz 3 StGB) begangen wird. Ein Anwendungsfall sind etwa Maßnahmen Dritter im Bereich der Desinformation sein (z.B. Fake-News).

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die bewirkte Verunglimpfung. Darüber hinaus ist aufgrund des Öffentlichkeitsbezugs eine Förderung der gesellschaftlichen Radikalisierung möglich. Die Tatfolgen beeinträchtigen die o.g. Schutzgüter.

Zu Nummer 9 (Verunglimpfung des Staates und seiner Symbole für extremistische Bestrebungen, § 90a Absatz 3 StGB)

Die Vorschrift schützt den Bestand und die verfassungsmäßige Ordnung der Bundesrepublik Deutschland und ihrer Länder in ihrer konkreten Verfassungsordnung (vgl. Fischer/Anstötz, StGB, 72. Aufl. 2025, § 90a Rn. 2). Hierbei handelt es sich um besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist zum einen „beschimpfen“ oder „böswillig verächtlich machen“ des Bundes oder der Länder bzw. ein Verunglimpfen der wichtigsten Staatssymbole (Abs. 1). Zum anderen u.a. das Zerstören, Beschädigen und Unbrauchbarmachen von Hoheitszeichen (Abs. 2). Beides mit der Absicht sich für Bestrebungen gegen den Bestand der Bundesrepublik Deutschland oder gegen Verfassungsgrundsätze einzusetzen und jeweils verbunden mit einem gewissen Öffentlichkeitsbezug, konkret öffentlich, in einer Versammlung oder durch Verbreiten eines Inhalts (§ 11 Absatz 3 StGB). Dies kann insbesondere Teil hybrider Maßnahmen Dritter im Bereich der Desinformation sein (Bsp.: Fake-News).

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die bewirkte Verunglimpfung. Aufgrund des Öffentlichkeitsbezugs ist darüber hinaus die Förderung der gesellschaftlichen Radikalisierung eine mögliche Tatfolge, Damit beeinträchtigen die Tatfolgen die o.g. Schutzgüter.

Zu Nummer 10 (Verfassungsfeindliche Verunglimpfung von Verfassungsorganen, § 90b Absatz 1 StGB)

Die Vorschrift schützt die bezeichneten Verfassungsorgane. Hierbei handelt es sich um besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist die das Ansehen des Staates gefährdende Verunglimpfung von Verfassungsorganen (Gesetzgebungsorgan, Regierung, Verfassungsgerichte bzw. deren Mitglieder) in der Öffentlichkeit, in einer Versammlung oder durch Verbreiten eines Inhalts (§ 11 Absatz 3 StGB). Der Täter muss absichtlich handeln. Dies kann insbesondere Teil hybrider Maßnahmen Dritter im Bereich der Desinformation sein (z.B. Fake-News).

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die bewirkte Verunglimpfung, d.h. die Herabwürdigung. Aufgrund des Öffentlichkeitsbezugs ist darüber hinaus die Förderung der gesellschaftlichen Radikalisierung eine mögliche Tatfolge, damit beeinträchtigen die Tatfolgen die o.g. Schutzgüter.

Zu Nummer 11 (Offenbaren von Staatsgeheimnissen, § 95 Absatz 1 StGB)

Die Vorschrift schützt die äußere Sicherheit der Bundesrepublik Deutschland. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist einem Unbefugten oder der Öffentlichkeit die Möglichkeit zu verschaffen, von einem Staatsgeheimnis im Sinne des § 93 Absatz 1 StGB Kenntnis zu nehmen.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die konkrete Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland aufgrund der möglichen Kenntnisnahme von einem Staatsgeheimnis durch Unbefugte oder der Öffentlichkeit und damit auch durch eine fremde Macht. Insbesondere durch die mögliche Folgeverwendung des Staatsgeheimnisses drohen gemeinwohlschädliche Auswirkungen zulasten des o.g. Schutzgutes (vgl. § 4 Absatz 2 SÜG).

Zu Nummer 12 (Landesverräterische Ausspähung; Auskundschaften von Staatsgeheimnissen, § 96 Absatz 2 Satz 1 StGB)

Die Vorschrift schützt die äußere Sicherheit der Bundesrepublik Deutschland. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist das Sich-Verschaffen von Staatsgeheimnissen, die von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten werden, um einem Unbefugten oder der

Öffentlichkeit die Möglichkeit zu verschaffen, von diesen Kenntnis zu nehmen. Staatsgeheimnisse sind Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht geheim gehalten werden müssen, um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden (§ 93 Absatz 1 StGB).

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die Vorbereitungshandlung zum Offenbaren von Staatsgeheimnissen, womit eine konkrete Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland einhergeht. Insbesondere durch die mögliche Folgeverwendung des Staatsgeheimnisses (z.B. durch fremde Mächte) drohen gemeinwohlschädliche Auswirkungen zulasten des o.g. Schutzgutes (vgl. § 4 Absatz 2 SÜG).

Zu Nummer 13 (Preisgabe von Staatsgeheimnissen, § 97 Absatz 1 StGB)

Die Vorschrift schützt die äußere Sicherheit der Bundesrepublik Deutschland. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist die Preisgabe von Staatsgeheimnissen im Sinne des § 93 Absatz 1 StGB.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die durch die Preisgabe des Staatsgeheimnisses (mindestens) fahrlässige Herbeiführung eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland. Insbesondere durch die mögliche Folgeverwendung des Staatsgeheimnisses drohen gemeinwohlschädliche Auswirkungen zulasten des o.g. Schutzgutes (vgl. § 4 Absatz 2 SÜG).

Zu Nummer 14 (Landesverräterische Agententätigkeit, § 98 Absatz 1 Satz 1 StGB)

Die Vorschrift schützt die äußere Sicherheit der Bundesrepublik Deutschland. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand, da die Tatbegehung in Nr. 1 für eine fremde Macht erfolgt. Dieser Tatbestand beschreibt typischerweise besonderes Gefährdungspotenzial, sei es durch die besonderen Gefährdungsfähigkeiten eines Staates in der Tatbegehung oder durch die Einbettung in ein über das einzelne Delikt hinausweisendes Gesamtgeschehen (bei staatlichem Vorgehen ist generell von planvollem Handeln und systematischem Vorgehen auszugehen). Bzgl. Nr. 2 bezieht sich die Tathandlung auf ein zweifelsfreies und ernst gemeintes Bereiterklären für eine fremde Macht Staatsgeheimnisse zu Erlangen bzw. diese mitzuteilen.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die Ausübung der Tätigkeit bzw. das Bereiterklären, verbunden mit der abstrakten Gefahr, die regelmäßig durch die Involvierung einer „fremden Macht“ im Zusammenhang mit Staatsgeheimnissen besteht. Das Schutzgut der äußeren Sicherheit ist damit gefährdet.

Zu Nummer 15 (Landesverräterische Fälschung, § 100a Absatz 1 und 2 StGB)

Die Vorschrift schützt die äußere Sicherheit der Bundesrepublik Deutschland. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung sind gezielte Falschmeldungen, die den Staat diffamieren und geeignet sind, das Vertrauen anderer Länder in die außenpolitische Verlässlichkeit der Bundesrepublik Deutschland zu erschüttern.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik

Deutschland oder ihre Beziehungen zu einer fremden Macht. Im Informationszeitalter werden Nachrichten ohne Verzug über die ganze Welt verbreitet, d.h. es ist so gut wie unmöglich, sie wieder „einzufangen“ und ihre Unrichtigkeit klarzustellen. Es kann dadurch ein unabsehbarer außenpolitischer Schaden entstehen.

Zu Nummer 16 (Angriff gegen Organe und Vertreter ausländischer Staaten, § 102 Absatz 1 erste Alternative StGB)

Die Vorschrift schützt neben Leib und Leben, konkret von ausländischen Staatsoberhäuptern und Regierungsvertretern, welche sich in amtlicher Eigenschaft im Inland aufhalten, auch das Interesse der Bundesrepublik Deutschland an guten und ungestörten Beziehungen zu anderen Staaten. Hierbei handelt es sich um besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist ein Angriff auf Leib oder Leben, der sich gezielt auch auf den auslandsstaatlichen Status der betroffenen Personen beziehen muss.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist neben der möglichen Tötung oder Körperverletzung auch eine Belastung funktionierender bzw. diplomatischer Beziehungen zwischen dem ausländischen Staat und der Bundesrepublik Deutschland

Zu Nummer 17 (Nötigung des Bundespräsidenten und von Mitgliedern eines Verfassungsorgans, § 106 Absatz 1 StGB)

Die Vorschrift schützt den Bundespräsidenten und die Funktionsfähigkeit und -freiheit der Mitglieder der genannten Verfassungsorgane und damit ein gewichtiges Rechtsgut.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist die rechtswidrige Nötigung von Verfassungsorganen mit Gewalt oder durch Drohung mit einem empfindlichen Übel.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die Manipulation des Verfassungsorgans dahingehend, seine aus der Organstellung folgenden Befugnisse in einem bestimmten Sinne auszuüben bzw. davon Abstand zu nehmen. Das o.g. Schutzgut wird damit verletzt.

Zu Nummer 18 (Wahlbehinderung, § 107 Absatz 1 StGB)

Das Rechtsgut „Schutz der Wahlen“, konkret des ordnungsgemäßen Gesamtablaufs sowie die Richtigkeit des Wahlergebnisses und damit die Volkssouveränität als Teil der freiheitlichen, demokratischen Grundordnung, ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist der Einsatz von Gewalt oder die Drohung mit Gewalt, um eine Wahl oder die Feststellung ihres Ergebnisses zu verhindern oder zu stören, d.h. nicht unerheblich zu erschweren bzw. zu verzögern.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die Verhinderung oder Störung einer Wahl oder der Feststellung ihres Ergebnisses und damit die Wahlbehinderung einer Vielzahl von Personen. Dies führt zu einer erheblichen Beeinträchtigung der Kernfunktionen der Demokratie und bedroht das Vertrauen der Bevölkerung in deren Funktionsfähigkeit und damit das o.g. Rechtsgut.

Zu Nummer 19 (Wahlfälschung, § 107a Absatz 2 StGB)

Die Vorschrift schützt das unverfälschte Wahlergebnis und somit mittelbar die demokratische Entscheidungsfindung und damit die Volkssouveränität als Teil der freiheitlichen, demokratischen Grundordnung. Ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft liegt damit vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist die unrichtige Verkündung des Ergebnisses einer Wahl.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist eine unrichtige Wahlverkündung. Dies führt zu einer erheblichen Beeinträchtigung der Kernfunktionen der Demokratie und bedroht das Vertrauen der Bevölkerung in deren Funktionsfähigkeit.

Zu Nummer 20 (Wählernötigung, § 108 Absatz 1 StGB)

Die Vorschrift schützt die freie Stimmabgabe, d.h. die Entscheidung des einzelnen Wahlberechtigten über das Ob und das Wie seiner Stimmabgabe. Damit wird werden mittelbar der ordnungsgemäße Ablauf der Wahl und damit die Volkssouveränität als Teil der freiheitlichen, demokratischen Grundordnung geschützt. Ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft liegt somit vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist der Einsatz von Gewalt, Drohung mit einem empfindlichen Übel, Missbrauch eines beruflichen oder wirtschaftlichen Abhängigkeitsverhältnisses oder sonstiger wirtschaftlicher Druck, um einen Wahlberechtigten zu nötigen bzw. daran zu hindern zu wählen oder von seinem Wahlrecht in einem bestimmten Sinne Gebrauch zu machen.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Taterfolg ist, dass der Wahlberechtigte entgegen seinem Willen gezwungen wird, überhaupt oder in einem bestimmten Sinn zu wählen oder seine Stimmabgabe zu unterlassen, obwohl er zur Wahl bereit ist. Das o.g. Schutzgut wird dadurch massiv beeinträchtigt. Die Tathandlung führt folglich zu einer Beeinträchtigung der Kernfunktionen der Demokratie und bedroht das Vertrauen der Bevölkerung in deren Funktionsfähigkeit.

Zu Nummer 21 (Störpropaganda gegen die Bundeswehr, § 109d Absatz 1 StGB)

Die Vorschrift schützt die Funktionsfähigkeit der Bundeswehr und damit mittelbar die Landesverteidigung, die der Gewährleistung des Bestandes und der Sicherheit des Bundes dient. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung sind unwahre oder gröblich entstellte Behauptungen tatsächlicher Art, deren Verbreitung geeignet ist, die Tätigkeit der Bundeswehr zu stören, wider besseres Wissen zum Zwecke der Verbreitung aufstellt oder solche Behauptungen in Kenntnis ihrer Unwahrheit verbreitet, um die Bundeswehr in der Erfüllung ihrer Aufgabe der Landesverteidigung zu behindern.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist eine potentielle Störung der Tätigkeit der Bundeswehr bzw. eine Behinderung in der Erfüllung ihrer Aufgabe der Landesverteidigung. Die damit verbundene Schwächung der äußeren Sicherheit stellt eine erhebliche Gefährdung des o.g. Schutzgutes dar.

Zu Nummer 22 (Sabotagehandlungen an Verteidigungsmitteln, § 109e Absatz 1 und 2 StGB)

Die Vorschrift schützt die Funktionsfähigkeit von Verteidigungsmitteln und dient damit mittelbar der Verteidigungsfähigkeit zur Gewährleistung des Bestandes und der Sicherheit des

Bundes. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung sind Sabotagehandlungen, die die Funktionsfähigkeit von Wehrmitteln sowie Einrichtungen und Anlagen der Verteidigung der Bundesrepublik Deutschland sowie des Zivilschutzes gegen Kriegsgefahren betreffen.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die konkrete Gefährdung der Sicherheit der Bundesrepublik Deutschland, der Schlagkraft der Truppe oder Menschenleben und damit insbesondere eine Schwächung der äußeren Sicherheit, was eine erhebliche Gefährdung des o.g. Schutzgutes darstellt.

Zu Nummer 23 (Sicherheitsgefährdender Nachrichtendienst, § 109f Absatz 1 StGB)

Die Vorschrift schützt die Sicherheit der Bundesrepublik Deutschland und die Schlagkraft der Streitkräfte. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Als Tathandlung wird vorausgesetzt, dass jemand für eine Dienststelle, eine Partei oder eine andere Vereinigung außerhalb des räumlichen Geltungsbereichs des Strafgesetzbuchs oder für eine verbotene Vereinigung oder für einen ihrer Mittelsmänner Nachrichten über Angelegenheiten der Landesverteidigung sammelt, diesbezüglich einen Nachrichtendienst betreibt oder für diese Tätigkeiten anwirbt bzw. sie unterstützt und dadurch Bestrebungen dient, die gegen die Sicherheit der Bundesrepublik Deutschland oder die Schlagkraft der Streitkräfte gerichtet sind.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist, dass Bestrebungen gedient wird, die sich gegen die Sicherheit der Bundesrepublik Deutschland oder die Schlagkraft der Streitkräfte richten.

Zu Nummer 24 (Sicherheitsgefährdendes Abbilden, § 109g Absatz 1 und 3 StGB)

Die Vorschrift schützt die Sicherheit der Bundesrepublik Deutschland und die Schlagkraft der Streitkräfte. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist das Abbilden und Beschreiben militärischer Gegenstände bzw. das Gelangenlassen einer solchen Abbildung oder Beschreibung an andere, in dem Wissen, dass dadurch die Sicherheit der Bundesrepublik Deutschland oder die Schlagkraft der Streitkräfte gefährdet wird.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist die wissentliche Gefährdung der Sicherheit der Bundesrepublik Deutschland oder der Schlagkraft der Streitkräfte.

Zu Nummer 25 (Anwerben für fremden Wehrdienst, § 109h Absatz 1 StGB)

Die Rechtsgüter „Schutz des Wehrpotentials“ und „Wahrung der politischen Neutralität“ dienen dem Bestand und der Sicherheit des Bundes sowie bestimmten auf das Verhältnis zum Ausland gerichteten Interessen der Bundesrepublik Deutschland. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist das Anwerben zum Wehrdienst und das Zuführen zu Werbern oder zum Wehrdienst und dessen Einrichtungen zugunsten einer ausländischen Macht.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Taterfolg ist eine erfolgte Verpflichtung bzw. die Zuführung des Opfers in den Einflussbereich einer ausländischen Macht bzw. von Werbern oder einer militärischen Einrichtung. Damit einher geht eine Entziehung des Opfers aus dem Einflussbereich der Bundesrepublik Deutschland, sodass die Opfer nicht mehr als „Wehrpotential“ bzw. personelle Ressource für die Bundesrepublik Deutschland zur Verfügung stehen, was eine Schwächung der Sicherheit der Bundesrepublik Deutschland zur Folge hat.

Zu Nummer 26 (Öffentliche Aufforderung zu Straftaten, § 111 Absatz 1 StGB), sofern die rechtswidrige Tat, zu der aufgefordert wird, eine besonders schwere Straftat im Sinne dieser Vorschrift ist)

Die Vorschrift schützt das Rechtsgut der jeweils angesonnenen Vorschrift und den inneren Gemeinschaftsfrieden. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Vorausgesetzt wird, dass öffentlich, in einer Versammlung oder durch Verbreiten eines Inhalts zu einer bestimmten besonders schweren Straftat aufgefordert wird, also jedenfalls dann, wenn diese eine Höchstfreiheitsstrafe von fünf Jahren aufweist.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist ein Angriff sowohl gegen die Rechtsgüter der Bezugstaten als auch gegen das überindividuelle Rechtsgut des inneren Gemeinschaftsfrieden, aufgrund der mit der öffentlichen Aufforderung verbundenen Gefahr des „aus dem Rudern Laufens“ eines durch den Auffordernden in Gang gesetzten Kausalverlaufs. Die o.g. Rechtsgüter sind dadurch unmittelbar betroffen.

Zu Nummer 27 (Betreiben krimineller Handelsplattformen im Internet (§ 127 Absatz 1 StGB), wenn eine besonders schwere Straftat nach § 127 Absatz 1 Satz 2 Nummer 2 StGB ermöglicht oder gefördert wird)

Die Vorschrift schützt die öffentliche Sicherheit und Ordnung und zugleich die Rechtsgüter der in Bezug genommen Straftaten (damit u.a. Leib und Leben). Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand, sofern jemand eine Handelsplattform im Internet betreibt, deren Zweck darauf gerichtet ist, die Begehung von besonders schweren Straftaten nach § 127 Absatz 1 Satz 2 Nummer 2 StGB zu ermöglichen oder zu fördern. Dies betrifft vor allem solche Plattformen, auf denen professionell illegale Güter und Dienstleistungen („Cybercrime-as-a-Service“) sowie der Austausch von kriminalitätsbezogenen Informationen angeboten werden.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist, dass durch die aktive Bereitstellung der virtuellen Infrastruktur einem unbegrenzten Adressatenkreis inkriminierte Angebote zugänglich gemacht werden und damit breitflächig, mitunter anonym, schwere Kriminalität gefördert wird, wie z.B. Menschenhandel im Internet, wodurch die Gemeinschaft geschädigt wird. Die o.g. Schutzgüter werden dadurch stark gefährdet.

Zu Nummer 28 (Bildung krimineller Vereinigungen, § 129 Absatz 1 Satz 1 iVm Absatz 5 Satz 1 und 2 StGB)

Die Rechtsgüter „Öffentliche Sicherheit“, „Staatliche Ordnung“ und „Öffentlicher Frieden“ sind besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft. Die besondere Gewichtigkeit ergibt sich daraus, dass die öffentliche Sicherheit und Ordnung fundamentale Basis für ein funktionierendes Zusammenleben und die Wahrnehmung von Grundrechten in einer Gemeinschaft bildet.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Ein besonders schwerer Fall liegt vor, wenn der Täter Rädelsführer oder Hintermann einer Vereinigung ist, deren Zweck oder Tätigkeit auf die Begehung von Straftaten gerichtet ist. Rädelsführer ist, wer in der Vereinigung dadurch eine führende Rolle spielt, dass er sich in besonders maßgebender Weise für sie betätigt. Hintermann ist, wer – im Unterschied zum Rädelsführer – zwar nicht Mitglied der Vereinigung ist, gleichwohl aber die Vereinigung als Außenstehender dadurch wesentlich fördert, dass er geistig oder wirtschaftlich maßgebenden Einfluss auf die Führung der Vereinigung hat. Rädelsführer und Hintermann haben somit maßgeblichen Einfluss auf die Vereinigung.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Diesbezüglich ist festzuhalten, dass bereits durch die bloße Existenz krimineller Vereinigungen auf Grund ihrer inneren Struktur, spezifischen Organisation und Zielsetzung das Sicherheitsgefühl der Allgemeinheit beeinträchtigt und unter dem Aspekt der öffentlichen Sicherheit und Ordnung als massive Bedrohung anzusehen ist (Bsp.: Organisierte Kriminalität oder politisch/ideologisch-extremistische Organisationen, insb. aus dem extremen linken und rechten Spektrum). Der kriminellen Vereinigung wohnt eine Eigendynamik inne, die zu einer Steigerung der Gefährlichkeit für wichtige Rechtsgüter der Gemeinschaft führt. Diese für größere Personenzusammenschlüsse typische Eigendynamik hat ihre besondere Gefährlichkeit darin, dass sie geeignet ist, dem einzelnen Beteiligten die Begehung von Straftaten zu erleichtern und bei ihm das Gefühl persönlicher Verantwortung zurückzudrängen. Tatfolge des Handelns als Rädelsführer bzw. Hintermann ist, dass durch deren Mitwirken die Vereinigung maßgeblich in ihrem kriminellen Tun unterstützt wird und somit entscheidend zu einer Steigerung der Gefährlichkeit für wichtige Rechtsgüter der Gemeinschaft beigetragen wird. Dadurch werden die o.g. Rechtsgüter stark gefährdet.

Zu Nummer 29 (Bildung terroristischer Vereinigungen, § 129a Absatz 3 und 5 Satz 1 zweite Alternative sowie Satz 2 StGB)

Die Vorschrift schützt die innere öffentliche Sicherheit, da sie auf den Schutz vor besonders gefährlichen Vereinigungen gerichtet ist und der Bildung und dem Fortbestand derartiger schwerkrimineller Gruppierungen entgegenwirken soll. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Absatz 3 setzt als Tathandlung das Gründen oder das Sichbeteiligen als Mitglied an einer Vereinigung voraus, deren Tätigkeit bzw. Zweck auf die Androhung von Straftaten nach § 129a Absatz 1 und 2 StGB gerichtet ist. D.h. es wird eine künftige Straftat nach § 129a Absatz 1 und 2 StGB in Aussicht gestellt, auf deren Begehung die Vereinigung Einfluss hat oder zumindest zu haben vorgibt. Absatz 5 setzt als Tathandlung das Unterstützen bzw. das Werben um Mitglieder oder Unterstützer voraus. Die Unterstützungshandlung bezieht sich dabei auf terroristische Vereinigungen, die besonders schwere Strafen androhen. Das Werben bezieht sich hingegen auf terroristische Vereinigungen, deren Zwecke oder deren Tätigkeiten auf die tatsächliche Begehung von besonders schweren Straftaten gerichtet sind.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Diesbezüglich ist festzuhalten, dass bereits durch die bloße Existenz terroristischer Vereinigungen auf Grund ihrer inneren Struktur, spezifischen Organisation und insbesondere ihrer Zielsetzung das Sicherheitsgefühl der Allgemeinheit beeinträchtigt und unter dem Aspekt der inneren öffentlichen Sicherheit als massive Bedrohung anzusehen ist (Bsp.: Politisch/ideologisch-extremistische Organisationen, die die Abschaffung der freiheitlich-demokratischen Grundordnung der Bundesrepublik Deutschland sowie die Schaffung eines neuen deutschen Staatswesens zum Ziel haben). Der terroristischen Vereinigung wohnt eine Eigendynamik inne, die zu einer Steigerung der Gefährlichkeit für wichtige Rechtsgüter der Gemeinschaft führt. Diese für größere Personenzusammenschlüsse typische Eigendynamik hat ihre besondere Gefährlichkeit darin, dass sie geeignet ist, dem einzelnen Beteiligten die Begehung von Straftaten zu erleichtern und bei ihm das Gefühl persönlicher Verantwortung

zurückzudrängen. Durch die o.g. Tathandlungen wird die Gefährlichkeit der Vereinigung weiter gefestigt. Das o.g. Rechtsgut wird dadurch stark gefährdet.

Zu Nummer 30 (Sexueller Missbrauch von Schutzbefohlenen, § 174 Absatz 1 und 2 StGB)

Das Rechtsgut „Sexuelle Selbstbestimmung von Schutzbefohlenen“ ist ein besonders gewichtiges Rechtsguter mit hoher Bedeutung für die Rechtsgemeinschaft. Die besondere Gewichtigkeit ergibt sich daraus, dass sich die Schutzbefohlenen in einem besonderen Vertrauensverhältnis befinden. Dieses schützenwerte Verhältnis ergibt sich z.B. aufgrund staatlicher Anordnung (z.B. Schulpflicht, staatliche Betreuungsverhältnis), aufgrund von Arbeitsverhältnissen oder aufgrund der familiären Stellung. Für die Rechtsgemeinschaft ist es von hoher Bedeutung, dass sich Schutzbefohlene, die sich, u.U. auch zwangsweise, in einem solchen Rechtsverhältnis befinden, sich dabei auf den Schutz der Rechtsordnung verlassen können. Anderenfalls führt es zu gesellschaftlichem Misstrauen gegenüber staatlicher Anordnung sowie gegenüber gesellschaftlich gewünschten und volkswirtschaftlich nötigen Arbeitsverhältnissen. Der besondere staatliche Schutzauftrag für die Familie folgt aus Artikel 6 Grundgesetz.

Die besonderen Tatfolgen ergeben sich aus der entwicklungspsychologisch nachhaltigen Schädigung des Schutzbefohlenen, der ggf. erhebliche Schwierigkeiten hat, sich wieder in die Gesellschaft zu integrieren, was wiederum nicht im Sinne der Rechtsgemeinschaft ist. Die besondere Tatbegehung ergibt sich daraus, dass eine Autoritätsperson, die zum Vertrauen verpflichtet ist, gerade dieses Vertrauen missbraucht.

Zu Nummer 31 (Sexueller Mißbrauch von Gefangenen, behördlich Verwahrten oder Kranken und Hilfsbedürftigen in Einrichtungen, § 174a Absatz 1 und 2 StGB)

Die Rechtsgüter „Sexuelle Selbstbestimmung von Gefangenen, behördlich Verwahrten oder Kranken und Hilfsbedürftigen in Einrichtungen sowie die Integrität dieser Institutionen“ sind besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft. Die besondere Gewichtigkeit ergibt sich daraus, dass die Rechtsgemeinschaft ein hohes Interesse an der Integrität der Institutionen sowie ein hohes Interesse an dem Schutz des Zwecks der Verwahrung hat (z.B. Strafvollzug) als auch ein Vertrauen in die Objektivität der für Gefangene (u.s.w.) verantwortlichen Personen besteht. Ebenso besteht dieses hohe Interesse in dem Schutz der sexuellen Selbstbestimmung der in Absatz 1 und Absatz 2 genannten Personen. Dies gilt umso mehr, als bei Absatz 1 eine staatliche Zwangsmaßnahme vorausgeht und der Staat daher eine besondere Pflicht hat, bei deren Vollstreckung für deren Ordnungsmäßigkeit zu sorgen. Bei Absatz 2 ergibt sich die besondere Schutzbedürftigkeit aus der Würde des (hilflosen) Menschen.

Eine qualifizierte Anforderung besteht in dem Obhutsverhältnis (Opfer muss Täter der konkreten Ausgestaltung nach anvertraut gewesen sein) bzw. bei Absatz 2 im Ausnutzen (Tatbegehung aufgrund geschwächter Widerstandskraft des Opfers).

Bei Absatz 1 sind die Tatfolgen für den Betroffenen erheblich, der das Vertrauen in den Staat durch derartige Tathandlungen verlieren kann und somit in die Gesellschaft schwer (wieder) einzugliedern ist. Bei Absatz 2 kommen als Tatfolge gemeinwohlschädliche Auswirkungen hinzu (Vertrauen der Allgemeinheit in den Staat, Kranke und Hilflose besonders zu schützen).

Zu Nummer 32 (Sexueller Mißbrauch unter Ausnutzung einer Amtsstellung, § 174b Absatz 1 StGB)

Die Rechtsgüter „Sexuelle Selbstbestimmung sowie Integrität bei der Ausübung staatlicher Macht“ sind besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft. Die besondere Gewichtung zusammen mit der hohen Bedeutung ergibt sich aus dem hohen Vertrauen der Rechtsgemeinschaft in die Ordnungsmäßigkeit der Amtsführung

und auch das hohe Vertrauen in eine umfassende Schutzwürdigkeit von Personen, denen freiheitsentziehenden Maßnahmen drohen können.

Die qualifizierte Anforderung besteht darin, dass Täter nur sein kann, wer an einem Straf- oder Unterbringungsverfahren als entscheidungserheblicher Amtsträger mitwirkt. Es reicht, dass der Täter das Verfahren nur zum Schein einleitet, um das Opfer unter Druck zu setzen, was besonders verwerflich ist und das Vertrauen der Rechtsgemeinschaft in einen funktionierenden Staat erschüttern kann.

Die Tatfolgen sind für den Betroffenen erheblich, da er das Vertrauen in den Staat durch eine solche Tathandlung verlieren kann und somit in die Gesellschaft schwer eingliederbar ist.

Zu Nummer 33 (Sexueller Mißbrauch unter Ausnutzung eines Beratungs-, Behandlungs- oder Betreuungsverhältnisses, § 174c Absatz 1 und 2 StGB)

Das Rechtsgut „Sexuelle Selbstbestimmung von Personen, die wegen einer psychischen oder körperlichen Beeinträchtigung oder einer Suchtkrankheit auf die sie beratenden, behandelnden oder betreuenden Personen angewiesen sind“ ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft.

Die Gewichtung ergibt sich aus der Vertraulichkeit und Störungsfreiheit der angesprochenen Abhängigkeitsverhältnisse, an der die Rechtsgemeinschaft ein hohes Interesse hat. Gleichzeitig besteht ein hohes Interesse an dem Schutz der erkrankten Personen, die auf ein solches Abhängigkeitsverhältnis angewiesen sind. Das große Hilfsbedürfnis kranker bzw. labiler Personen, verbunden mit deren deutlich reduzierten Kritik- und Widerstandsfähigkeit hat besondere gesellschaftliche Relevanz und bedarf des Schutzes vor sexueller Ausbeutung.

Die Tatfolgen sind sowohl für das Vertrauen des Opfers, als auch der Bevölkerung in ein derartiges Verhältnis erheblich.

Zu Nummer 34 (Sexueller Übergriff; sexuelle Nötigung; Vergewaltigung, § 177 Absatz 1 und 2 StGB)

Das Rechtsgut „Sexuelle Selbstbestimmung einer Person“ ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft. Die Gewichtung ergibt sich aus der hohen Bedeutung des Schutzguts für die Rechtsgemeinschaft: Der Schutz vor der Verletzung der sexuellen Selbstbestimmung ist ein gewichtiger Teilaspekt der Menschenwürde.

Die Tatbegehung ist aufgrund des damit verbundenen Gewalt- und Aggressionspotential, das vorrangig auf die Unterwerfung und Demütigung des Opfers abzielt, besonders qualifiziert.

Tatfolgenqualifiziert sind die mit der Tat verbundenen gravierenderen Langzeitfolgen für das Opfer.

Zu Nummer 35 (Förderung sexueller Handlungen Minderjähriger, § 180 Absatz 2)

Das Rechtsgut „Sexuelles Selbstbestimmungsrecht Minderjähriger“ ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft. Die Entwicklung der sexuellen Selbstbestimmung in einer sensiblen Entwicklungsphase frei von störenden Einflussnahmen Dritter, ist ein Rechtsgut von besonders hoher Bedeutung für die Rechtsgemeinschaft.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Die Tathandlung betrifft ein minderjähriges Opfer, auf das unmittelbar eingewirkt wird, auch und

gerade unter Zwang, damit es gegen Entgelt sexuelle Handlungen an Dritten vornimmt bzw. von Dritten an sich vornehmen lässt bzw. das zur Durchführung solcher Sexualkontakte vermittelt wird.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist das Erleben von Sexualität als „käuflicher Ware“ und ein erster Schritt in die Kinderprostitution. Besonders gravierende Aspekte der Tatfolgen sind dabei die psychischen Langzeitfolgen mit ggf. Depressionen, Traumata und Verhaltensauffälligkeiten, die von Rückzug bis hin zu risikoreichem Verhalten reichen sowie der (ggf. dauerhaften) Erschütterung des Vertrauens in zwischenmenschliche Beziehungen.

Zu Nummer 36 (Zuhälterei, § 181a Absatz 1 StGB)

Das Rechtsgut „Sexuelle Selbstbestimmung, verstanden als die Freiheit, über die Bedingungen und Umstände der eigenen Sexualkontakte zu entscheiden“ ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft. Das bereits besonders gewichtige Rechtsgut enthält durch den implizierten Schutz der Würde der Prostituierten eine zusätzliche Verstärkung. Bei der Zuhälterei handelt sich um ein ausbeuterisches oder dirigistisches Verhalten, das darauf abzielt, eine andere Person, die der Prostitution nachgeht, zu kontrollieren oder ihr Einkommen weitgehend an sich zu ziehen. Die besonders verwerfliche Tatbegehung liegt in der Ausbeutung/Missbrauch des in der Regel vorausgehenden Näheverhältnis. Daraus folgt auch die hohe Bedeutung für die Rechtsgemeinschaft.

Die besondere Tatbegehung (und damit die besondere Verwerflichkeit) liegt darin, dass i.d.R. mehrere Täter an der Zuhälterei beteiligt sind und somit Täternetzwerke bestehen, was die Hilflosigkeit und Ohnmacht der Opfer verstärken.

Die Tatfolgen sind für die Prostituierten durch massive psychische Schäden, Vorenthaltung finanzieller Mittel zur Lebensgestaltung sowie Alterssicherung, damit einhergehender totalen Kontrolle und Abhängigkeit sowie damit einhergehender körperlicher und/oder psychischer Gewalt gravierend.

Zu Nummer 37 (Sexueller Missbrauch von Jugendlichen, § 182 Absatz 1 und 2 StGB)

Das Rechtsgut „Sexuelle Selbstbestimmung“ ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft. Die ordnungsgemäße Entwicklung der sexuellen Selbstbestimmung in einer sensiblen Entwicklungsphase ist ein Rechtsgut von besonders hoher Bedeutung für die Rechtsgemeinschaft. Es gilt, diese Entwicklung auch vor Ausnutzung mittels materieller Anreize besonders zu schützen.

Die Tatfolgen bei einem nach § 182 strafbaren sexuellen Missbrauch von Jugendlichen sind als besonders gravierend einzustufen. Besonders gravierende Aspekte der Tatfolgen sind dabei die psychischen Langzeitfolgen mit ggf. Angststörungen, Depressionen, Traumata und einem erhöhten Suizidrisiko, Verhaltensauffälligkeiten, die von Rückzug bis hin zu risikoreichem Verhalten reichen sowie der (ggf. dauerhaften) Erschütterung des Vertrauens in zwischenmenschliche Beziehungen.

Zu Nummer 38 (Aussetzung, § 221 Absatz 1 StGB)

Der Schutz der physischen Existenz und Gesundheit eines Menschen in hilfloser Lage ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft. Dies ergibt sich daraus, dass der Schutz des Lebens und der Gesundheit bereits per se ein Rechtsgut von besonders gewichtiger Bedeutung ist.

Erschwerend kommt hier die herbeigeführte oder ausgenutzte hilflose Lage hinzu. Qualifizierend wirkt dabei eine Garantenstellung.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Tatfolge ist der konkrete Gefährdungserfolg des Todes oder einer schweren Gesundheitsschädigung. Die Tatfolgen für das Opfer sind gravierend vor dem Hintergrund der enttäuschten (und von der Gesellschaft erwarteten) Solidaritäts- und Schutzpflicht.

Zu Nummer 39 (Menschenhandel, § 232 Absatz 1 StGB)

Der Schutz der persönlichen Freiheit einschließlich seiner sexuellen Selbstbestimmung vor Ausbeutung und seiner persönlichen Freiheit, über die Arbeitskraft zu verfügen sind Unterfälle der Menschenwürde und damit besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft. Menschenhandel ist eine schwere Verletzung der Menschenwürde und des Selbstbestimmungsrechts. Das Opfer befindet sich in einer Ausbeutungssituation, in denen die persönliche oder wirtschaftliche Zwangslage ausgenutzt wird (wie Zwangsarbeit, Prostitution, Bettelei oder Organentnahme). Im Kern geht es hier um ein Delikt, dass den Menschen als handelndes Subjekt gegen seine Instrumentalisierung und Ausbeutung schützt. Daher hat das Delikt eine hohe Bedeutung für die Rechtsgemeinschaft.

Die besondere Tatbegehung (und damit die besondere Verwerflichkeit) liegt in dem mehrstufigen Täternetzwerk, das die Nachschubebene (Rekrutierung der Opfer), die Logistikebene (Weitergabe der Opfer) sowie die eigentliche Ausbeutung (Basisebene) betrifft. Das Zusammenwirken von mehreren Tätern gegenüber einem Opfer erhöht dessen Hilflosigkeit und Ohnmacht und damit den Unrechtsgehalt.

Die Tatfolgen haben schwerwiegende Auswirkungen für die persönliche Freiheit der Opfer, verbunden mit tiefgehenden psychischen Störungen und sind damit besonders gravierend.

Zu Nummer 40 (Verschleppung, § 234a Absatz 3 StGB)

Der Schutz der persönlichen Freiheit und das Recht auf Verbleib im räumlichen Geltungsbereich des Gesetzes sind Unterfälle der Menschenwürde und damit besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft. Aufgrund der hohen kriminellen Energie sowie die Gefährlichkeit für das Opfer gilt dies auch für die Vorbereitung einer Verschleppung. Durch eine Verschleppung wird eines der zentralen Grundrechte (die Freiheit) massiv verletzt. Das Delikt führt zu einer hohen Beeinträchtigung des Sicherheitsgefühls der Bevölkerung und kann daher von der Rechtsgemeinschaft nicht hingenommen werden.

Die Tatfolgen sind auch bereits bei Vorbereitungshandlungen besonders gravierend, da damit bereits ernsthaft das Recht auf Freiheit sowie auf Verbleib im räumlichen Geltungsbereich des Gesetzes gefährdet wird.

Zu Nummer 42 (Zerstörung wichtiger Arbeitsmittel, § 305a Absatz 1)

Die Vorschrift dient neben dem Schutz des Eigentums an den in § 305a Absatz 1 StGB aufgeführten Arbeitsmitteln und Kfz auch dem öffentlichen Interesse an der Funktionsfähigkeit der in § 316b Absatz 1 Nummer 1 und 2 StGB aufgezählten Anlagen und Betriebe (BeckOK StGB/Weidemann, 67. Ed. 1.11.2025, StGB § 305a Rn. 2 f). Geschützt werden Arbeitsmittel zur Errichtung von Anlagen, die für die Allgemeinheit wichtig sind, so wie zum Beispiel Einsatzfahrzeuge der Sicherheits- und Rettungskräfte. Insofern wird von § 305a Absatz 1 StGB die Funktionsfähigkeit von besonders wichtigen Arbeitsmitteln geschützt, die von hoher Bedeutung für die Rechtsgemeinschaft sind.

Die Schwere der Straftat ergibt sich zudem aus der besonderen Begehungsform, die in Absatz 1 objektiviert ist. Der Tatbestand beschreibt die vollständige oder teilweise Zerstörung der besonders schutzwürdigen Arbeitsmittel. Anders als bei § 303 StGB reicht eine bloße Beschädigung nicht aus.

Taterfolg ist, dass ein besonders schutzwürdiges Arbeitsmittel, das von besonderer Bedeutung für die Rechtsgemeinschaft ist, nicht mehr zweckentsprechend genutzt werden kann. Das § 305a StGB auch im Katalog des § 129a Absatz 2 Nummer 2 StGB enthalten ist, unterstreicht strafrechtsimmanent das besondere Folgenpotential dieser Tat zur Verunsicherung der Bevölkerung.

Zu Nummer 43 (Gefährliche Eingriffe in den Straßenverkehr, § 315b Absatz 1 und 2)

Die Vorschrift schützt die allgemeine Sicherheit des Straßenverkehrs sowie Leib, Leben und Eigentum. Insbesondere Leben und Gesundheit sind besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft.

Die Schwere der Straftat ergibt sich aus der besonderen Begehungsform, die in § 315b Absatz 1 StGB objektiviert ist. Der Tatbestand beschreibt bestimmte Tathandlungen durch die die Sicherheit des Straßenverkehrs beeinträchtigt wird. Es reicht daher keine irgendwie geartete Straßenverkehrsgefährdung, sondern nur die in der Vorschrift näher umschriebenen Eingriffe (BeckOK StGB/Kudlich, 67. Ed. 1.11.2025, StGB § 315b Rn. 5). Diese müssen zudem zu einer Gefährdung von Leib oder Leben eines anderen Menschen oder fremden Sachen von bedeutendem Wert führen.

Taterfolg ist eine Beeinträchtigung der Sicherheit des Straßenverkehrs. Die normale Betriebsgefahr wird gesteigert und der Verkehr in seinem ungestörten Ablauf gefährdet. In dieser Gefährdung kann bereits zugleich auch eine Gefahr für ein besonders gewichtiges Rechtsgut liegen. Das Ausbleiben eines Schadens hängt nur noch vom Zufall ab. Weiterer Bestandteil des Taterfolgs ist eine Gefährdung eines der benannten besonders gewichtigen Rechtsgüter. Gerade mit Blick auf die hohe Anzahl von Verkehrsteilnehmern kann hier oft eine hohe Anzahl an Menschenleben betroffen sein.

Zu Nummer 44 (Störung öffentlicher Betriebe, § 316b Absatz 1 und 2)

Der Betrieb bestimmter, gemeinschaftswichtigen Zwecken dienender Unternehmen, Einrichtungen und Anlagen gegen störende Eingriffe ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft.

Die besondere Gewichtigkeit sowie die hohe Bedeutung für die Rechtsgemeinschaft ergeben sich aus der Bedeutung der Versorgung der Bevölkerung mit lebenswichtigen Gütern (u.a. Wasser, Strom) sowie die Bedeutung der Funktionsfähigkeit aller der öffentlichen Ordnung oder Sicherheit dienenden Einrichtungen oder Anlagen.

Die besondere Tatfolgen sind geprägt durch die tiefgreifende Verunsicherung der Allgemeinheit und die Destabilisierung des Vertrauens in die staatliche Integrität.

Zu Nummer 45 (Störung von Telekommunikationsanlagen, § 317 Absatz 1 und 2)

Die Funktionsfähigkeit des öffentlichen Telekommunikationsverkehrs ist ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft.

Die besondere Gewichtigkeit sowie die hohe Bedeutung für die Rechtsgemeinschaft ergeben sich daraus, dass die Funktionalität von Telefon, Internet und Mobilfunk für das moderne Leben, die Wirtschaft und die öffentliche Sicherheit essenziell ist. Verstärkend kommt die zunehmende Digitalisierung hinzu. Ausfälle von elektronisch verfügbaren Nachrichten, Zugänge zu Banken, Versicherungen, Gesundheitswesen etc. haben schwerwiegende Auswirkungen auf Gesellschaft, Staat und Wirtschaft.

Die besonderen Tatfolgen manifestieren sich im Ausfall einer lebensnotwendigen Infrastruktur mit massiven Störungen für sämtliche Bereiche der Bundesrepublik Deutschland.

Zu Nummer 46 (Beschädigung wichtiger Anlagen, § 318 Absatz 1 StGB)

Der Schutz gewisser Anlagen der öffentlichen Daseinsvorsorge einhergehend mit der Gefährdung von Leib und Leben der von ihrer Beeinträchtigung betroffenen Personen sind besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft. Die besondere Gewichtigkeit sowie die hohe Bedeutung für die Rechtsgemeinschaft ergeben sich daraus, dass hier Leib, Leben sowie die Funktionsfähigkeit wesentlicher Infrastruktur (Wasser, Verkehr, Bergbau) für die Allgemeinheit geschützt wird.

Die aufgeführten Anlagen (wie z.B. Wasserleitungen, Brücken, Fähren oder Dämme) sind für die Wasserversorgung, aber auch für die Fortbewegung oder dem Schutz der Bevölkerung insbesondere vor Hochwasser essentiell. Sofern ein entsprechender Schutz dieser Anlagen nicht gewährleistet werden kann, kommt es als besondere Tatfolge zu einem Vertrauensverlust der Bevölkerung in die staatliche Ordnung.

Zu Nummer 47 (Bestechlichkeit (§ 332 Absatz 1 Satz 1 StGB), auch in Verbindung mit § 336 StGB (Unterlassen der Diensthandlung))

Die Vorschrift schützt die generelle Gefährdung der Funktionsfähigkeit des Staatsapparates, die sich aus der verbotenen Beziehung zwischen Bestechendem und Bestochenem ergibt. Ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft liegt damit vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Nach Absatz 1 ist erforderlich, dass ein Amtsträger oder für den öffentlichen Dienst besonders Verpflichteter für eine vergangene, gleichzeitig vorgenommene oder künftige pflichtwidrige Diensthandlung einen Vorteil für sich oder einen Dritten fordert, sich versprechen lässt oder annimmt.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Diesbezüglich ist festzuhalten, dass bereits der Anschein von Käuflichkeit von Trägern staatlicher Funktionen das Vertrauen der Öffentlichkeit in die Sachlichkeit bzw. Lauterkeit staatlicher Tätigkeit nachhaltig beeinträchtigt. Ein Amtsträger, der eine Abwendung von Kernanforderungen seiner Dienstpflichten sogar in der Begehung von Straftaten betätigt, lässt darüber hinaus Wiederholungen erwarten. Dies hat eine breite Schädigung öffentlicher Funktionen wie letztlich auch des Vertrauens der Bevölkerung in die Funktionsfähigkeit der staatlichen Einrichtungen zur Folge. Das o.g. Rechtsgut wird dadurch stark gefährdet.

Zu Nummer 48 (§ 18 Absatz 1 bis 5 jeweils in Verbindung mit Absatz 6 und 9 AWG)

Die Vorschrift schützt die generelle Gefährdung der Funktionsfähigkeit des Staatsapparates, die sich aus der verbotenen Beziehung zwischen Bestechendem und Bestochenem ergibt. Ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft liegt damit vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Nach Absatz 1 ist erforderlich, dass ein Amtsträger oder für den öffentlichen Dienst besonders Verpflichteter für eine vergangene, gleichzeitig vorgenommene oder künftige pflichtwidrige Diensthandlung einen Vorteil für sich oder einen Dritten fordert, sich versprechen lässt oder annimmt.

Darüber hinaus ergibt sich die besondere Schwere der Tat auch aus der Tatfolge. Diesbezüglich ist festzuhalten, dass bereits der Anschein von Käuflichkeit von Trägern staatlicher Funktionen das Vertrauen der Öffentlichkeit in die Sachlichkeit bzw. Lauterkeit staatlicher Tätigkeit nachhaltig beeinträchtigt. Ein Amtsträger, der eine Abwendung von Kernanforderungen seiner Dienstpflichten sogar in der Begehung von Straftaten betätigt, lässt darüber hinaus Wiederholungen erwarten. Dies hat eine breite Schädigung öffentlicher Funktionen wie letztlich auch des Vertrauens der Bevölkerung in die Funktionsfähigkeit der staatlichen Einrichtungen zur Folge. Das o.g. Rechtsgut wird dadurch stark gefährdet.

Auch bei § 18 Absatz 9 AWG handelt es sich um eine besonders schwere Straftat. Die besondere Schwere folgt im Falle des Absatzes 9 daraus, dass nicht nur das Erfolgsunwert identisch mit dem der dort genannten Tatbestandsverwirklichungen (Absatz 1 Nummer 4, Absatz 1a, Absatz 2 Nummer 1, 3, 4 oder Nummer 6, Absatz 4 Satz 1 Nummer 5 oder Absatz 5 Satz 1) ist, sondern das Handlungsunwert durch die Art der Begehung noch darüber hinaus geht. Dies ist tatbestandlich objektiviert darin angelegt, dass hier eine Ausfuhrgenehmigung nicht nur fehlt, sondern durch eine aktive Handlung „erwirkt oder erschlichen“ wird. Besonders augenscheinlich wird dies, wenn eine solche Genehmigung durch eine Drohung oder Bestechung erwirkt wird, aber auch das täuschende Erschleichen verkörpert eine – im Vergleich zu der „bloß fehlenden“ Genehmigung – besonders schwere Begehungsform.

Zu Nummer 49 (§ 19 Absatz 1 KrWaffKontrG)

Die Vorschrift des Kriegswaffenkontrollgesetzes dient der Verhinderung der Beteiligung Deutscher an der Errichtung von Anlagen zur Herstellung von Atomwaffen und schützt damit mittelbar den Weltfrieden. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist die Ausübung der tatsächlichen Gewalt über eine Atomwaffe, d.h. einer Massenvernichtungswaffe, bei deren Einsatz Hunderttausende von Menschen in kurzer Zeit sterben können. Erfasst ist sowohl der unerlaubte täterschaftliche Umgang mit Atomwaffen (Nr. 1), als auch eine diesbezügliche Verleitung (Nr. 2) bzw. Förderung (Nr. 2a).

Die besondere Schwere der Tat ergibt sich aus der Tatfolge. Durch die Tathandlung wird die Herstellung und Ausbreitung von Massenvernichtungswaffen gefördert. Dies befeuert den Nuklearterrorismus und ist damit eine ernsthafte Bedrohung für das o.g. Schutzgut.

Zu Nummer 50 (§ 20a Absatz 1 KrWaffKontrG)

Die Vorschrift des Kriegswaffenkontrollgesetzes schützt mittelbar Leib und Leben und den Weltfrieden. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist die verbotene Tätigkeit des Einsetzens, Entwickeln, Herstellen, Handel treiben, Erwerben, Überlassen, Einführen, Ausführen, Durchführen oder sonstige Ausübung der tatsächlichen Gewalt über Antipersonenminen oder Streumunition und damit gemeingefährlichen Kriegswaffen, die ein großes Schadenspotential aufweisen.

Die besondere Schwere der Tat ergibt sich aus der Tatfolge. Durch die Tathandlung wird die Herstellung und Ausbreitung von Antipersonenminen oder Streumunition gefördert, womit eine ernsthafte Bedrohung für die o.g. Schutzgüter einhergeht.

Zu Nummer 51 (§ 22a Absatz 1 KrWaffKontrG)

Die Vorschrift des Kriegswaffenkontrollgesetzes schützt mittelbar den Weltfrieden. Damit liegt ein besonders gewichtiges Rechtsgut mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist der unerlaubte Umgang mit Kriegswaffen, d.h. ohne die entsprechende Genehmigung. Kriegswaffen sind solche Waffen, die explizit zur Kriegsführung bestimmt sind (§ 1 Absatz 1 KrWaffKontrG), d.h. ein großes Schadenspotential aufweisen.

Die besondere Schwere der Tat ergibt sich aus der Tatfolge. Durch die Tathandlung wird die Herstellung und Ausbreitung von Kriegswaffen gefördert, womit eine ernsthafte Bedrohung für das o.g. Schutzgut einhergeht.

Zu Nummer 52 (§ 51 Absatz 1 WaffG)

Die Vorschrift des Waffengesetzes schützt die öffentliche Sicherheit und Ordnung und Leib und Leben durch die Begrenzung der Verbreitung und Nutzung von Waffen. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist der Erwerb, Besitz, Überlassung, Führen, Verbringen, Mitnehmen, Herstellen, Bearbeiten, Instandsetzen oder Handel treiben mit verbotenen Schusswaffen zum Verschießen von Patronenmunition. Damit handelt es sich bei den verbotenen Schusswaffen um sog. „scharfe“ Schusswaffen, da nur diese Patronenmunition verschießt (u.a. vollautomatische Schusswaffen und Pumpguns).

Die besondere Schwere der Tat ergibt sich aus der Tatfolge. Durch die Tathandlung wird die Herstellung, Nutzung und Verbreitung von verbotenen scharfen Schusswaffen gefördert, was eine ernsthafte Bedrohung für die o.g. Schutzgüter bedeutet.

Zu Nummer 53 (§ 52 Absatz 1 WaffG)

Die Vorschrift schützt die öffentliche Sicherheit und Ordnung und Leib und Leben durch die Begrenzung der Verbreitung und Nutzung von Waffen. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Tathandlung ist das unerlaubte Ausüben der tatsächlichen Gewalt über Waffen oder Waffenteile bzw. Munition, u.a. ehemalige Kriegswaffen und Molotow-Cocktails.

Die besondere Schwere der Tat ergibt sich aus der Tatfolge. Durch die Tathandlung wird die Herstellung und Verbreitung der o.g. Waffen gefördert, was eine ernsthafte Bedrohung für die o.g. Schutzgüter bedeutet.

Zu Nummer 54 (§ 16 Absatz 1 CWÜAG)

§ 16 Absatz 1 des Ausführungsgesetzes zu dem Übereinkommen vom 13. Januar 1993 über das Verbot der Entwicklung, Herstellung, Lagerung und des Einsatzes chemischer Waffen und über die Vernichtung solcher Waffen (CWÜAG) schützt die Sicherheit der Bundesrepublik und den Völkerfrieden. Damit liegen besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft vor.

§ 16 Absatz 1 CWÜAG beinhaltet Strafvorschriften im Zusammenhang mit der Zuwiderhandlung von u.a. Ausfuhrbeschränkungen, die sich aus den Verpflichtungen des sog. „Che-miewaffenübereinkommens“ ergeben. Die besondere Schwere dieser Straftat ergibt sich aus der Gefahr, welche aus ihrer Verwirklichung entstehen kann. Tatbestandlich ist diese Gefahr – und folglich auch die besondere Schwere eines Verstoßes – darin angelegt, dass der Straftatbestand letztlich einer Verbreitung von chemischen Waffen, welche aufgrund ihrer verheerenden Wirkungen und perfiden Natur völkerrechtlich geächtet sind, entgegenwirkt. Ein Verstoß gegen dieses Verbot ist somit in objektivierter Weise mit einem besonderen Tatunrecht verbunden. Überdies ist ein Verstoß für Beteiligte auch aufgrund des Gepräges der Tatbestandsverwirklichung, welche gerade mit Blick auf die historische Verwendung dieser Waffen betrachtet werden muss, als besonders schwere Straftat zu erkennen. Da ein Vertrieb der entsprechenden Chemikalien nur von spezialisierten Händlern mit hoher chemischer Sachkenntnis in Betracht kommt, ist zudem davon auszugehen, dass diese Kenntnis von der (möglichen) Verwendung in Chemiewaffen haben. Nur vorsätzliche Taten werden von der Übermittlungsbefugnis erfasst, da das besondere

Tatunrecht einer aktiven Mitwirkung an der Verbreitung von Chemiewaffen nur bei vorsätzlicher Begehung anzunehmen ist.

Ein praktisches Beispiel für einen solchen Fall wäre der vorsätzliche Export einer Chemikalie, welche Nordkorea die Produktion von Chemiewaffen ermöglicht. Insbesondere vor dem Hintergrund der nordkoreanischen Unterstützung Russlands in seinem Angriffskrieg gegen die Ukraine kann eine solche CWÜ-widrige Aktivität zu einer erheblichen Gefährdung außen- und sicherheitspolitischer Interessen der Bundesrepublik Deutschland und seiner Verbündeten führen.

Zu Nummer 55 (§ 18 Transplantationsgesetz)

Die Vorschrift aus dem Transplantationsgesetz (TPG) dient dem Schutz von gleich mehreren besonders gewichtigen Rechtsgüter, die körperliche Unversehrtheit, der Schutz von Leib und Leben, das allgemeine Selbstbestimmungsrecht und nicht zuletzt die Menschenwürde (BeckOK StGB/ Heintschel-Heinegg/Kudlich, 67. Ed. 1.11.2025, TPG § 18 Rn. 11 ff.).

Dass eine besonders schwere Straftat vorliegt, ergibt sich aus dem Tatbestand. Die Tatbegehung wird regelmäßig im Kontext des Menschenhandels bzw. der Organisierten Kriminalität verwirklicht. Der Organhandel mit Bezug zum Ausland geht typischerweise mit einer besonderen Gefährdung schutzbedürftiger Personen einher.

Die besondere Schwere der Tat ergibt sich auch aus der Tatfolge. Tatfolge ist, dass Personen in finanziellen Notsituationen zu medizinisch nicht indizierten Eingriffen gezwungen werden und sodann durch das Fehlen einzelner Organe oder Organteile langfristig mit den gesundheitlichen Folgen leben müssen. Aufgrund langer Wartelisten für eine legale Transplantation wird durch die Straftat auch der Menschenhandel nur zu diesem Zwecke begünstigt.