Referentenentwurf

des Bundeskanzleramts

Entwurf eines Gesetzes zur Änderung des BND-Gesetzes

A. Problem und Ziel

Das Bundesverfassungsgericht hat mit Beschluss vom 28. September 2022, 1 BvR 2354/13, die Übermittlungsvorschriften in Staatsschutzangelegenheiten nach den §§ 20, 21 des Bundesverfassungsschutzgesetzes (BVerfSchG) teilweise mit dem Grundgesetz für unvereinbar erklärt und zugleich die mit dem Grundgesetz unvereinbaren Vorschriften bis zu einer Neuregelung, längstens jedoch bis zum 31. Dezember 2023 mit Maßgaben für weiterhin anwendbar erklärt. Da § 11 Absatz 3 des BNDG auf § 20 BVerfSchG verweist, besteht Handlungsbedarf auch für den Bundesnachrichtendienst. Im Zuge dessen sollen auch die anderen Übermittlungsvorschriften des BNDG sowie des Artikel 10-Gesetzes (G10) an die Vorgaben des Bundesverfassungsgerichts angepasst werden.

Aufgrund eines mutmaßlichen Verratsfalls im Jahr 2022 beim Bundesnachrichtendienst wurde der Bedarf an einer Stärkung und Optimierung von Maßnahmen zur Eigensicherung deutlich. Das Parlamentarische Kontrollgremium regt eine Überprüfung an (BT-Drs. 20/6575). Ziel der gesetzlichen Neuregelung ist es, die Verschlusssachen im Bundesnachrichtendienst noch stärker vor den Gefahren fremder Kenntnisnahme zu schützen und Informationsabflüsse aus dem Bundesnachrichtendienst heraus zu verhindern.

B. Lösung

Sämtliche Übermittlungsvorschriften im BNDG werden vom BVerfSchG entkoppelt und unter Berücksichtigung der aktuellen Rechtsprechung des Bundesverfassungsgerichts grundlegend normenklar und transparent gefasst.

Als Maßnahme der Eigensicherung werden zusätzliche Vorschriften zum Schutz von Verschlusssachen durch Kontrollen präzise für den Bundesnachrichtendienst gesetzlich geregelt.

Die neuen Regelungen dienen dazu, die Übermittlung von Informationen verfassungsfest auszugestalten und die Eigensicherung zu festigen.

Auf die Durchführung eines Digitalchecks wurde verzichtet, weil der Bundesnachrichtendienst keine digitalen Verwaltungsleistungen für den Bürger erbringt. Aus Geheimhaltungsgründen sollen die internen Prozesse der Informationsweitergabe zwischen dem Bundesnachrichtendienst und den Abnehmerbehörden nicht dargestellt werden.

C. Alternativen

Keine. Der vom Bundesverfassungsgericht bemängelte verfassungswidrige Zustand bei der Übermittlung in Staatsschutzsachen muss beseitigt werden.

ENTWURF

D. Haushaltsausgaben ohne Erfüllungsaufwand

Der Gesetzentwurf führt beim Bundesnachrichtendienst in Folge der personellen Aufwände zu jährlichen Haushaltsausgaben ohne Erfüllungsaufwand in Höhe von etwa 2,7 Mio. EUR.

Der Mehrbedarf an Sach- und Personalmitteln soll finanziell und planstellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

E.2 Erfüllungsaufwand für die Wirtschaft

Keine.

E.3 Erfüllungsaufwand der Verwaltung

Durch die Durchführung der neuen Kontrollbefugnisse beim Umgang mit Verschlusssachen erhöht sich beim Bundesnachrichtendienst der jährliche Erfüllungsaufwand um 3,9 Mio. EUR. Der einmalige Erfüllungsaufwand beläuft sich auf 10,0 Mio. EUR. Er resultiert aus der Beschaffung von Geräten zur Unterstützung der Kontrollen sowie der punktuellen Anpassung der vorhandenen IT-Systeme.

Der Erfüllungsaufwand soll finanziell und planstellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

Im Bundesnachrichtendienst werden die Anwendung der neuen Übermittlungsbefugnisse und die neuen Regelungen zur Eigensicherung zum Jahresende 2025 intern evaluiert. Der Bundesnachrichtendienst erfasst hierzu die notwendigen Zahlen. Der Bundesnachrichtendienst erhebt die Zahlen und Fallkonstellationen zu den einzelnen Übermittlungsbefugnissen und setzt diese in Relation zu den Fällen, in denen eine Übermittlung unterbleiben musste. Das Ziel der neuen Regelungen zum Schutz von Verschlusssachen ist es, Verratsfälle, wie demjenigen aus 2022 (BT-Drs. 20/5183, S. 2, 20/6070, S. 39), zu unterbinden. Dieses Ziel kann erreicht werden, indem der Umgang mit Verschlusssachen verstärkt kontrolliert und damit ein Informationsabfluss verhindert wird. Der Bundesnachrichtendienst hält die Art, die Anzahl und die Ergebnisse der einzelnen Kontrollen fest und wertet diese in einem Bericht das Parlamentarische Kontrollgremium aus.

Der mögliche zusätzliche Erfüllungsaufwand für das Bundesverwaltungsgericht wegen dessen erstinstanzlicher Zuständigkeit nach § 50 Absatz 1 Nummer 4 VwGO durch Rechtsschutzbegehren in Zusammenhang mit Kontrollen zur Sicherung von Verschlusssachen lässt sich vorab nicht verlässlich spezifizieren. Es ist voraussichtlich mit niedrigen zweistelligen Verfahrensanstrengungen pro Jahr zu rechnen.

ENTWURF

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.

ENTWURF

Referentenentwurf des Bundeskanzleramtes

Entwurf eines Gesetzes zur Änderung des BND-Gesetzes

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des BND-Gesetzes

Das BND-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch Artikel 3 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 2274) geändert worden ist, wird wie folgt geändert:

1. Dem § 1 wird folgende Inhaltsübersicht vorangestellt:

„Inhaltsübersicht

Abschnitt 1 Organisation, Aufgaben und allgemeine Befugnisse

§ 1 Organisation und Aufgaben

§ 2 Befugnisse

§ 3 Besondere Auskunftsverlangen

§ 4 Besondere Auskunftsverlangen zu Bestandsdaten

§ 5 Besondere Formen der Datenerhebung

Abschnitt 2 Weiterverarbeitung von Daten

§ 6 Speicherung, Veränderung und Nutzung personenbezogener Daten

§ 7 Berichtigung, Löschung und Verarbeitungsbeschränkung personenbezogener Daten

§ 8 Dateianordnungen

§ 9 Auskunft an den Betroffenen

Abschnitt 3 Übermittlung von Daten und gemeinsame Dateien

Unterabschnitt 1 Allgemeine Vorschriften bei Übermittlung von personenbezogenen Daten durch den Bundesnachrichtendienst

§ 9a Zweckbindung der Übermittlung personenbezogener Daten

§ 9b Protokollierung der Übermittlung

§ 9c Verbundene personenbezogene Daten

§ 9d Pflicht zur Übermittlung vervollständigter oder berichtigter Daten

ENTWURF

§ 9e Verbot der Übermittlung

§ 9f Schutz von minderjährigen Personen bei Übermittlungen an inländische Stellen

§ 9g Schutz von minderjährigen Personen bei Übermittlungen an ausländische Stellen oder an über- oder zwischenstaatliche Stellen

§ 9h Übermittlung zum Schutz der betroffenen Person

Unterabschnitt 2 Datenübermittlung an den Bundesnachrichtendienst und Übermittlung von personenbezogenen Daten aus allgemein zugänglichen Quellen durch den Bundesnachrichtendienst

§ 10 Übermittlung von personenbezogenen Daten an den Bundesnachrichtendienst

§ 10a Übermittlung von personenbezogenen Daten aus allgemein zugänglichen Quellen

Unterabschnitt 3 Übermittlung von personenbezogenen Daten aus nicht allgemein zugänglichen Quellen an inländische Stellen

§ 11 Übermittlung an inländische Nachrichtendienste

§ 11a Übermittlung an inländische Strafverfolgungsbehörden

§ 11b Übermittlung an inländische öffentliche Stellen

§ 11c Übermittlung an nicht öffentliche inländische Stellen

§ 11d Übermittlung von personenbezogenen Daten aus einer Vertraulichkeitsbeziehung an inländische Stellen

Unterabschnitt 4 Übermittlung von personenbezogenen Daten aus nicht allgemein zugänglichen Quellen an ausländische Stellen sowie an über- oder zwischenstaatliche Stellen

§ 11e Übermittlung an ausländische öffentliche Stellen und an über- oder zwischenstaatliche Stellen

§ 11f Übermittlung an nicht öffentliche ausländische Stellen

§ 11g Übermittlung von personenbezogenen Daten aus einer Vertraulichkeitsbeziehung an ausländische Stellen oder über- oder zwischenstaatliche Stellen

Unterabschnitt 5 Gemeinsame Dateien

§ 12 Projektbezogene gemeinsame Dateien mit inländischen öffentlichen Stellen

§ 13 Gemeinsame Dateien mit ausländischen öffentlichen Stellen

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

§ 15 Dateianordnung bei gemeinsamen Dateien mit ausländischen öffentlichen Stellen

§ 16 Eingabe in und Zugriff auf die vom Bundesnachrichtendienst geführten gemeinsamen Dateien mit ausländischen öffentlichen Stellen

§ 17 Beteiligung an gemeinsamen Dateien mit ausländischen öffentlichen Stellen

§ 18 (weggefallen)

ENTWURF

Abschnitt 4 Technische Aufklärung

Unterabschnitt 1 Verarbeitung von personenbezogenen Daten im Rahmen der strategischen Ausland-Fernmeldeaufklärung

§ 19 Strategische Ausland-Fernmeldeaufklärung

§ 20 Besondere Formen der strategischen Ausland-Fernmeldeaufklärung

§ 21 Schutz von Vertraulichkeitsbeziehungen

§ 22 Kernbereichsschutz

§ 23 Anordnung

§ 24 Eignungsprüfung

§ 25 Pflichten der Anbieter von Telekommunikationsdiensten, Entschädigung

§ 26 Verarbeitung von personenbezogenen Verkehrsdaten

§ 27 Auswertung der Daten und Prüfpflichten

§ 28 Datenerhebung durch eine ausländische öffentliche Stelle

Unterabschnitt 2 (weggefallen)

§ 29 (weggefallen)

§ 30 (weggefallen)

Unterabschnitt 3 Kooperationen im Rahmen der strategischen Ausland-Fernmeldeaufklärung

§ 31 Kooperationen mit ausländischen öffentlichen Stellen

§ 32 Verarbeitung von selektierten personenbezogenen Daten im Rahmen von Kooperationen

§ 33 Verarbeitung von unselektierten personenbezogenen Verkehrsdaten im Rahmen von Kooperationen

Unterabschnitt 4 Besondere Formen der technischen Aufklärung

§ 34 Eingriff in informationstechnische Systeme von Ausländern im Ausland

§ 35 Schutz von Vertraulichkeitsbeziehungen

§ 36 Kernbereichsschutz

§ 37 Anordnung

§ 38 (weggefallen)

§ 39 (weggefallen)

Unterabschnitt 5 Unabhängige Rechtskontrolle

§ 40 Ausübung der unabhängigen Rechtskontrolle

§ 41 Unabhängiger Kontrollrat

§ 42 Zuständigkeit des gerichtsähnlichen Kontrollorgans; Vorlagepflicht des Bundesnachrichtendienstes

ENTWURF

§ 43 Besetzung des gerichtsähnlichen Kontrollorgans; Wahl der Mitglieder; Wahl der Präsidentin oder des Präsidenten und der Vizepräsidentin oder des Vizepräsidenten des Unabhängigen Kontrollrates

§ 44 Rechtstellung und Ernennung der Mitglieder des gerichtsähnlichen Kontrollorgans

§ 45 Amtszeit der Mitglieder des gerichtsähnlichen Kontrollorgans; Ruhestand

§ 46 Besoldung der Mitglieder des gerichtsähnlichen Kontrollorgans

§ 47 Weitere Rechte und Pflichten der Mitglieder des gerichtsähnlichen Kontrollorgans

§ 48 Amtsbezeichnungen

§ 49 Spruchkörper des gerichtsähnlichen Kontrollorgans; Beschlussfassung

§ 50 Leitung des administrativen Kontrollorgans

§ 51 Zuständigkeit des administrativen Kontrollorgans

§ 52 Beanstandungen

§ 53 Mitarbeiterinnen und Mitarbeiter des Unabhängigen Kontrollrates

§ 54 Geheimhaltung; Aussagegenehmigung

§ 55 Bericht des Unabhängigen Kontrollrates an das Parlamentarische Kontrollgremium

§ 56 Pflicht des Bundesnachrichtendienstes zur Unterstützung

§ 57 Personal- und Sachausstattung; Personalverwaltung

§ 58 Austausch zwischen dem Parlamentarischen Kontrollgremium und dem Unabhängigen Kontrollrat; Zusammenarbeit zwischen dem Unabhängigen Kontrollrat, der G10-Kommission und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Unterabschnitt 6 Mitteilungen und Evaluierung

§ 59 Mitteilung an Betroffene und Benachrichtigungspflichten

§ 60 Mitteilungsverbote

§ 61 Evaluierung

§ 62 Dienstvorschriften

Abschnitt 5 Gemeinsame Bestimmungen

§ 63 Unabhängige Datenschutzkontrolle

§ 64 Anwendung des Bundesdatenschutzgesetzes

§ 65 Politische Unterrichtung und Information der Öffentlichkeit

Abschnitt 6 Sicherung von Verschlusssachen im Bundesnachrichtendienst

Unterabschnitt 1 Befugnisse, Durchführung und Anordnung

§ 65a Maßnahmen zur Sicherung von Verschlusssachen

§ 65b Kontrolle und Durchsuchung von Personen, Taschen und Fahrzeugen zur Sicherung von Verschlusssachen

§ 65c Kontrolle und Durchsuchung von Räumen zur Sicherung von Verschlusssachen

ENTWURF

§ 65d IT-Kontrollen zur Sicherung von Verschlusssachen

§ 65e Anordnung von Maßnahmen zur Sicherung von Verschlusssachen

§ 65f Durchführung von Maßnahmen zur Sicherung von Verschlusssachen

Unterabschnitt 2 Verarbeitung und Übermittlung von personenbezogenen Daten aus Maßnahmen zur Sicherung von Verschlusssachen

§ 65g Kennzeichnung, Speicherung, Löschung und Zweckbindung

§ 65h Schutz des Kernbereichs privater Lebensgestaltung

§ 65i Personenbezogene Daten aus Vertraulichkeitsbeziehungen

§ 65j Schutz von minderjährigen Personen

§ 65k Protokollierung

§ 65l Übermittlung von personenbezogenen Daten aus Maßnahmen zur Sicherung von Verschlusssachen

Abschnitt 7 Straf- und Bußgeldvorschriften

§ 66 Strafvorschriften

§ 67 Bußgeldvorschriften

Abschnitt 8 Schlussvorschriften

§ 66 Einschränkung von Grundrechten

§ 69 Übergangsvorschriften“.

2. In § 1 Absatz 2 Satz 2 wird die Angabe „39“ durch „37“ ersetzt.

3. § 2 Absatz 1a wird wie folgt gefasst:

   „(1a) Der Bundesnachrichtendienst darf zum Schutz seiner Mitarbeiterinnen und Mitarbeiter, seiner Einrichtungen und seiner Quellen Legenden einsetzen sowie die hierfür erforderlichen Tarnmittel herstellen und nutzen.“

4. § 6 Absatz 2 wird wie folgt gefasst:

   „(2) Die Speicherung, Veränderung und Nutzung personenbezogener Daten einer minderjährigen Person ist nur unter den Voraussetzungen des § 11 des Bundesverfassungsschutzgesetzes sowie nur dann zulässig, wenn nach den Umständen des Einzelfalls nicht ausgeschlossen werden kann, dass von der minderjährigen Person eine Gefahr ausgeht

   1. für Leib oder Leben einer Person,

   2. für deutsche Einrichtungen oder

   3. Einrichtungen der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages.

   Die Speicherung, Veränderung und Nutzung personenbezogener Daten einer minderjährigen Person ist ferner zulässig, wenn dies zu deren Schutz erforderlich ist.“

ENTWURF

5. In § 9 Absatz 2 werden die Wörter „Bundesministerium des Innern, für Bau und für Heimat“ durch die Wörter „Bundesministerium des Innern und für Heimat“ ersetzt.

6. Nach der Überschrift von Abschnitt 3 wird folgender Unterabschnitt 1 eingefügt:

„Unterabschnitt 1

Allgemeine Vorschriften bei Übermittlung von personenbezogenen Daten durch den Bundesnachrichtendienst

§ 9a

Zweckbindung der Übermittlung personenbezogener Daten

(1) Die empfangende Stelle darf personenbezogene Daten nur zu den Zwecken verarbeiten, zu denen sie ihr vom Bundesnachrichtendienst übermittelt worden sind. Eine Weiterverarbeitung zu anderen Zwecken durch die empfangende Stelle ist unzulässig, es sei denn, der Bundesnachrichtendienst stimmt der Weiterverarbeitung zu. Der Bundesnachrichtendienst darf einer über Satz 1 hinausgehenden Weiterverarbeitung nur zustimmen, wenn er die personenbezogenen Daten der empfangenden Stelle auch zu dem anderen Zweck hätte übermitteln dürfen.

(2) Die empfangende Stelle der personenbezogenen Daten ist verpflichtet, dem Bundesnachrichtendienst auf Verlangen Auskunft über die Weiterverarbeitung zu erteilen.

(3) Der Bundesnachrichtendienst hat die empfangende Stelle bei der Übermittlung von personenbezogenen Daten darauf hinzuweisen,

1. zu welchen Zwecken sie die Daten verarbeiten darf und

2. dass sie ihm 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 den Absatz 1 und°3 hinaus, dass

1. die ausländische Stelle oder die über- oder zwischenstaatliche Stelle entsprechend Absatz 2 zur Auskunft verpflichtet werden 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.

ENTWURF

§ 9b

Protokollierung der Übermittlung

(1) 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.

(2) Die Protokolldaten sind bis zum Ablauf des zweiten Kalenderjahres, das auf das Kalenderjahr der Protokollierung folgt, aufzubewahren. Nach Ablauf der Aufbewahrungsfrist sind die Protokolldaten unverzüglich zu löschen.

(3) Die Löschung der Protokolldaten kann unterbleiben, wenn die Trennung von anderen Informationen, die zur Erfüllung der Aufgaben des Bundesnachrichtendienstes erforderlich sind, nicht oder nur mit übermäßigem Aufwand möglich ist.

§ 9c

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 nicht möglich 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.

(2) Die weiteren personenbezogenen Daten der betroffenen oder der dritten Person sind kenntlich zu machen. Die datenempfangende Stelle darf die übermittelten weiteren personenbezogenen Daten nicht weiterverarbeiten.

§ 9d

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 dies für die Beurteilung eines Sachverhalts offensichtlich ohne Bedeutung ist.

ENTWURF

§ 9e

Verbot der Übermittlung

(1) Der Bundesnachrichtendienst darf keine personenbezogenen Daten 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.

Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(2) Eine Übermittlung ist trotz entgegenstehender überwiegender Sicherheitsinteressen nach Absatz 1 Nummer 2 geboten, wenn dies zur Abwehr einer dringenden Gefahr für Leib oder Leben einer Person erforderlich ist. Satz 1 gilt nicht, wenn durch die Übermittlung eine erhebliche Gefahr für Leib oder Leben einer anderen Person zu besorgen ist und dieses Schutzinteresse überwiegt. In den Fällen des Satz 2 wird das Parlamentarische Kontrollgremium unterrichtet.

(3) 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,

   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.

(4) 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.

§ 9f

Schutz von minderjährigen Personen bei Übermittlungen an inländische Stellen

(1) Personenbezogene Daten einer Person, die noch nicht 14 Jahre alt ist, darf der Bundesnachrichtendienst an inländische Stellen vorbehaltlich Absatz 2 nicht übermitteln.

(2) Eine Übermittlung von personenbezogenen Daten einer Person, die noch nicht 14 Jahre alt ist, darf an inländische Stellen erfolgen, wenn nach den Umständen des Einzelfalls aufgrund tatsächlicher Anhaltspunkte nicht ausgeschlossen werden kann, dass von der Person eine konkretisierte Gefahr ausgeht

1. für Leib oder Leben einer Person oder

2. für die Sicherheit deutscher Einrichtungen oder Einrichtungen der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages.

§ 9g

Schutz von minderjährigen Personen bei Übermittlungen an ausländische Stellen und an über- oder zwischenstaatliche Stellen

(1) Personenbezogene Daten einer Person, die noch nicht 16 Jahre alt ist, darf der Bundesnachrichtendienst vorbehaltlich von Absatz 2 weder an eine ausländische Stelle noch an eine über- oder zwischenstaatliche Stelle übermitteln.

(2) Eine Übermittlung von personenbezogenen Daten einer Person, die noch nicht 16 Jahre, aber mindestens 14 Jahre alt ist, darf an eine ausländische Stelle oder an eine über- oder zwischenstaatliche Stelle erfolgen, wenn nach den Umständen des Einzelfalls aufgrund tatsächlicher Anhaltspunkte nicht ausgeschlossen werden kann, dass die Übermittlung erforderlich ist zur Abwehr einer konkretisierten Gefahr

1. für Leib oder Leben einer Person oder

2. für die Sicherheit deutscher Einrichtungen oder Einrichtungen der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages.

§ 9h

Übermittlung zum Schutz der betroffenen Person

(1) Der Bundesnachrichtendienst darf zum Schutz der betroffenen Person mit deren Einwilligung ihre personenbezogenen Daten übermitteln. Kann die Einwilligung nicht oder nicht rechtzeitig eingeholt werden, darf der Bundesnachrichtendienst personenbezogene Daten auch übermitteln, wenn

1. die Übermittlung offensichtlich im Interesse der betroffenen Person liegt, und

ENTWURF

2. kein Grund zu der Annahme besteht, dass sie ihre Einwilligung zu der Übermittlung verweigern würde, wenn sie Kenntnis von dieser hätte.

(2) Eine Übermittlung personenbezogener Daten minderjähriger Personen ist über Absatz 1 hinaus auch zulässig, wenn dies zum Schutz der minderjährigen Person erforderlich ist.“

7. Vor § 10 wird folgende Überschrift eingefügt:

„Unterabschnitt 2

Datenübermittlung an den Bundenachrichtendienst und Übermittlung von personenbezogenen Daten aus allgemein zugänglichen Quellen durch den Bundesnachrichtendienst“.

8. Nach § 10 wird folgender § 10a eingefügt:

„§ 10a

Übermittlung von personenbezogenen Daten aus allgemein zugänglichen Quellen

(1) Der Bundesnachrichtendienst darf personenbezogene Daten, die er aus allgemein zugänglichen Quellen erhoben hat, einer anderen Stelle übermitteln, wenn dies erforderlich ist

1. zur Erfüllung seiner Aufgaben oder

2. der Aufgaben der empfangenden Stelle.

Eine automatisierte Übermittlung ist zulässig.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die aus allgemein zugänglichen Quellen systematisch erhoben oder zusammengeführt wurden. Die Übermittlung richtet sich in diesen Fällen nach den Unterabschnitten 3 und 4.“

9. Nach § 10a wird folgende Überschrift eingefügt:

„Unterabschnitt 3

Übermittlung von personenbezogenen Daten aus nicht allgemein zugänglichen Quellen an inländische Stellen“.

10. § 11 wird wie folgt gefasst:

„§ 11

Übermittlung an inländische Nachrichtendienste

Der Bundesnachrichtendienst darf personenbezogene Daten an das Bundesamt für Verfassungsschutz, an die Verfassungsschutzbehörden der Länder und an das

ENTWURF

Bundesamt für den Militärischen Abschirmdienst übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung erforderlich ist

1. zur Erfüllung seiner Aufgaben oder

2. zur Erfüllung der Aufgaben der empfangenden Stelle.“

11. Nach § 11 werden die folgenden §§ 11a bis 11g eingefügt:

„§ 11a

Übermittlung an inländische Strafverfolgungsbehörden

(1) Der Bundesnachrichtendienst darf personenbezogene Daten an inländische Strafverfolgungsbehörden übermitteln, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung erforderlich ist zur Verfolgung von besonders schweren Straftaten, für die bestimmte, den Verdacht begründende Tatsachen vorliegen. Besondere schwere Straftaten im Sinne des Satz 1 sind Straftaten, die im Höchstmaß mit Freiheitsstrafe bedroht sind von

1. mindestens zehn Jahren oder

2. fünf Jahren und mit den Aufgaben des Bundesnachrichtendienstes gemäß § 1 Absatz 2 im Zusammenhang stehen, aus dem

   a) Strafgesetzbuch

      aa) § 80a (Aufstacheln zum Verbrechen der Aggression), § 83 Absatz 2 (Vorbereitung eines hochverräterischen Unternehmens), § 84 (Fortführung einer für verfassungswidrig erklärten Partei), § 85 Absatz 1 (Verstoß gegen ein Vereinigungsverbot), § 87 (Agententätigkeit zu Sabotagezwecken), § 88 (Verfassungsfeindliche Sabotage), § 89 Absatz 1 (Verfassungsfeindliche Einwirkung auf Bundeswehr und öffentliche Sicherheitsorgane), § 95 (Offenbaren von Staatsgeheimnissen), § 96 Absatz 2 StGB (Auskundschaften von Staatsgeheimnissen), § 97 Absatz 1 (Preisgabe von Staatsgeheimnissen), § 98 (Landesverräterische Agententätigkeit), § 99 (Geheimdienstliche Agententätigkeit), § 100a (Landesverräterische Fälschung),

      bb) § 102 StGB (Angriff gegen Organe und Vertreter ausländischer Staaten), § 106 (Nötigung des Bundespräsidenten und von Mitgliedern eines Verfassungsorgans), § 107 (Wahlbehinderung), § 107a StGB (Wahlfälschung), § 108 (Wählernötigung), § 108b (Wählerbestechung), § 108e StGB (Bestechlichkeit und Bestechung von Mandatsträgern),

      cc) §°109d (Störpropaganda gegen die Bundeswehr), §°109e (Sabotagehandlungen an Verteidigungsmitteln), §°109f StGB (Sicherheitsgefährdender Nachrichtendienst), §°109g Absatz°1 StGB (Sicherheitsgefährdendes Abbilden),

      dd) §°125a (Besonders schwerer Fall des Landfriedensbruchs), §°127 (Betreiben krimineller Handelsplattformen im Internet), § 129 Absatz 1 Satz 1 und Absatz 5 (Bildung krimineller Vereinigungen) und § 129a (Bildung terroristischer Vereinigungen), jeweils auch in Verbindung mit § 129b, sowie § 130 Absatz 1 und 3 (Volksverhetzung), § 138 (Nichtanzeige geplanter Straftaten),

ENTWURF

ee) § 180 Absatz 2 (Förderung sexueller Handlungen Minderjähriger), § 181a Absatz 1 (Zuhälterei) und § 182 Absatz 1 und 2 (Sexueller Missbrauch von Jugendlichen),

ff) Sechszehnter Abschnitt (Straftaten gegen das Leben)

gg) Siebzehnter Abschnitt (Straftaten gegen die körperliche Unversehrtheit),

hh) Achtzehnter Abschnitt (Straftaten gegen die persönliche Freiheit),

ii) § 253 (Erpressung), § 261 Absatz 1, 2 und°4 (Geldwäsche),

jj) § 275 Absatz 2 (Vorbereitung der Fälschung von amtlichen Ausweisen) und § 276 Absatz 2 (Verschaffen von falschen amtlichen Ausweisen), jeweils auch in Verbindung mit § 276a,

kk) § 303b Absatz 2 und 3 (Computersabotage), § 305a (Zerstörung wichtiger Arbeitsmittel),

ll) Achtundzwanzigster Abschnitt (Gemeingefährliche Straftaten),

mm) Neunundzwanzigster Abschnitt (Straftaten gegen die Umwelt),

nn) Dreißigster Abschnitt (Straftaten im Amt),

b) Außenwirtschaftsgesetz: § 18 Absatz 1 bis 5, auch in Verbindung mit Absatz 9,

c) Gesetz über die Kontrolle von Kriegswaffen § 19 Absatz 1, § 20a Absatz 1, auch in Verbindung mit §°21, und § 22 Absatz 1,

d) Ausführungsgesetz 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 § 16 Absatz 1,

e) Aufenthaltsgesetz: § 96 Absatz 1 (Einschleusen von Ausländern),

f) Waffengesetz: § 51 Absatz 1 und § 52 Absatz 1, oder

g) § 23 Absatz 4 des Geschäftsgeheimnisgesetzes.

(2) Der Bundesnachrichtendienst darf personenbezogene Daten, die nach § 2 Absatz 1 Satz 1 Nummer 1 erhoben wurden, über Absatz 1 hinaus an inländische Strafverfolgungsbehörden übermitteln, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung erforderlich ist zur Verfolgung von Straftaten, für die bestimmte, den Verdacht begründende Tatsachen vorliegen, nach dem Strafgesetzbuch:

1. §°86 (Verbreiten von Propagandamitteln verfassungswidriger und terroristischer Organisationen), §°86a (Verwenden von Kennzeichen verfassungswidriger und terroristischer Organisationen), §°91 (Anleitung zur Begehung einer schweren staatsgefährdenden Gewalttat),

2. §°97 Absatz°2 (Preisgabe von Staatsgeheimnissen),

3. §°109g Absatz°2 (Sicherheitsgefährdendes Abbilden),

ENTWURF

4. §°126a (Gefährdendes Verbreiten personenbezogener Daten), §°133 (Verwahrungsbruch),

5. §°202a (Ausspähen von Daten), §°202b (Abfangen von Daten), §°202c (Vorbereiten des Ausspähens und Abfangens von Daten),

6. §°303a (Datenveränderung) und §°303b Absatz°1 (Computersabotage) oder

7. §°353b (Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht).

(3) Der Bundesnachrichtendienst übermittelt personenbezogene Daten an inländische Strafverfolgungsbehörden, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung erforderlich ist zur Verfolgung von besonders schweren Straftaten, für die bestimmte, den Verdacht begründende Tatsachen vorliegen, nach

1. §°80a (Aufstacheln zum Verbrechen der Aggression), §°81 (Hochverrat gegen den Bund), §°82 (Hochverrat gegen ein Land), §°83 Absatz 1 (Vorbereitung eines hochverräterischen Unternehmens),

2. §°87 (Agententätigkeit zu Sabotagezwecken), §°88 (Verfassungsfeindliche Sabotage), §°89 Absatz°1 (Verfassungsfeindliche Einwirkung auf Bundeswehr und öffentliche Sicherheitsorgane), §°94 (Landesverrat) §°95 (Offenbaren von Staatsgeheimnissen), §°96 StGB (Auskundschaften von Staatsgeheimnissen), §°97a (Verrat illegaler Geheimnisse), §°97b (Verrat in irriger Annahme eines illegalen Geheimnisses), §°98 (Landesverräterische Agententätigkeit), §°99 (Geheimdienstliche Agententätigkeit), §°100 (Friedensgefährdende Beziehungen), §°100a (Landesverräterische Fälschung), jeweils auch in Verbindung mit §°1 des NATO-Truppen-Schutzgesetzes,

3. §°109e (Sabotagehandlungen an Verteidigungsmitteln), §°109f StGB (Sicherheitsgefährdender Nachrichtendienst), §°109g Absatz°1 StGB (Sicherheitsgefährdendes Abbilden), jeweils auch in Verbindung mit §°1 des NATO-Truppen-Schutzgesetzes,

4. §°129a (Bildung terroristischer Vereinigungen), auch in Verbindung mit §°129b, §°130 Absatz°1 und°3 (Volksverhetzung), §°211 (Mord), §°212 (Totschlag), §°239a (Erpresserischer Menschenraub), §°239b (Geiselnahme), §°306 (Brandstiftung), §°306a (Schwere Brandstiftung), §°306b (Besonders schwere Brandstiftung , §°306c (Brandstiftung mit Todesfolge), §°307 Absatz°1 bis°3 (Herbeiführen einer Explosion durch Kernenergie), §°308 Absatz°1 bis°3 (Herbeiführen einer Sprengstoffexplosion), §°315 Absatz°3 (Gefährliche Eingriffe in den Bahn-, Schiffs- und Luftverkehr), §°316b Absatz°3 (Störung öffentlicher Betriebe) und §°316c Absatz°1 und°3 (Angriffe auf den Luft- und Seeverkehr), soweit diese sich gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes richten, oder

5. §°303b Absatz°2 und°4 (Computersabotage), soweit sich diese gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland, insbesondere gegen sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen richten.

(4) Absatz 1 bis 3 findet keine Anwendung für die mit dem Zweck der politischen Unterrichtung gekennzeichneten personenbezogenen Daten, die durch Maßnahmen nach den §§ 19 und 34 erhoben wurden.

ENTWURF

§ 11b

Übermittlung an inländische öffentliche Stellen

(1) Der Bundesnachrichtendienst darf personenbezogene Daten an die nicht in den §§ 11 und 11a genannten inländischen öffentlichen Stellen übermitteln, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung dem Schutz eines besonders gewichtigen Rechtsguts dient, für das bereits im Einzelfall eine hinreichend konkretisierte Gefahr besteht oder für das eine Gefahr in absehbarer Zeit in bestimmter Art zu entstehen droht. Besonders gewichtige Rechtsgüter im Sinne von Satz 1 sind

1. Leib, Leben oder Freiheit einer Person,

2. der Bestand oder die Sicherheit des Bundes oder eines Landes,

3. der Bestand oder die Sicherheit der Europäischen Union, eines Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder eines ihrer Mitgliedstaaten oder des Nordatlantikvertrages oder eines seiner Mitgliedstaaten,

4. die freiheitliche demokratische Grundordnung,

5. die Funktionsfähigkeit und Sicherheit der Bundeswehr sowie verbündeter Streitkräfte im Rahmen der Erfüllung der ihnen obliegenden Aufgaben,

6. die Sicherheit und Arbeitsfähigkeit

   a) staatlicher Einrichtungen sowie

   b) wesentlicher Infrastruktureinrichtungen oder Anlagen

   mit unmittelbarer Bedeutung für das Gemeinwesen in der Bundesrepublik Deutschland oder in Mitgliedstaaten der Europäischen Union sowie Einrichtungen der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages,

7. die Handlungsfähigkeit der Bundesrepublik Deutschland und der Europäischen Union auf dem Gebiet des Grenzschutzes sowie des Aufenthalts- und Staatsangehörigenrechts,

8. die Sicherheit von informationstechnischen Systemen in Fällen von herausgehobener Bedeutung für die Allgemeinheit,

9. die wesentliche Funktionsfähigkeit des inländischen und europäischen Wirtschafts- und Wissenschaftsstandorts,

10. die außenpolitische Handlungsfähigkeit der Bundesrepublik Deutschland,

11. der Schutz von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist.

Soweit die Übermittlung personenbezogener Daten durch den Bundesnachrichtendienst an inländische öffentliche Stellen in anderen Rechtsvorschriften vorgesehen ist, bleiben diese unberührt.

(2) Abweichend von Absatz 1 ist eine Übermittlung an die in Absatz 1 Satz 1 genannten inländischen öffentlichen Stellen auch zulässig, wenn die Übermittlung dem

ENTWURF

Schutz eines besonders gewichtigen Rechtsguts nach Absatz 1 Satz 2 dient und tatsächliche Anhaltspunkte vorliegen, dass die Übermittlung erforderlich ist,

1. um der empfangenden öffentlichen Stelle Hintergrundinformationen zu Themen und Staaten in ihrem Zuständigkeitsbereich zur Erstellung eines eigenen Lagebildes bereitzustellen,

2. zur Verhinderung von strategischer Einflussnahme und Ausspähung durch fremde Mächte,

3. zur Aufklärung von Teilnehmerinnen und Teilnehmern am Außenwirtschaftsverkehr über Umstände, die für die Einhaltung von Beschränkungen des Außenwirtschaftsverkehrs von Bedeutung sind,

4. zur Minderung der Verwundbarkeit und Stärkung des Schutzes der Sicherheit von informationstechnischen Systemen vor internationalen kriminellen, terroristischen oder staatlichen Angriffen,

5. zur Vorbereitung und Durchführung eigener Maßnahmen des Bundesnachrichtendienstes,

6. zur Vorbereitung und Durchführung der Landes- und Bündnisverteidigung sowie von Auslandseinsätzen der Bundeswehr oder

7. um auf vergleichbare Weise Gefährdungen der in § 19 Absatz 4 genannten Gefahrenbereiche entgegenzuwirken, insbesondere soweit es hierzu erforderlich ist, personenbezogene Daten von Personen zu übermitteln, die an derartigen Gefährdungen beteiligt sind.

Die nach Satz 1 übermittelten personenbezogenen Daten dürfen nicht zur operativen Anwendung unmittelbaren Zwangs genutzt werden.

(3) Der Bundesnachrichtendienst darf die mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten, die durch Maßnahmen nach den §§ 19 und 34 erhoben wurden, auch automatisiert an die Bundeswehr übermitteln, sofern diese

1. im Rahmen von Maßnahmen nach § 19 auf Grundlage von Suchbegriffen erhoben wurden, die strategischen Aufklärungsmaßnahmen nach § 19 Absatz 4 Nummer 1 Buchstabe a, b, f, g, h oder Buchstabe e in der Ausprägung der Piraterie sowie Nummer 2 Buchstabe a, b oder c zugeordnet sind, oder

2. im Rahmen von individuellen Aufklärungsmaßnahmen nach § 34 Absatz 1 mit Bezug zu den in § 19 Absatz 4 Nummer 1 Buchstabe a, b, f, g, h oder Buchstabe e in der Ausprägung der Piraterie sowie Nummer 2 Buchstabe a, b oder c genannten Gefahren erhoben wurden.

(4) Der Bundesnachrichtendienst darf die mit dem Zweck der politischen Unterrichtung gekennzeichneten personenbezogenen Daten, die durch Maßnahmen nach den §§ 19 und 34 erhoben wurden, an die in Absatz 1 Satz 1 genannten inländischen öffentlichen Stellen nur übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass eine Übermittlung erforderlich ist zur Abwendung einer unmittelbar bevorstehenden Gefahr für

1. Leib, Leben oder Freiheit einer Person,

2. lebenswichtige Güter der Allgemeinheit oder

ENTWURF

3. den Bestand oder die Sicherheit des Bundes oder eines Landes oder für die Sicherheit eines Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages.

(5) Der Bundesnachrichtendienst übermittelt personenbezogene Daten an die in Absatz 1 Satz 1 genannten inländischen öffentlichen Stellen, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung zur Abwehr einer unmittelbar bevorstehenden Gefahr für ein besonders gewichtiges Rechtsgut nach Absatz 1 Satz 2 erforderlich ist. Satz 1 findet keine Anwendung für mit dem Zweck der politischen Unterrichtung gekennzeichnete personenbezogene Daten, die durch Maßnahmen nach den §§ 19 und 34 erhoben wurden.

§ 11c

Übermittlung an nicht öffentliche inländische Stellen

(1) Der Bundesnachrichtendienst darf personenbezogene Daten an nicht öffentliche inländische Stellen übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung erforderlich ist

1. zur Abwendung einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person oder für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,

2. zur Gewährleistung der Sicherheit von lebenswichtigen Gütern der Allgemeinheit,

3. zum 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,

4. zum Schutz der freiheitlich demokratischen Grundordnung oder

5. zur Minderung der Verwundbarkeit und Stärkung des Schutzes der Sicherheit von informationstechnischen Systemen vor internationalen kriminellen, terroristischen oder staatlichen Angriffen.

(2) Übermittlungen nach Absatz 1 bedürfen der vorherigen Zustimmung durch die Behördenleitung des Bundesnachrichtendienstes oder ihre Vertretung. Bei Gefahr im Verzug darf die Übermittlung ohne vorherige Zustimmung erfolgen. Die Zustimmung ist unverzüglich nachzuholen. Wird die Zustimmung nicht erteilt, ist die empfangende Stelle verpflichtet, die übermittelten Daten nach Aufforderung des Bundesnachrichtendienstes unverzüglich zu löschen. Der Bundesnachrichtendienst unterrichtet das Bundeskanzleramt in regelmäßigen Abständen über Übermittlungen nach Absatz 1.

(3) Der Bundesnachrichtendienst darf die mit dem Zweck der politischen Unterrichtung gekennzeichneten personenbezogenen Daten, die durch Maßnahmen nach den §§ 19 und 34 erhoben wurden, an nicht öffentliche inländische Stellen nur übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass eine Übermittlung erforderlich ist zur Abwendung einer unmittelbar bevorstehenden Gefahr für

1. Leib, Leben oder Freiheit einer Person, oder

2. lebenswichtige Güter der Allgemeinheit.

ENTWURF

(4) Der Bundesnachrichtendienst darf personenbezogene Daten an nicht öffentliche inländische Stellen auch ohne Vorliegen der Voraussetzungen des Absatzes 1 oder 3 übermitteln, wenn die Daten

1. dieser nicht öffentlichen inländischen Stelle lediglich zur Konkretisierung einer Anfrage des Bundesnachrichtendienstes übermittelt werden und

2. dieser nicht öffentlichen inländischen Stelle bereits bekannt sind.

§ 11d

Übermittlung von personenbezogenen Daten aus einer Vertraulichkeitsbeziehung an inländische Stellen

(1) Eine Übermittlung von personenbezogenen Daten aus einer Vertraulichkeitsbeziehung im Sinne des § 21 Absatz 1 Satz 2, die durch Maßnahmen nach den §§ 19 und 34 erhoben wurden, ist unzulässig. Abweichend von Satz 1 ist eine Übermittlung nach den §§ 11 bis 11c zulässig,

1. wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass die in § 21 Absatz 1 Satz 2 aufgeführte Person Täterin oder Täter, Teilnehmerin oder Teilnehmer einer der in § 11a Absatz 1 genannten Straftaten ist oder

2. dies erforderlich ist zur Abwendung einer konkretisierten Gefahr für

   a) Leib, Leben oder Freiheit einer Person,

   b) lebenswichtige Güter der Allgemeinheit oder

   c) den Bestand oder die Sicherheit des Bundes oder eines Landes oder die Sicherheit eines Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages.

(2) Der Unabhängige Kontrollrat prüft das Vorliegen der Voraussetzungen einer Übermittlung nach Absatz 1 vor deren Vollzug. Bestätigt der Unabhängige Kontrollrat die Rechtmäßigkeit der Übermittlung nicht, hat die Übermittlung zu unterbleiben.

(3) Bei Gefahr im Verzug erfolgt eine vorläufige Prüfung der Rechtmäßigkeit durch ein Mitglied des gerichtsähnlichen Kontrollorgans des Unabhängigen Kontrollrates, wenn andernfalls der Übermittlungszweck vereitelt oder wesentlich erschwert würde. Wird im Rahmen der vorläufigen Prüfung festgestellt, dass die Übermittlung rechtmäßig ist, darf diese vollzogen werden. In diesem Fall ist die Prüfung durch den Unabhängigen Kontrollrat unverzüglich nachzuholen. Hebt der Unabhängige Kontrollrat die Entscheidung nach Satz 2 auf, wird die empfangende Stelle zur unverzüglichen Löschung der Daten aufgefordert.

ENTWURF

Unterabschnitt 4

Übermittlung von personenbezogenen Daten aus nicht allgemein zugänglichen Quellen an ausländische Stellen sowie an über- oder zwischenstaatliche Stellen

§ 11e

Übermittlung an ausländische öffentliche Stellen und an über- oder zwischenstaatliche Stellen

(1) Der Bundesnachrichtendienst darf personenbezogene Daten an ausländische öffentliche Stellen sowie an über- oder zwischenstaatliche Stellen übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass dies erforderlich ist zur Aufklärung von Straftaten durch die empfangende Stelle, für die bestimmte, den Verdacht begründende Tatsachen vorliegen und die den in § 11b Absatz 1 und 2 genannten Straftaten in Art und Schwere vergleichbar 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 im Sinne von § 11c Absatz 1 Satz 2 oder

2. der Sicherheit des Empfängerstaates

dient und eine hinreichend konkretisierte Gefahr für dieses Rechtsgut oder die Sicherheit des Empfängerstaates besteht.

(3) Eine Übermittlung an ausländische Stellen nach Absatz 1 ist ferner zulässig, wenn dies dem Schutz eines Rechtsguts nach Absatz 2 Nummer 1 oder der Sicherheit des Empfängerstaats dient und

1. eine Weiterverarbeitung für Folgemaßnahmen mit unmittelbarer Außenwirkung zulasten der betroffenen Person oder Dritter ausgeschlossen ist, oder

2. der Vorbereitung und Durchführung eigener Maßnahmen des Bundesnachrichtendienstes dient.

Zum Ausschluss der Weiterverarbeitung für Folgemaßnahmen mit unmittelbarer Außenwirkung nach Nummer 1 kann der Bundesnachrichtendienst eine Zusicherung der empfangenden Stelle einholen. § 9a Absatz 4 Satz 2 gilt entsprechend.

(4) Der Bundesnachrichtendienst darf die mit dem Zweck der politischen Unterrichtung gekennzeichneten personenbezogenen Daten, die durch Maßnahmen nach den §§ 19 und 34 erhoben wurden, an ausländische öffentliche sowie über- oder zwischenstaatliche Stellen nur übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass eine Übermittlung erforderlich ist zur Abwendung einer unmittelbar bevorstehenden Gefahr für

1. Leib, Leben oder Freiheit einer Person,

ENTWURF

2. lebenswichtige Güter der Allgemeinheit oder

3. den Bestand oder die Sicherheit des Bundes oder eines Landes oder für die Sicherheit eines Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages.

§ 11f

Übermittlung an nicht öffentliche ausländische Stellen

(1) Eine Übermittlung personenbezogener Daten an nicht öffentliche ausländische Stellen ist unzulässig, es sei denn es bestehen tatsächliche Anhaltspunkte, dass eine Übermittlung erforderlich ist zur Abwendung einer unmittelbar bevorstehenden Gefahr für

1. Leib, Leben oder Freiheit einer Person,

2. lebenswichtige Güter der Allgemeinheit,

3. den Bestand oder die Sicherheit des Bundes oder eines Landes oder für die Sicherheit eines Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages oder

4. die Sicherheit von informationstechnischen Systemen vor internationalen kriminellen, terroristischen oder staatlichen Angriffen.

(2) Übermittlungen nach Absatz 1 bedürfen der vorherigen Zustimmung durch die Behördenleitung des Bundesnachrichtendienstes oder ihre Vertretung. Bei Gefahr im Verzug darf die Übermittlung ohne vorherige Zustimmung erfolgen. Die Zustimmung ist unverzüglich nachzuholen. Wird die Zustimmung nicht erteilt, ist die empfangende Stelle verpflichtet, die übermittelten Daten nach Aufforderung des Bundesnachrichtendienstes unverzüglich zu löschen. Der Bundesnachrichtendienst unterrichtet das Bundeskanzleramt in regelmäßigen Abständen über Übermittlungen nach Absatz 1.

(3) Der Bundesnachrichtendienst darf die mit dem Zweck der politischen Unterrichtung gekennzeichneten personenbezogenen Daten, die durch Maßnahmen nach den §§ 19 und 34 erhoben wurden, an nicht öffentliche ausländische Stellen nur übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass eine Übermittlung erforderlich ist zur Abwendung einer unmittelbar bevorstehenden Gefahr für

1. Leib, Leben oder Freiheit einer Person oder

2. lebenswichtige Güter der Allgemeinheit.

(4) Der Bundesnachrichtendienst darf personenbezogene Daten an nicht öffentliche ausländische Stellen ohne Vorliegen der Voraussetzungen des Absatzes 1 oder 3 übermitteln, wenn die Daten

1. dieser nicht öffentlichen ausländischen Stelle lediglich zur Konkretisierung einer Anfrage übermittelt werden, und

2. dieser nicht öffentlichen ausländischen Stelle bereits bekannt sind.

ENTWURF

§ 11g

Übermittlung von personenbezogenen Daten aus einer Vertraulichkeitsbeziehung an ausländische Stellen oder über- oder zwischenstaatliche Stellen

Für die Übermittlung von personenbezogenen Daten aus einer Vertraulichkeitsbeziehung (§ 21 Absatz 1 Satz 2) an ausländische Stellen oder über- oder zwischenstaatliche Stellen gilt § 11d entsprechend.“

12. Vor § 12 wird folgende Überschrift eingefügt:

„Unterabschnitt 5

Gemeinsame Dateien“.

13. § 18 wird aufgehoben.

14. Abschnitt 4 wird wie folgt geändert:

a) In § 21 Absatz 2 Nummer 1 wird die Angabe „§ 29 Absatz 3“ durch die Angabe „§ 11a Absatz 1 und 2“ ersetzt.

b) § 25 wird wie folgt geändert:

aa) In Absatz 3 Satz 4 werden die Wörter „Bundesministerium des Innern, für Bau und Heimat“ durch die Wörter „Bundesministerium des Innern und für Heimat“ und die Angabe „10. August 2018 (GMBl S. 826)“ durch die Angabe „13. März 2023 (GMBl S. 542)“ ersetzt.

bb) In Absatz 4 Satz 2 werden die Wörter „Bundesministerium des Innern, für Bau und für Heimat“ durch die Wörter „Bundesministerium des Innern und für Heimat“ ersetzt.

c) In § 28 Absatz 3 Satz 3 wird die Angabe „§ 30“ durch die Angabe „§ 11f“ ersetzt.

d) Der Unterabschnitt 2 wird aufgehoben.

e) In § 35 Absatz 2 Nummer 1 wird die Angabe „§ 29 Absatz 3“ durch die Angabe „§ 11b Absatz 1 und 2“ ersetzt.

f) Die §§ 38 und 39 werden aufgehoben.

g) In § 42 Absatz 1 Nummer 5 wird die Angabe „§ 29 Absatz 8 und § 30 Absatz 9“ durch die Angabe „§°11d und §°11g in Verbindung mit §°11d“ ersetzt.

h) In § 42 Absatz 2 Nummer 2 wird die Angabe „§ 29 Absatz 7 und § 30 Absatz 5“ durch die Angabe „§°11b Absatz°4, §°11c Absatz°3, §°11e Absatz°4 und §°11f Absatz°3“ ersetzt.

15. In § 63 werden die Wörter „Bundesministerium des Innern, für Bau und Heimat“ durch die Wörter „Bundesministerium des Innern und für Heimat“ ersetzt.

16. § 65 wird wie folgt geändert:

ENTWURF

a) In der Überschrift wird das Wort „Berichtspflicht“ durch die Wörter „Politische Unterrichtung“ ersetzt.

b) Absatz 1 wird wie folgt geändert:

aa) In Satz 1 werden nach dem Wort „unterrichtet“ die Wörter „zum Zweck der Information der Bundesregierung zur Wahrnehmung ihrer außen- und sicherheitspolitischen Verantwortung“ eingefügt. Das Wort „Übermittlung“ wird durch das Wort „Weitergabe“ ersetzt.

bb) Satz 2 wird durch die folgenden Sätze ersetzt:

„Soweit es für diesen Zweck erforderlich ist, darf der Bundesnachrichtendienst auch weitere inländische öffentliche Stellen unterrichten. Die empfangende Stelle darf die zur Verfügung gestellten Daten nur zu diesem Zweck verarbeiten. Die §§°11 bis 11 g finden keine Anwendung“

c) Nach Absatz 1 wird folgender Absatz 2 eingefügt:

„(2) Der Bundesnachrichtendienst darf entsprechend Absatz°1 die Europäische Union sowie die Organisation des Nordatlantikvertrags zum Zweck der Wahrnehmung ihrer außen- und sicherheitspolitischen Verantwortung unterrichten“.

d) Der bisherige Absatz 2 wird Absatz 3.

17. Nach § 65 wird folgender Abschnitt 6 eingefügt:

„Abschnitt 6

Sicherung von Verschlusssachen im Bundesnachrichtendienst

Unterabschnitt 1

Befugnisse, Durchführung und Anordnung

§ 65a

Maßnahmen zur Sicherung von Verschlusssachen

(1) Der Bundesnachrichtendienst trifft Maßnahmen zur Sicherung von Verschlusssachen nach den §§ 65b bis 65d, um zu erkennen und zu verhindern, dass

1. 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

2. Verschlusssachen aus Dienststellen des Bundesnachrichtendienstes unbefugt ausgebracht werden.

(2) Maßnahmen nach Absatz 1 dürfen nur durchgeführt werden bei

ENTWURF

1. Mitarbeiterinnen und Mitarbeitern des Bundesnachrichtendienstes,

2. Mitarbeiterinnen und Mitarbeitern anderer inländischer oder ausländischer öffentlicher Stellen, die sich in Dienststellen des Bundesnachrichtendienstes aufhalten, und

3. anderen Personen, die sich mit Erlaubnis des Bundesnachrichtendienstes in seinen Dienststellen aufhalten.

Die in Satz 1 genannten Personen sind zur Mitwirkung bei der Durchführung von Maßnahmen zur Sicherung von Verschlusssachen verpflichtet.

(3) Der Bundesnachrichtendienst hat die in Absatz 2 Satz 1 genannten Personen in geeigneter Form zu belehren über

1. den ordnungsgemäßen Umgang mit Verschlusssachen,

2. die Möglichkeit, dass bei ihnen Maßnahmen nach den §§ 65b bis 65d durchgeführt werden können, sowie

3. deren Pflicht zur Mitwirkung bei der Durchführung der Maßnahmen.

§ 65b

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, nach § 65f Absatz 2 durchführen und

2. Durchsuchungen von Personen, Taschen und Fahrzeugen sowie mitgeführten Gegenständen nach § 65f Absatz 3 vornehmen, wenn tatsächliche Anhaltpunkte dafür vorliegen, dass die Durchsuchung zur Sicherung von Verschlusssachen erforderlich ist.

§ 65c

Kontrolle und Durchsuchung von Räumen zur Sicherung von Verschlusssachen

(1) Zur Sicherung von Verschlusssachen darf der Bundesnachrichtendienst

1. verdachtsunabhängige Raumkontrollen nach § 65f Absatz 2 in seinen Dienststellen durchführen und

2. Durchsuchungen von Räumen in seinen Dienststellen einschließlich der in den Räumen vorhandenen Gegenstände nach § 65f Absatz 3 vornehmen, wenn Tatsachen die Annahme rechtfertigen, dass dies zur Sicherung von Verschlusssachen erforderlich ist.

ENTWURF

(2) Zur Sicherung von Verschlusssachen darf der Bundesnachrichtendienst in seinen Dienststellen in Gemeinschaftsflächen und allgemein zugänglichen Räumen, deren Beschaffenheit die Begehung von Verstößen gegen Vorschriften zum Schutz von Verschlusssachen begünstigt, technische Mittel zur offenen optischen Überwachung einsetzen. Der Einsatz ist durch geeignete Maßnahmen erkennbar zu machen.

§ 65d

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, mit technischen Mitteln eingreifen sowie die auf den Geräten gespeicherten Informationen einschließlich personenbezogener Daten verarbeiten, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass die betroffene Person eine Straftat plant, begeht oder begangen hat, die einen unmittelbaren Bezug zu sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten im Sinne des § 2 Absatz 1 Satz 1 Nummer 1 aufweist. Straftaten nach Satz 1 sind insbesondere

1. Straftaten des Friedensverrats oder des Hochverrats (§§ 80a bis 83 des Strafgesetzbuches),

2. Straftaten der Gefährdung des demokratischen Rechtsstaates (§§ 86 bis 89c, § 91 des Strafgesetzbuches),

3. Straftaten des Landesverrats und der Gefährdung der äußeren Sicherheit sowie Straftaten gegen ausländische Staaten (§§ 94 bis 100, § 102 des Strafgesetzbuches)

4. Straftaten gegen die Landesverteidigung (§§ 109e bis § 109g des Strafgesetzbuches),

5. Straftaten gegen die öffentliche Ordnung (§ 126a, § 133 des Strafgesetzbuches),

6. Straftaten nach den §§ 202a bis 202c und §§ 303a bis 303b des Strafgesetzbuches, soweit diese die Sicherheit von Verschlusssachen beeinträchtigen, und

7. Straftaten nach § 353b des Strafgesetzbuches.

Die Maßnahme darf sich auch gegen Personen im Sinne von § 65a Absatz 2 Satz 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 ihr herrühren, für sie weitergeben werden. Die Sätze 1 bis Satz 3 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 vorschriftenwidrig in Dienststellen des Bundesnachrichtendienstes eingebracht hat, sicherstellen, in die sichergestellten Geräte mit technischen Mitteln eingreifen sowie die auf den Geräten

gespeicherten Informationen einschließlich personenbezogener Daten verarbeiten, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass die betroffene Person eine Straftat nach Absatz 2 Sätze 1 und 2 plant, begeht oder begangen hat. Die Maßnahme darf sich auch gegen Personen im Sinne von § 65a Absatz 2 Satz 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 ihr herrühren, für sie weitergeben werden. Die Sicherstellung nach Satz 1 darf 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 das Gerät sicherstellen. Er hat geeignete Maßnahmen zu treffen, um die berechtigte Person ausfindig zu machen. Wenn die berechtigte Person nicht innerhalb von einem Monat ausfindig gemacht werden kann, darf der Bundesnachrichtendienst in das Gerät mit technischen Mitteln eingreifen sowie die auf den Geräten gespeicherten Informationen einschließlich personenbezogener Daten soweit 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 vorschriftenwidrig 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 3 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 hat der Bundesnachrichtendienst sicherzustellen, dass

1. an dem Gerät nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, rückgängig gemacht werden.

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 2 nicht, 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 nach § 65f Absatz 3 durchsuchen, wenn diese das Gerät nicht freiwillig herausgibt.

§ 65e

Anordnung von Maßnahmen zur Sicherung von Verschlusssachen

(1) Maßnahmen nach den §§ 65b bis 65d, mit Ausnahme von Kontrollen nach § 65b Nummer 1, bedürfen der Anordnung der oder des Geheimschutzbeauftragten des Bundesnachrichtendienstes oder einer von ihr oder ihm bestimmten Vertretung, in den Fällen des § 65d Absatz 3 der Anordnung durch die Behördenleitung des Bundesnachrichtendienstes oder ihre Vertretung. Die Anordnung sowie die im Rahmen der Maßnahmen nach Satz 1 erhobenen Informationen einschließlich personenbezogenen Daten sind durch den Bundesnachrichtendienst zu dokumentieren. In der Anordnung sind anzugeben:

1. Art und Beschreibung der Maßnahme nach den § 65b Nummer 2, §§ 65c und 65d,

2. die betroffenen Personen,

3. Anlass der Maßnahme und

4. Begründung der Maßnahme.

In den Fällen des § 65c 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.

(2) Ist eine Anordnung nach Absatz 1 Satz 1 aufgrund 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 § 65d Absätze 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. Die besondere Eilbedürftigkeit ist in der Anordnung zu begründen. Wird die Anordnung nach Absatz 1 nicht nachgeholt, so hat der Bundesnachrichtendienst die bereits erhobenen Daten unverzüglich zu löschen und das private Gerät der Informations- und Kommunikationstechnik an die betroffene Person herauszugeben.

(3) Widerspruch und Anfechtungsklage gegen Maßnahmen nach Absatz 1 haben keine aufschiebende Wirkung.

§ 65f

Durchführung von Maßnahmen zur Sicherung von Verschlusssachen

(1) Bei der Durchführung von Maßnahmen zur Sicherung von Verschlusssachen hat der Bundesnachrichtendienst unter mehreren möglichen und geeigneten Maßnahmen diejenigen zu treffen, die den Einzelnen am wenigsten beeinträchtigen. Eine Maßnahme darf nicht zu einem Nachteil führen, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht.

(2) Eine Kontrolle nach § 65b Nummer 1 und § 65c Absatz 1 Nummer 1 ist 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 stattfindet.

(3) Eine Durchsuchung nach § 65b Nummer 2, § 65c Nummer 2 und § 65d Absatz 8 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. in Fahrzeugen einschließlich dort befindlicher Gegenstände der betroffenen Person sowie

4. in sonstigen Gegenständen der betroffenen Person, die zur Verbringung von Verschlusssachen geeignet sind.

(4) Im Rahmen 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 § 65d vorliegen.

(5) Bei der Durchsuchung von Gegenständen nach Absatz 3 hat die betroffene Person das Recht, anwesend zu sein. Ihr ist auf Verlangen eine Bescheinigung über die Durchsuchung und über den Grund der Durchsuchung zu erteilen.

(6) Maßnahmen nach den §§ 65b bis 65d, die auf die Herausgabe einer Sache oder auf die Vornahme einer Handlung oder auf Duldung gerichtet sind, kann der Bundesnachrichtendienst mit Zwangsmitteln nach Absatz 7 durchsetzen. Dies gilt nicht für Kontrollen nach § 65b Nummer 1 an Eingängen zum Zwecke des § 65a Absatz 1 Nummer 1. § 6 Absatz 2 und § 18 Absatz 2 des Verwaltungs-Vollstreckungsgesetzes sind entsprechend anzuwenden.

(7) Der Bundesnachrichtendienst darf zur Durchsetzung von Maßnahmen nach den §§ 65b bis 65d folgende Mittel anwenden:

1. unmittelbare Einwirkung auf die betroffene Person durch körperliche Gewalt oder durch Hilfsmittel der körperlichen Gewalt; 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 oder Widerstand leisten oder sich der Kontrolle entziehen,

ENTWURF

2. unmittelbare Einwirkung auf Gegenstände mittels körperlicher Gewalt oder durch Hilfsmittel der körperlichen Gewalt.

Die Anwendung der Zwangsmittel nach Satz 1 darf nur durch Personen erfolgen, die durch die Behördenleitung des Bundesnachrichtendienstes oder ihre Vertretung hierzu besonders ermächtigt wurden.

Unterabschnitt 2

Verarbeitung und Übermittlung von personenbezogenen Daten aus Maßnahmen zur Sicherung von Verschlusssachen

§ 65g

Kennzeichnung, Speicherung, Löschung und Zweckbindung

(1) Der Bundesnachrichtendienst darf die im Rahmen der Maßnahmen nach den §§ 65b bis 65d erforderlichen Informationen einschließlich personenbezogener Daten verarbeiten, soweit nicht die anzuwendenden Bestimmungen des Bundesdatenschutzgesetzes oder besondere Regelungen in diesem Abschnitt entgegenstehen. Personenbezogene Daten, die im Rahmen von Maßnahmen nach den §§ 65b bis 65d erhobenen worden sind, sind entsprechend zu kennzeichnen.

(2) Die Informationen 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. § 65d Absatz 7 Satz 2 bleibt unberührt.

(3) Der Bundesnachrichtendienst darf personenbezogene Daten, die im Rahmen von Maßnahmen nach den §§ 65b bis 65d erhoben wurden, über die Absätze 1 und 2 hinaus nur weiterverarbeiten, wenn die weitere Verarbeitung nach § 2 Absatz 1 Satz 1 Nummer 1 oder Nummer 2 erforderlich ist. § 7 ist mit der Maßgabe anzuwenden, dass die Prüffrist sechs Monate beträgt.

§ 65h

Schutz des Kernbereichs privater Lebensgestaltung

(1) Die Datenerhebung zum Zweck der Erlangung von Erkenntnissen über den Kernbereich privater Lebensgestaltung ist unzulässig. Der Bundesnachrichtendienst darf Erkenntnisse, die den Kernbereich privater Lebensgestaltung berühren, nicht verarbeiten, weitergeben oder in anderer Weise nutzen. Der Bundesnachrichtendienst hat, soweit möglich, technisch und auf sonstige Weise sicherzustellen, dass Erkenntnisse, die den Kernbereich privater Lebensgestaltung betreffen, nicht erlangt werden.

(2) Soweit Erkenntnisse erlangt wurden, die den Kernbereich privater Lebensgestaltung betreffen, sind diese Daten unverzüglich zu löschen.

(3) Wird für den Bundesnachrichtendienst erkennbar, dass durch eine Maßnahme nach den §§ 65b bis 65d in den Kernbereich privater Lebensgestaltung eingedrungen

wird, ist diese unverzüglich zu unterbrechen. Ist für den Bundesnachrichtendienst zu erwarten, dass bei einer Fortführung der Maßnahme nicht nur am Rande Erkenntnisse über den Kernbereich privater Lebensgestaltung erlangt werden, so hat er die Maßnahme abzubrechen.

§ 65i

Personenbezogene Daten aus Vertraulichkeitsbeziehungen

Sofern in den sichergestellten Unterlagen und Daten Kommunikation aus Vertraulichkeitsbeziehungen nach § 21 Absatz 1 Satz 2 enthalten ist, gilt § 21 für diese Kommunikationen entsprechend.

§ 65j

Schutz von minderjährigen Personen

(1) Der Bundesnachrichtendienst darf im Rahmen von Maßnahmen nach den §§ 65b bis 65d erhobene personenbezogene Daten von minderjährigen Personen, die nicht zu den in § 65a Absatz 2 genannten Personen gehören, nicht weiterverarbeiten. Die erhobenen personenbezogenen Daten nach Satz 1 sind zu löschen, es sein denn, die Trennung der personenbezogenen Daten von anderen Informationen, die im Rahmen von Maßnahmen nach den §§ 65b bis 65d 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 16 Jahre alt sind und die zu dem in § 65a Absatz 2 genannten Personenkreis gehören.

§ 65k

Protokollierung

(1) Werden Informationen einschließlich personenbezogener Daten aus Maßnahmen nach den §§ 65b bis 65d in automatisierten Dateien verarbeitet, so hat der Bundesnachrichtendienst die Erhebung, Veränderung, Abfrage sowie Löschung der erhobenen personenbezogenen Daten zu protokollieren. Werden Daten nach § 65h Absatz 2 gelöscht, so ist zusätzlich auch der Grund der Löschung zu protokollieren.

(2) Die Protokolldaten dürfen ausschließlich zur Durchführung von Kontrollen der betrieblichen Datenverarbeitung einschließlich der Datenschutzkontrollen verwendet werden.

(3) Die Protokolldaten sind bis zum Ablauf des zweiten Kalenderjahres, das auf das Kalenderjahr der Protokollierung folgt, aufzubewahren. Nach Ablauf der Aufbewahrungsfrist sind die Protokolldaten unverzüglich zu löschen. Der Bundesnachrichtendienst hat die Protokolle der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen ihrer oder seiner Zuständigkeit nach § 63 zur Verfügung zu stellen.

(4) Der behördliche Datenschutz des Bundesnachrichtendienstes kann die Einhaltung der Vorgaben des Unterabschnitts 2 jederzeit überprüfen.

ENTWURF

§ 65l

Übermittlung von personenbezogenen Daten aus Maßnahmen zur Sicherung von Verschlusssachen

(1) Die Übermittlung personenbezogener Daten, die im Rahmen von Maßnahmen zur Sicherung von Verschlusssachen nach den §§ 65b bis 65d erhoben wurden, richtet sich nach § 25 Absatz 1 des Bundesdatenschutzgesetzes.

(2) Stellt der Bundesnachrichtendienst im Rahmen von Maßnahmen nach §§ 65b bis 65d 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.“

18. Die bisherigen Abschnitte 6 und 7 werden die Abschnitte 7 und 8.

Artikel 2

Änderung des Artikel 10-Gesetzes

Das Artikel 10-Gesetz vom 26. Juni 2001 /BGBl I S. 1254, 2298; 2017 I S. 154), das zuletzt durch Artikel 6 Absatz 4 des Gesetzes vom 5. Juli 2021 (BGBl S. 2274) geändert worden ist, wird wie folgt geändert:

1. Nach § 5a wird folgender § 5b eingefügt:

„§ 5b

Schutz zeugnisverweigerungsberechtigter Personen

Für den Schutz zeugnisverweigerungsberechtigter Personen gilt § 3b entsprechend.“

2. In § 7 werden die Absätze 1 bis 4a durch die folgenden Absätze 1 bis 3 ersetzt:

„(1) Durch Beschränkungen nach § 5 erhobene personenbezogene Daten dürfen an die Verfassungsschutzbehörden des Bundes und der Länder sowie an das Bundesamt für den Militärischen Abschirmdienst unter den Voraussetzungen des § 11 des BND-Gesetzes übermittelt werden.

(2) Durch Beschränkungen nach § 5 erhobene personenbezogene Daten dürfen an inländische Strafverfolgungsbehörden unter den Voraussetzungen des § 11a des BND-Gesetzes übermittelt werden.

(3) Durch Beschränkungen nach § 5 erhobene personenbezogene Daten dürfen an inländische öffentliche Stellen unter den Voraussetzungen des § 11b des BND-Gesetzes übermittelt werden.“

3. § 7a wird wie folgt geändert:

a) Die Absätze 1 und 2 werden wie folgt gefasst:

ENTWURF

„(1) Der Bundesnachrichtendienst darf durch Beschränkungen nach § 5 Absatz 1 Satz 3 Nummer 2, 3, 7 und 8 erhobene personenbezogene Daten unter den Voraussetzungen des § 11e des BND-Gesetzes an die mit nachrichtendienstlichen Aufgaben betrauten ausländischen öffentlichen Stellen übermitteln.

(2) Die Übermittlung bedarf der Zustimmung des Bundeskanzleramtes.“

b) Absatz 5 wird wie folgt gefasst:

„(5) Das Bundeskanzleramt unterrichtet monatlich die G10-Kommission über Übermittlungen nach Absatz 1.“

4. § 8 wird wie folgt geändert:

a) Die Absätze 5 und 6 werden wie folgt gefasst:

„(5) Die erhobenen personenbezogenen Daten dürfen unter den Voraussetzungen der §§ 11 bis 11b des BND-Gesetzes übermittelt werden, wenn zudem tatsächliche Anhaltspunkte den Verdacht begründen, dass jemand eine Straftat plant oder begeht, die geeignet ist, zu der Entstehung oder Aufrechterhaltung der in Absatz 1 bezeichneten Gefahr beizutragen.

(6) Die erhobenen personenbezogenen Daten dürfen an Strafverfolgungsbehörden unter den Voraussetzungen des § 11a des BND-Gesetzes übermittelt werden, wenn zudem bestimmte Tatsachen den Verdacht begründen, dass jemand eine in Absatz 5 bezeichnete Straftat begeht oder begangen hat.“

b) Folgender Absatz 7 wird angefügt:

„(7) § 7 Absatz 5 und 6 sowie § 7a gelten entsprechend.“

Artikel 3

Inkrafttreten

Dieses Gesetz tritt am 1. Januar 2024 in Kraft.

ENTWURF

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Mit der Gesetzesnovelle soll die aktuelle Rechtsprechung des Bundesverfassungsgerichts für den Bundesnachrichtendienst im BNDG sowie im G10 umgesetzt sowie der Schutz von Verschlusssachen im Bundesnachrichtendienst gestärkt werden

II. Wesentlicher Inhalt des Entwurfs

Bis zum 31. Dezember 2023 hat eine Neuregelung der Übermittlungsvorschriften des BNDG aufgrund der Entscheidung des Bundesverfassungsgerichts vom 28. September 2022 (1 BvR 2354/13) zu den Übermittlungsregelungen im BVerfSchG zu erfolgen, da § 11 BNDG als allgemeine Übermittlungsnorm an die Übermittlungsnormen im BVerfSchG anknüpft.

Nachrichtendienste dürfen Daten im Vorfeld konkreter Gefahren erheben. Diese weitreichenden Überwachungsbefugnisse sind verfassungsrechtlich nur gerechtfertigt, wenn die aus der Überwachung gewonnen Informationen nicht ohne Weiteres an andere Behörden mit operativen Anschlussbefugnissen übermittelt werden dürfen („informationelles Trennungsprinzip“). Materielle Voraussetzung für Übermittlungen durch den Bundesnachrichtendienst an andere Stellen im In- und Ausland, die (auch) operative Anschlussbefugnisse haben, sind tatsächliche Anhaltspunkte für das Vorliegen einer konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut (BVerfG, Beschluss vom 28. September 2022, 1 BvR 2354/13, Rn. 120 f.). Für die Übermittlung von nachrichtendienstlichen Informationen ins Ausland gelten die gleichen Anforderungen wie für eine Übermittlung im Inland (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 261). In jedem Fall müssen die Übermittlungsregelungen normenklar gefasst sein (vgl. zuletzt BVerfG, Beschluss vom 28. September 2022, 1 BvR 2354/13, Leitsatz 2 sowie Rn. 110 ff.).

Die Vorgaben des Bundesverfassungsgerichts werden durch normenklare Regelungen und eine Entkopplung vom BVerfSchG (d.h. durch Auflösung der im geltenden Recht bestehenden Verweisungen) umgesetzt. Dazu werden ausdifferenzierte Regelungen unter Berücksichtigung insbesondere der Art der Empfängerbehörde (Nachrichtendienste, Bundeswehr, Gefahrabwehrbehörden, Strafverfolgungsbehörden; Inland/ Ausland) vorgesehen.

Bei der Regelung von Übermittlungen an öffentliche Stellen mit auch operativen Anschlussbefugnissen legt dieser Entwurf einen Regel-Ausnahmekatalog unter Berücksichtigung des gesetzgeberischen Ermessensspielraumes zugrunde. Die Regel ist, dass Übermittlungen an öffentliche Stellen mit auch operativen Anschlussbefugnissen nur bei Vorliegen einer konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut erfolgen dürfen. In eng begrenzten Fallgestaltungen wird aufgrund der überragenden Bedeutung dieser Rechtsgüter und bestimmter Risikofaktoren, die das Gefährdungspotenzial für eine Rechtsgutverletzung steigern, ein Ausnahmekatalog mit Fallkonstellationen geschaffen, in denen vom Vorliegen einer konkretisierten Gefahr abgesehen wird. Begrenzt wird die Eingriffswirkung in diesem Fällen zusätzlich durch den Ausschluss operativer Anwendung unmittelbaren Zwangs. Dieses Regel-Ausnahme-Verhältnis entspricht der grundsätzlichen Regelungssystematik der Rechtsprechung des Bundesverfassungsgerichts. In dieser ist bereits eine Privilegierung bestimmter Empfangsbehörden vorgesehenen (insbesondere andere inländischer Nach-

richtendienste ohne operative Anschlussbefugnisse). Zugleich trifft der Gesetzgeber transparent anhand spezifisch dargestellter Belange eine zukunftsfeste Entscheidung zur Rolle des Bundesnachrichtendienstes in der Sicherheitsarchitektur der Bundesrepublik Deutschland. Die Übermittlungsregelungen für die strategische Fernmeldeaufklärung nach §§ 5 und 8 G 10 werden entsprechend angepasst.

Die Befugnisse des Bundesnachrichtendienstes zur Durchführung von Maßnahmen zur Sicherung von Verschlusssachen als Konkretisierung der bereits geltenden Vorschriften des Sicherheitsüberprüfungsgesetzes (SÜG) und des § 2 Absatz 1 Satz 1 Nummer 1 BNDG werden klar und abschließend geregelt. Dies umfasst die Befugnisse zur Durchführung von Personen-, Taschen-, Fahrzeug- und Raumkontrollen, die Befugnisse zur Überprüfung von dienstlichen Geräten der Informations- und Kommunikationstechnik sowie zur Überprüfung von unerlaubt in dessen Dienststellen eingebrachten privaten Geräten der Informations- und Kommunikationstechnik, insbesondere von privaten Geräten wie etwa Mobiltelefonen. Unterschieden wird zwischen verdachtsunabhängigen Maßnahmen mit einer geringen Eingriffstiefe, z.B. Torkontrollen mit technischen Mitteln und verdachtsabhängigen, eingriffsintensiven Maßnahmen, z.B. zur Durchsuchung von Personen und Taschen. Für die besonders eingriffsintensive Befugnis zur Auswertung von privaten Geräten der Informations- und Kommunikationstechnik bedarf es verdachtsbegründeter Anhaltspunkte für das Begehen einer Straftat mit Bezug zu einer sicherheitsgefährdenden oder geheimdienstlichen Tätigkeit der Mitarbeiterin oder des Mitarbeiters. Für die Durchführung der Maßnahmen wird ein formelles Anordnungsverfahren geregelt und die Befugnis zur Anwendung des unmittelbaren Zwangs zur Durchsetzung der Maßnahmen normiert. Das Trennungsprinzip wird nicht berührt, da die Maßnahmen ausschließlich behördenintern ausgeübt werden dürfen.

Mit den gesetzlichen Änderungen soll keine Umnummerierung des BNDG einhergehen, da die erst kürzlich angepassten Normen in den Systemen des Bundesnachrichtendienstes übernommen wurden (z.B. bei Kennzeichnungspflichten). Eine Umnummerierung würde daher zu einem hohen Verwaltungsaufwand führen, den es zu vermeiden gilt.

III. Alternativen

Keine.

IV. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes ergibt sich aus Artikel 73 Absatz 1 Nummer 1 GG.

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland geschlossen hat, vereinbar.

VI. Gesetzesfolgen

Die Regelungen tragen zur Sicherheit der Bundesrepublik Deutschland bei und stellen dabei einen ausgewogenen Ausgleich zwischen den damit verfolgten Gemeinwohlbelangen und den Interessen einzelner Personen, die durch die Datenverarbeitung in ihren Persönlichkeitsrechten betroffen sind, her.

ENTWURF

1. Rechts- und Verwaltungsvereinfachung

Durch Aufhebung der Verweisungsketten im BNDG auf das BVerfSchG wird die Rechtsanwendung vereinfacht, weil sich nunmehr die Übermittlungsbefugnisse normenklar aus dem BNDG ergeben.

2. Nachhaltigkeitsaspekte

Der Gesetzentwurf steht im Einklang mit der Nationalen Nachhaltigkeitsstrategie. Der Datenschutz wird nach den Maßgaben des Bundesverfassungsgerichts gestärkt, indem der Bundesnachrichtendienst mit rechtssicheren und normenklaren Übermittlungsbefugnissen ausgestattet wird.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Haushaltsausgaben ohne Erfüllungsaufwand entstehen für den Bundesnachrichtendienst in Folge der personellen Aufwände aufgrund Sacheinzel- und Gemeinkosten im Umfang von geschätzt etwa 2,7 Mio. EUR pro Jahr.

Der Mehrbedarf an Sach- und Personalmitteln soll finanziell und planstellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

4. Erfüllungsaufwand

Mit der Umsetzung des Gesetzes entstehen personelle und finanzielle Aufwände beim Bundesnachrichtendienst, um die Kontrollen beim Umgang mit Verschlusssachen in den Dienststellen des Bundesnachrichtendienstes zu verstärken.

Es entstehen einmalige Ausgaben aus dem Erfüllungsaufwand für Investitionen in Höhe von geschätzt 10,0 Mio. EUR. Die jährlichen Ausgaben aus dem Erfüllungsaufwand belaufen sich auf 3,9 Mio. EUR.

Der Erfüllungsaufwand für den Bundesnachrichtendienst resultiert aus der Durchführung der erweiterten Kontrollbefugnisse, dem Betrieb der dafür notwendigen technischen Geräte und der Verarbeitung bzw. Auswertung der gewonnenen Informationen. Der personelle Aufwand für die Durchführung von Kontrollen und den Betrieb der Geräte in den innerdeutschen Dienststellen des Bundesnachrichtendienstes wird auf insgesamt 9.400 Personentage pro Jahr (dies entspricht 47 Personen pro Jahr) geschätzt. Die personellen Aufwände in den anderen Dienststellen wird auf 400 Personentage pro Jahr (dies entspricht zwei Personen pro Jahr) geschätzt. Hinzu kommen Aufwände für insbesondere die Auswertung sichergestellter Geräte der Informations- und Kommunikationstechnik, die regelmäßige Datenpflege sowie der Umgang mit festgestellten Verstößen gegen die Verschlusssachenanweisung. Der mit diesen Aufgaben einhergehende Aufwand wird auf 600 Personentagen pro Jahr (dies entspricht drei Personen pro Jahr) geschätzt. Die zugehörigen Personalausgaben belaufen sich auf jährlich etwa 2,5 Mio. EUR.

Zur Unterstützung der mit den Kontrollbefugnissen einhergehenden Aufgaben sind technische Geräte bereitzustellen. Alle größeren Dienststellen sollen mit fest zu installierenden Detektionssystemen ausgestattet werden, u.a. um die Mitnahme privater Film- und Fotogeräte, sowie privater Geräte und Mittel der Informationstechnik, die zur Aufzeichnung und Speicherung dienstlicher Informationen geeignet sind, zu detektieren. Zudem sollen mobile Geräte für kleinere Dienststellen sowie ergänzende Kontrollen bereitgestellt werden. Diese einmaligen Investitionskosten hierfür werden auf ca. 9,5 Mio. EUR geschätzt.

Zur IT-gestützten Verarbeitung und Übermittlung der gewonnenen Informationen – darunter fallen u.a. die Protokollierung sowie die Einhaltung der Löschfristen und der Übermittlungsvorgaben – sind die bestehenden IT-Systeme einmalig entsprechend zu ertüchtigen. Dies

betrifft sowohl die punktuelle Anpassung der vorhandenen Software als auch die Erweiterung der Server und der Speichersysteme. Die hierfür anfallenden einmaligen Aufwände werden auf 0,5 Mio. EUR geschätzt. Laufende jährliche Aufwände resultieren aus Wartung und Betrieb der einmaligen Investitionen in prognostizierter Höhe von 1,4 Mio. EUR.

Für den Bundesnachrichtendienst erfolgen aufgrund der notwendigen Geheimhaltung keine konkreten Ausführungen.

Der Erfüllungsaufwand soll finanziell und planstellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

Der mögliche zusätzliche Erfüllungsaufwand für das Bundesverwaltungsgericht wegen dessen erstinstanzlicher Zuständigkeit nach § 50 Absatz 1 Nummer 4 VwGO durch Rechtsschutzbegehren in Zusammenhang mit Kontrollen zur Sicherung von Verschlusssachen lässt sich vorab nicht verlässlich spezifizieren. Insbesondere das Auslesen von privaten Geräten der Informations- und Kommunikationstechnik, z.B. Mobiltelefonen, von Mitarbeiterinnen und Mitarbeitern des Bundesnachrichtendienstes ist an gewichtige Schwellen, insbesondere an einen Straftatenverdacht, geknüpft. Es ist daher voraussichtlich mit niedrigen zweistelligen Verfahrensanstrengungen pro Jahr zu rechnen.

5. Weitere Kosten

Keine.

6. Weitere Gesetzesfolgen

Keine.

B. Besonderer Teil

Zu Artikel 1 (Änderung des BND-Gesetzes)

Zu Nummer 1 (Inhaltsverzeichnis)

Das neue Inhaltsverzeichnis erleichtert das Erfassen der Regelungssystematik des Gesetzes und das Auffinden einzelner Regelungsbestandteile. Es steigert damit die Verständlichkeit des Gesetzes und dient der Transparenz.

Zu Nummer 2 (§ 1 Absatz 2 Satz 2)

Mit diesem Gesetz wird § 39 aufgehoben, da die Übermittlungsvorschrift nun in Abschnitt 3 aufgegangen ist. Deshalb erfolgt die Anpassung der Angabe.

Zu Nummer 3 (§ 2 Absatz 1a)

§ 2 Absatz 1a ist eine neue Vorschrift, die die Zulässigkeit des Einsatzes einer Verwaltungs-, Arbeitgeber- und Objektlegende zum Schutz des Bundesnachrichtendienstes und seiner Mitarbeiterinnen und Mitarbeiter klarstellt. Im Gegensatz zu § 5 Satz 2 BNDG i.V.m. § 8 Absatz 2 Satz 1 BVerfSchG erfolgt hier die Nutzung der Legende nicht unmittelbar zur heimlichen Beschaffung von Informationen. Die Legendennutzung erfolgt zum Schutz der Einrichtungen und der Mitarbeiterinnen und Mitarbeiter des Bundesnachrichtendienstes. Es besteht daher ein unmittelbarer Bezug zu der Befugnis nach § 2 Absatz 1 Satz 1 Nummer 1 BNDG, so dass die Regelung in § 2 Absatz 1 Satz 1 verortet ist.

ENTWURF

Legenden des Bundesnachrichtendienstes sind unter anderem in privatrechtlichen und öffentlich-rechtlichen Zusammenhängen erforderlich. Ein Beispiel hierfür ist, wenn ein Unternehmen eine Verwaltungslegende des Bundesnachrichtendienstes in ihren Steuerunterlagen verwendet oder ein Institut eine Verwaltungslegende des Bundesnachrichtendienstes als offiziellen Partner im Sinne der Compliance-Regeln benennt. Der neugefasste Absatz 1a schafft somit Rechtssicherheit auch für die Kooperations- und Vertragspartner des Bundesnachrichtendienstes.

Zu Nummer 4 (§ 6)

Zu Absatz 2

Neu aufgenommen wird die Möglichkeit der Speicherung personenbezogenen Daten von minderjähren Personen zu deren Schutz sowie die Speichermöglichkeit bei einer von Minderjährigen ausgehenden Gefahr für Einrichtungen der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages. Die Beurteilung der der Minderjährigkeit einer Person richtet sich nach den Vorschriften des Bürgerlichen Gesetzbuchs.

Deutschland trägt durch seine internationale Verantwortung auch Schutzpflichten gegenüber bestimmten internationalen Einrichtungen, so dass eine Erweiterung in Übereinstimmung mit internationalen Verpflichtungen steht. Darüber hinaus wird darauf verzichtet, die Speichermöglichkeit von personenbezogenen Daten Minderjähriger auf Gefahren im Ausland zu begrenzen. Es kann nicht darauf ankommen, ob eine Person oder Einrichtung im In- oder Ausland gefährdet ist; die Schutzpflicht der Bundesrepublik Deutschland besteht ebenso bei Gefahren im Inland.

Die Speicherung von personenbezogenen Daten zum Schutz von Minderjährigen ist in Einzelfall erforderlich, um deren Übermittlung nach § 9 h (Übermittlung zum Schutz der betroffenen Person) zu ermöglichen. Ein möglicher Anwendungsfall ist die Evakuierung von Personen aus einem Land, in dem ein gewaltsam herbeigeführter Regimewechsel stattgefunden hat. Hierbei ist neben der Speicherung der personenbezogenen Daten der Erwachsenen auch die Speicherung der Daten der mit zu evakuierenden Minderjährigen notwendig, da diese sonst nicht an bei der Evakuierung unterstützende Stellen übermittelt werden könnten. Die Notwendigkeit der Speicherung ergibt sich auch , wenn sich aus einem Bürgerkriegsland heraus eine dort verbleibende deutsche Staatsangehörige oder ein deutscher Staatsangehöriger an den Bundesnachrichtendienst wendet, damit ihre oder seine Kinder in Deutschland aufwachsen können oder sich die Kinder unbegleitet auf die Flucht begeben haben und nunmehr schutzsuchend sind.

Zu Nummer 5

Die Anpassung der Aufzählung in Absatz 3 und 4 ist Folge der Ziffer II. des Organisationserlasses des Bundeskanzlers vom 8. Dezember 2021 (BGBl I 5176).

Zu Nummer 6

Mit dieser Nummer werden die Übermittlungsvorschriften des BNDG an die Rechtsprechung des Bundesverfassungsgerichts angepasst und vollständig vom BVerfSchG entkoppelt. Dabei hat sich das Bundesverfassungsgericht mit Beschluss vom 28. September 2022 (1 BvR 2354/13) letztmals dezidiert mit den Übermittlungsvorschriften befasst und u.a. festgestellt, dass §§ 20, 21 BVerfSchG mit dem Grundgesetz nicht vereinbar sind. Die Entscheidung hat auch Auswirkungen auf die Frage der Rechtmäßigkeit der Übermittlungsvorschriften des Bundesnachrichtendienstes, da § 11 Absatz 3 BNDG auf § 20 BVerfSchG verweist.

Die in diesem Abschnitt ausgeformten Vorschriften setzen den aus Anlass der Entscheidung des Bundesverfassungsgerichts (Urteil vom 19. Mai 2020, 1 BvR 2835/17, BVerfGE

154, 152) mit der letzten BNDG-Novelle (BT-Drs. 19/26103) eingeschlagenen Weg zur Systematisierung auch der Übermittlungsbefugnisse des Bundesnachrichtendienstes fort. Mit dieser Novelle hatte der Deutsche Bundestag in Kenntnis der Vorschriften des BVerfSchG eigenständige Normen zur Übermittlung von durch technische Aufklärung gewonnenen Informationen beschlossen, die sich von den Vorschriften des BVerfSchG unterscheiden, um der Unterschiedlichkeit der beiden Nachrichtendienste Rechnung zu tragen.

Das Bundesverfassungsgericht fordert für die Übermittlung von mit nachrichtendienstlichen Mitteln erhobenen personenbezogenen Daten an Gefahrenabwehrbehörden, dass diese dem Schutz eines besonders gewichtigen Rechtsguts dient, für das wenigstens eine hinreichend konkretisierte Gefahr besteht (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 235). Die Übermittlung an Strafverfolgungsbehörden kommt nur zur Verfolgung besonders schwerer Straftaten in Betracht (BVerfG, aaO, Rn. 251). Die Übermittlung an andere Stellen ohne operative Anschlussbefugnisse muss zumindest dem Schutz eines besonders gewichtigen Rechtsguts dienen (BVerfG, aaO, Rn. 251).

Deshalb werden die Übermittlungsvorschriften des BNDG grundlegend überarbeitet, auch um dem Grundsatz der Normenklarheit bei den allgemeinen Übermittlungsnormen zu entsprechen. Die Übermittlungsschwellen werden unter Beachtung der Vorgaben des Bundesverfassungsgerichts nachrichtendienstspezifisch ausgestaltet.

Abschnitt 3 ist wie folgt gegliedert:

Unterabschnitt 1 enthält als allgemeiner Teil grundsätzliche Vorschriften, die für alle Übermittlungen nach dem BNDG gelten, mit Vorgaben zur Zweckbindung und Zweckänderungsmöglichkeiten, zur Protokollierung und zum Minderjährigenschutz, zu Übermittlungsverboten sowie zusätzliche Bestimmungen für die Übermittlung an ausländische Stellen wie die Beachtung von Menschenrechtsstandards, die Berücksichtigung nationale Sicherheitsinteressen und Auskunftspflichten der empfangenden Stelle.

Unterabschnitt 2 enthält die unveränderte Regelung zur Übermittlung personenbezogener Daten an den Bundesnachrichtendienst sowie eine Regelung zur Übermittlung personenbezogener Daten aus allgemein zugänglichen Quellen durch den Bundesnachrichtendienst. Unterabschnitt 3 betrifft Übermittlungen von personenbezogenen Daten aus nicht allgemein zugänglichen Quellen an inländische Stellen. Unterabschnitt 4 regelt die Übermittlungen von personenbezogenen Daten aus nicht allgemein zugänglichen Quellen an ausländische Stellen und an über- oder zwischenstaatliche Stellen. Die beiden Unterabschnitte 3 und 4 enthalten die ausdifferenzierten Übermittlungsregelungen, um die vom Bundesverfassungsgericht vorgegebenen materiellen und prozessualen Voraussetzungen übersichtlich umzusetzen.

Es wird folgende Konzeption bei der Ausformung der Übermittlungsvorschriften zugrunde gelegt: Übermittlungen an Nachrichtendienste und Bundeswehr werden unter gesonderten Voraussetzungen geregelt. Für die Übermittlung an Strafverfolgungsbehörden sowie an andere Stellen werden hohe Schwellen festgelegt. Zusätzlich werden spezifische Belange formuliert, bei denen vom Vorliegen einer konkretisierten Gefahr abgesehen wird.

Die Übermittlungsvorschriften gelten für vom Bundesnachrichtendienst selbst aus nicht allgemein zugänglichen Quellen erhobene personenbezogene Daten sowie für solche von anderen Stellen, die er mit selbst erhobenen personenbezogenen Daten anreichert. Fällt ihm, beispielweise aufgrund seines Alleinstellungsmerkmals als einziger deutscher Auslandsnachrichtendienst und Ansprechpartner insbesondere im internationalen Raum die Aufgabe der Weitergabe von Informationen an den adressierten Empfänger z.B. eine andere inländische öffentliche Stelle, zu, handelt es sich nicht um eine Übermittlung durch den Bundesnachrichtendienst im Sinne dieser Regelungen. Beispiel ist hierfür, dass ein ausländischer Nachrichtendienst ihm Informationen mit dem Hinweis zur Weitergabe an deutsche Polizeibehörden übergibt.

Die Normen des Abschnitts 3 regeln die Übermittlung von Daten an andere Stellen zur Verwendung in deren Sphäre. Werden Daten ausschließlich zum Zweck der Durchführung einer Unterstützungsleistung einem Dritten zugänglich gemacht (z.B. zum Zweck der Entschlüsselung, Übersetzung oder sonstigen Unterstützungsleistung wie etwa zur Sicherstellung bzw. Verbesserung von informationstechnischen Prozessabläufen oder Controllingprozessen im Bundesnachrichtendienst oder bei der Entwicklung technischer Datenverarbeitungssysteme für den Bundesnachrichtendienst), so handelt es sich nicht um eine Übermittlung. Oftmals ermöglicht erst die Unterstützungsleistung durch die empfangende Stelle die weitere Verarbeitung von Daten durch den Bundesnachrichtendienst. Der einer Übermittlung innewohnende Grundrechtseingriff liegt in diesem Fall gerade nicht vor, da die Daten nur für die Unterstützung des Bundesnachrichtendienstes genutzt werden dürfen und für die empfangende Stelle nicht frei verwendbar sind.

Zu Unterabschnitt 1 (Allgemeine Vorschriften bei Übermittlung von personenbezogenen Daten durch den Bundesnachrichtendienst)

Unterabschnitt 1 regelt vorab die allgemeinen Vorschriften, die für die den folgenden Unterabschnitten geregelten Übermittlungsbefugnisse Anwendung finden.

Zu § 9a (Zweckbindung der Übermittlung personenbezogener Daten)

Die Norm ist angelehnt an die bisherigen § 29 Absatz 12 BNDG und § 30 Absatz 8 Satz 3 bis 6 BNDG.

Zu Absatz 1

Der Bundesnachrichtendienst bestimmt als übermittelnde Behörde, zu welchen Zwecken die empfangende Stelle die Daten verarbeiten darf. Die Fortgeltung der Zweckbindung bei der weiteren Nutzung der personenbezogenen Daten durch die empfangende Stelle ist von herausgehobener Wichtigkeit. So kann es z.B. aus Gründen des Quellen- oder Methodenschutzes erforderlich sein, dass die übermittelten personenbezogenen Daten lediglich zur Unterrichtung der empfangenden Stelle übermittelt werden und durch diese nicht für Folgemaßnahmen verwendet oder nicht weitergegeben werden dürfen. Der Bundesnachrichtendienst kann in der Folge abfragen, wie die Weiterverarbeitung erfolgt ist.

Eine Weiterverarbeitung zu anderen Zwecken ist nur mit Zustimmung des Bundesnachrichtendienstes zulässig. Der Bundesnachrichtendienst darf einer über Satz 1 hinausgehenden Weiterverarbeitung nur zustimmen, wenn er die personenbezogenen Daten der empfangenden Stelle auch zu dem anderen Zweck hätte übermitteln dürfen, d.h. die jeweiligen Übermittlungsvoraussetzungen der §§°11 bis°11g. müssen auch für die Übermittlung zu dem geänderten Zweck vorliegen.

Zu Absatz 2

Die empfangende Stelle muss den Bundesnachrichtendienst auf Verlangen über eine Weiterverarbeitung informieren. Hierauf muss der Bundesnachrichtendienst die empfangende Stelle vorab nach Absatz 3 Nummer 2 hinweisen.

Zu Absatz 3

Aus Absatz 3 ergibt sich die Hinweispflicht des Bundesnachrichtendienstes zu den Pflichten des Empfängers aus den Absätzen 1 und 2.

ENTWURF

Zu Absatz 4

Ausländische Stellen sowie über- oder zwischenstaatliche Stellen müssen als empfangende Stelle dazu verpflichten werden, dem Bundesnachrichtendienst auf Verlangen Auskunft über die Weiterverarbeitung der Daten zu geben. Sie müssen darüber hinaus die Zusage abgeben, die übermittelten Daten auf dessen Verlangen zu löschen. Diese Verpflichtungen können im Wege von ausdrücklichen Hinweisen, denen entsprechend internationalen nachrichtendienstlichen Gepflogenheiten Geltung zugesprochen werden darf sowie Vereinbarungen bei jeder Übermittlung separat oder im Rahmen von generalisierten Vereinbarungen mit der empfangenden Stelle erfolgen. Diese flankierenden Maßnahmen stellen sicher, dass die Verantwortlichkeit für die übermittelten personenbezogenen Daten für den Bundesnachrichtendienst nicht mit der Übermittlung endet und eine Einwirkungsmöglichkeit auf die empfangende Stelle und damit verbunden auf die übermittelten personenbezogenen Daten des Bundesnachrichtendienstes erhalten bleibt. Nur so ist dem Bundesnachrichtendienst eine nachträgliche Kontrolle möglich. Da eine Übermittlung personenbezogener Daten ins Ausland grundsätzlich ein höheres Gefahrenpotential für den Schutz der Daten birgt, sieht Satz 2 im Falle von tatsächlichen Anhaltspunkten für eine Nichterfüllung der Zusicherung ein Übermittlungsverbot vor. Für diese Negativprognose darf der Bundesnachrichtendienst auch auf die bisher mit dem Empfänger gemachten Erfahrungen zurückgreifen.

Die Übermittlung von Daten ins Ausland bedarf darüber hinaus einer Rechtstaatlichkeitsvergewisserung über den Umgang der ausländischen Stellen mit den ihnen übermittelten Daten (vgl. BVerfGE 154, 152, Rn. 233 ff.). Absatz 4 wird hierbei ergänzt durch die Regelungen in § 9e Absatz 2 (Verbot der Übermittlung an ausländische Stellen oder an über- oder zwischenstaatliche Stellen).

Zu § 9b (Protokollierung der Übermittlung)

Die Norm ist angelehnt an den bisherigen § 29 Absatz 16 BNDG und regelt eine Protokollierungspflicht nunmehr für alle Übermittlungen des Bundesnachrichtendienstes. Die Protokollierung nach § 9b ersetzt nicht die Dokumentation der Übermittlungen.

Zu Absatz 1

Jede Übermittlung erfordert eine Protokollierung unter Vorhaltung spezifischer Informationen. Eine Übermittlung kann auch mündlich erfolgen, auch in diesen Fällen ist eine Protokollierung erforderlich. Die Protokollierung kann dann beispielsweise im Rahmen eines Ergebnisprotokolls zu einem Fachgespräch erfolgen. Die Protokollierung hat schriftlich zu erfolgen, eine bestimmte Form wird nicht vorgegeben.

Die Protokollierungspflicht umfasst auch die Nennung der der Übermittlung zugrunde gelegten Rechtsvorschriften (BVerfG, Beschluss vom 28. September 2022, 1 BvR 2354/13, Rn. 138). Allein die Nennung der Rechtsgrundlage ermöglicht jedoch noch nicht die Kontrolle, inwieweit die jeweiligen gesetzlichen Übermittlungsvorschriften eingehalten wurden. Aus diesem Grund umfasst die Protokollierungspflicht auch die empfangende Stelle der personenbezogenen Daten sowie den Zeitpunkt der Übermittlung.

Zu Absatz 2

Die Aufbewahrungspflicht sowie der Löschzeitpunkt werden verbindlich vorgegeben. Bei der Einhaltung der Löschfrist ist insbesondere in den Fällen der mündlichen Übermittlung zu beachten, dass keine Löschung aller Daten erforderlich ist. In diesen Fällen sind nur die Protokollierungsbestandteile zu löschen. Hierfür muss der Bundesnachrichtendienst Sorge tragen.

Zu Absatz 3

Die Regelung betrifft eine Ausnahme zur Löschung der Protokolldaten, wenn eine Trennung von anderen Daten unmöglich ist. Dies kann bei mündlichen Übermittlungen der Fall sein, wenn beispielsweise im Rahmen eines Ergebnisprotokolls zu einem Fachgespräch die Übermittlung protokolliert wird. Die Löschung kann unterbleiben, da mit der Löschung der Protokollierungsdaten auch der Inhalt des Gesprächs gelöscht werden müsste. Dieser kann jedoch auch nach Ablauf von zwei Jahren noch relevant sein.

Zu § 9c (Verbundene personenbezogene Daten)

Die Norm entspricht dem bisherigen § 29 Absatz 14 BNDG und dem geltenden § 4 Absatz 5 G10.

Zu Absatz 1

Sofern personenbezogene Daten so verbunden sind, dass eine Trennung nur mit unvertretbarem Aufwand möglich ist, dürfen auch die verbundenen personenbezogenen Daten übermittelt werden. Die Regelung dient dazu, einen Interessensausgleich zwischen dem Übermittlungsinteresse und den Interessen Unbeteiligter stattfinden zu lassen (vgl. dazu Bock, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 25 BVerfSchG Rn. 2) und löst den Konflikt zwischen effektiver Arbeitsweise und datenschutzrechtlichen Interessen Dritter. Die Trennung der personenbezogenen Daten von anderen Daten kann z.B. bei der Übermittlung von Asservaten durch den Bundenachrichtendienst nicht möglich sein. Hierbei kommt es gerade darauf an, das gesamte Asservat weiterzugeben, z.B. um der empfangenden Stelle gerade die Verschlüsselungsmethodik zur Kenntnis zu geben.

Es wird im Vergleich zum bisher geltenden Recht darauf verzichtet, auf die Verbindung in „Akten“ Bezug zu nehmen, um die Möglichkeit der elektronischen Datenhaltung bzw. Aktenführung auch im Gesetz abzubilden.

Zu Absatz 2

Absatz 2 schließt die Weiterverarbeitung der weiteren Daten aus, um den Interessen Dritter oder der Betroffenen Rechnung zu tragen.

Zu § 9d (Pflicht zur Übermittlung vervollständigter oder berichtigter Daten)

Zu Absatz 1

Die Vorschrift bildet die Pflichten des Bundesnachrichtendienstes u.a. aus den geltenden § 29 Absatz 15 und § 18 BNDG in Verbindung mit § 26 BVerfSchG ab. Hintergrund der Regelung ist, dass ein durch die Übermittlung der personenbezogenen Daten entstandener falscher Sachverhalt korrigiert werden muss. Dies dient im Ergebnis den Interessen des Betroffenen. Diese (Nachberichts-)Pflicht ist in anderen Bereichen des Datenschutzes so nicht anzutreffen (Bock, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 26 BVerfSchG Rn. 1).

Zu Absatz 2

Der Bundesnachrichtendienst beurteilt anhand des Gesamtvorgangs, ob auf eine Berichtigung oder Vervollständigung verzichtet werden kann. Dies kann beispielsweise der Fall sein, wenn eine unrichtige Information, z.B. zur Uhrzeit eines Gesprächs, offensichtlich keinen Einfluss auf den übermittelten Gesamtsachverhalt oder sonstige Auswirkungen für die betroffene Person nicht erkennbar sind.

Zu § 9e (Verbot der Übermittlung)

Die Vorschrift setzt die bisherigen § 18 BNDG i.V.m. § 23 BVerfSchG sowie die §§ 29 Absatz 10, 30 Absatz 6 und 8 BNDG um und bündelt die Übermittlungsverbote. Durch die Verortung im allgemeinen Teil der Übermittlungsvorschriften gilt die Regelung für alle Übermittlungen an in- und ausländische Empfänger nach dem BNDG.

Zu Absatz 1

In Absatz 1 werden die Übermittlungsverbote benannt.

Zu Nummer 1

Nach Nummer 1 hat die Übermittlung zu unterbleiben, wenn eine Abwägung ergibt, dass die schützenswerten Individualinteressen einer Person das Allgemeininteresse an der Übermittlung überwiegen. Hierbei sind insbesondere die Art der Information und ihre Erhebung zu berücksichtigen. Dieser Umstand trägt den verschiedenen Arten des Informationsaufkommens im Bundesnachrichtendienst Rechnung. Dabei ist ein besonders schutzwürdiges Interesse, welches bei der Abwägung zu berücksichtigen ist, unter anderem die Minderjährigkeit einer betroffenen Person, welche nicht von den Regelungen in den §§ 9f und 9g erfasst wird (z.B. eine 17jährige Person). In diesen Fällen ist eine Übermittlung nur unter besonderer Berücksichtigung ihrer Interessen zulässig. Ein anderes Beispiel für schutzwürdige Interessen der betroffenen Person sind Informationen zu ethnischen oder religiösen Hintergründen dieser Person, die der empfangenden Stelle nicht übermittelt werden, weil die Art der Information zu unangemessenen Folgen für die betroffene Person führen könnten.

Zu Nummer 2

Nummer 2 nennt einer Übermittlung entgegenstehende überwiegende Sicherheitsinteressen als weiteren Grund. Interessen im Sinne dieser Norm sind umfassend zu verstehen; es sind nicht nur Sicherheitsinteressen des Bundesnachrichtendienstes. Gründe nach Nummer 2 können auch Gründe des Quellen- und Methodenschutzes sein.

Zu Nummer 3

Nach Nummer 3 hat eine Übermittlung auch dann zu unterbleiben, wenn gesetzliche Weiterverarbeitungsregeln entgegenstehen. Unberührt bleiben jedoch Geheimhaltungspflichten, die sich aus untergesetzlichen Normen ergeben, insbesondere die jeweils geltende Verschlusssachenanweisung des Bundesnachrichtendienstes i.S.d. § 35 Absatz 4 Sicherheitsüberprüfungsgesetz (SÜG) sowie Regelungen des Gesetzes über die internationale Rechtshilfe in Strafsachen.

Zu Absatz 2

Im Hinblick auf Sicherheitsinteressen, auch mit Blick auf den Quellen- oder Methodenschutz, überwiegt im Fall einer dringenden Gefahr für Leib oder Leben einer Person grundsätzlich die Schutzpflicht für dieses Rechtsgut. Eine andere Wertung kann sich nur in der Abwägung gegen eine gleichgeartete Gefahr für ein gleichartiges Rechtsgut ergeben (Absatz 2 Satz 2). In einer solchen Konstellation ist das Parlamentarische Kontrollgremium zu unterrichten.

Zu Absatz 3

Dieser Absatz betrifft Übermittlungen an ausländische Stellen und entspricht den Vorgaben des Bundesverfassungsgerichts (BVerfGE 154, 152 Rn. 93 ff., 237 ff.) und dem bisherigen

§ 30 Absatz 6 BNDG. Kernelement ist eine Abwägung zwischen den schutzwürdigen Interessen der betroffenen Person und dem Interesse der Allgemeinheit an einer Übermittlung der Daten. Eine Übermittlung ist unzulässig, wenn für den Bundesnachrichtendienst erkennbar ist, dass der betroffenen Person bei der Weiterverarbeitung erhebliche Menschenrechtsverletzungen oder die Verletzung von elementaren rechtsstaatlichen Grundsätzen drohen. Der Bundesnachrichtendienst muss bei dieser Prognosebeurteilung auf die bei ihm zu der empfangenden Stelle vorhandenen Erkenntnisse und Erfahrungen mit dem Umgang von personenbezogenen Daten zurückgreifen. Im Zweifelsfall ist die Zusicherung der empfangenden Stelle für die Einhaltung eines angemessenen Schutzes der übermittelten Daten nebst einer Prognose des Bundesnachrichtendienstes, ob Anhaltspunkte, dass diese nicht eingehalten wird, von maßgeblicher Bedeutung.

Zu Absatz 4

Absatz 4 enthält für Übermittlungen an ausländische Empfänger hierzu ein besonderes Regelbeispiel für überwiegende Sicherheitsinteressen nach Absatz 1 Nummer 2.

Zu § 9f (Schutz von minderjährigen Personen bei Übermittlungen an inländische Stellen)

Zu Absatz 1

Die Übermittlung von personenbezogenen Daten von Minderjährigen unter 14 Jahren an inländische Stellen durch den Bundesnachrichtendienst sind grundsätzlich – vorbehaltlich Absatz 2 – ausgeschlossen.

Zu Absatz 2

Personenbezogene Daten von Minderjährigen unter 14 Jahren dürfen nur in den Ausnahmefällen des Absatz 2 zum Schutz der dort genannten Rechtsgüter übermittelt werden. Die Interessen von Minderjährigen ab 14 Jahren sind im Rahmen der Prüfung von Übermittlungsverboten nach § 9e besonders zu berücksichtigen und können einer Übermittlung im Einzelfall entgegenstehen (vgl. Begründung zu § 9e, Artikel 1 Nummer 5 dieses Gesetzentwurfes).

Zu § 9g (Schutz von minderjährigen Personen bei Übermittlungen an ausländische Stellen und an über- oder zwischenstaatliche Stellen)

Zu Absatz 1

Diese Regelung erhöht den Schutz von Minderjährigen, die noch nicht 16 Jahre alt sind, bei der Übermittlung von personenbezogenen Daten an ausländische Stellen oder an über- oder zwischenstaatliche Stellen. Im Vergleich zu § 9f, in dem es um die Übermittlung an inländische Stellen geht, wird hier der Schutz Minderjähriger nochmals ausgeweitet. Dabei wird berücksichtigt, dass das Schutzniveau für Minderjährige im Ausland von dem in der Bundesrepublik Deutschland abweichen kann und Minderjährige bereits frühzeitiger möglicherweise schärferen Maßnahmen ausgesetzt sein könnten.

Zu Absatz 2

Absatz 2 legt fest, dass personenbezogene Daten von Minderjährigen unter 14 Jahren nicht und ab 14 Jahren bis 15 Jahren nur in den genannten gewichtigen Ausnahmefällen übermittelt werden dürfen. Die Interessen von Minderjährigen ab 16 Jahren bei Übermittlungen an ausländische Stellen oder über- oder zwischenstaatliche Stellen sind im Rahmen der Prüfung von Übermittlungsverboten nach § 9e besonders zu berücksichtigen und können einer Übermittlung im Einzelfall entgegenstehen (vgl. Begründung zu § 9e, Artikel 1 Nummer 5 dieses Gesetzentwurfes).

ENTWURF

Zu § 9h (Übermittlung zum Schutz der betroffenen Person)

Diese Regelung wird neu eingeführt. Sie soll dem Schutz betroffener Personen in atypischen – insofern von den sonstigen Übermittlungsvorschriften, die ihrerseits den Schutz betroffener Personen vor belastenden Übermittlungen bezwecken, noch nicht zureichend abgedeckten – Fällen verbessert Rechnung tragen. Sie ist indes bei Übermittlungen einschlägig, welche die betroffenen Personen begünstigen. Der Eingriff in das Grundrecht auf Informationelle Selbstbestimmung der betroffenen Person, der durch die Datenübermittlung erfolgt, wird durch den legitimen Zweck der Erfüllung der grundrechtlichen Schutzpflichten gerechtfertigt.

Zu Absatz 1

Mit dieser Vorschrift darf der Bundesnachrichtendienst personenbezogene Daten zum Schutz der betroffenen Person übermitteln. Ein möglicher Anwendungsfall ist die Evakuierung bestimmter Personen aus einem Land, in dem ein gewaltsam herbeigeführter Regimewechsel stattgefunden hat. Dabei kann es erforderlich sind, dass der Bundesnachrichtendienst auch Personen evakuiert, die ihn bei seiner Arbeit vor Ort unterstützt haben. Wird die Evakuierung durch einen anderen Staat koordiniert, müssten auch die personenbezogenen Daten der zu evakuierenden Personen an diesen Staat, möglicherweise auch nicht öffentliche Stellen (z.B. Rotes Kreuz, Ärzte ohne Grenzen) übermittelt werden. In diesem Fall dient die Übermittlung allein dem Schutz der betroffenen Person. Kann die Einwilligung nicht oder nicht rechtzeitig eingeholt werden, wie es z.B. in einem Evakuierungsfall regelmäßig der Fall sein wird, darf auf die mutmaßliche Einwilligung der betroffenen Person bzw. der Sorgeberechtigten abgestellt werden. Insbesondere in zeitkritischen Fällen dürfte es die Regel sein, dass die Einholung einer Einwilligung nach inländischen verwaltungsrechtlichen Grundsätzen typischerweise nicht durchführbar ist.

Zu Absatz 2

Neu ist auch die Befugnis zur Übermittlung personenbezogener Daten von Minderjährigen zu deren Schutz. Dies könnte beispielsweise der Fall sein, wenn sich aus einem Bürgerkriegsland heraus eine dort verbleibende deutsche Staatsangehörige oder ein deutscher Staatsangehöriger an den Bundesnachrichtendienst wendet, damit ihre oder seine Kinder – für die ggf. eine andere oder eine weitere Person sorgeberechtigt ist – in Deutschland aufwachsen können, sich die Kinder unbegleitet auf die Flucht begeben haben und nunmehr schutzsuchend sind (vgl. z.B. Rotax, FPR 2008, 151, 152) oder die Vermittlung von Ausstiegshilfen aus einem extremistischen oder terroristischen Umfeld. In diesen Konstellationen kommt es nicht darauf an, ob die Erkenntnisse mit der mutmaßlichen Einwilligung des oder der Sorgeberechtigten erhoben wurden, denn zum Schutz des betroffenen Minderjährigen kann die Jugendhilfe auch gegen den Willen der Sorgeberechtigten Maßnahmen ergreifen (vgl. Heiß, NZFam 2015, 532). Es können hier gerade Sachverhalte zugrunde liegen, in denen das Kind oder der bzw. die Jugendliche Schutz gegenüber dem oder den Personensorgeberechtigten benötigt.

Ausreichend ist, wenn die Feststellungen des Bundesnachrichtendienstes rein tatsächlicher Natur sind.

Die Beurteilung der Minderjährigkeit einer Person richtet sich nach den Vorschriften des Bürgerlichen Gesetzbuchs.

Zu Nummer 7

Die Einfügung der Überschrift dient der Übersichtlichkeit.

Zu Nummer 8

Zu § 10a (Übermittlung von personenbezogenen Daten aus allgemein zugänglichen Quellen)

Die Regelung zur Übermittlung von personenbezogenen Daten aus allgemein öffentlichen Quellen ist neu.

Zu Absatz 1

Der Bundesnachrichtendienst setzt zur Informationsgewinnung nicht nur nachrichtendienstliche Mittel ein. Auch Informationen aus öffentlich zugänglichen Quellen werden erhoben und weiterverarbeitet. Dazu gehört die Auswertung von Fachzeitschriften, aber auch die Recherche im Internet und auf speziellen Datenbanken. Dies können auch zahlungspflichtige Angebote sein, die aber grundsätzlich allen offenstehen.

Die erhöhten Übermittlungsschwellen für mit nachrichtendienstlichen Mitteln erhobene personenbezogene Daten werden mit den weitreichenden Überwachungsbefugnissen der Nachrichtendienste begründet (BVerfG, Beschluss vom 28. September 2022, 1 BvR 2354/13, Rn. 120). Erkenntnisse aus öffentlich zugänglichen Quellen werden im Gegensatz hierzu gerade nicht durch solche Befugnisse erhoben, sondern stehen allen offen oder gegen ein Entgelt zur Verfügung, so dass eine Gleichbehandlung dieser Daten mit solchen, die mit nachrichtendienstlichen Mitteln erhoben wurden, verfassungsrechtlich nicht geboten ist. Ein Eingriff in das allgemeine Persönlichkeitsrecht in der Ausprägung als Recht auf informationelle Selbstbestimmung nach Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz ist in diesen Fällen in der Regel nicht gegeben (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07, Rn. 308).

Indes ist auch hier keine schrankenlose Übermittlungsbefugnis vorgesehen. Auch diese Übermittlungsbefugnis unterliegt – wenn auch geringeren – Schranken. Die Übermittlung muss zur Erfüllung der Aufgaben des Empfängers oder für die Aufgaben des Bundesnachrichtendienstes erforderlich sein. Mit dieser modifizierten Übermittlungsschwelle wird das Recht des Betroffenen wegen des geringeren Eingriffsgewichts hinreichend geschützt.

Zu Absatz 2

Für durch den Bundesnachrichtendienst systematisch aus allgemein zugänglichen Quellen erhobene oder gezielt zusammengeführte personenbezogene Daten zu einer Person (z.B. Nutzung der Daten für die Erstellung von Personagrammen) gelten allerdings die jeweils einschlägigen Übermittlungsvoraussetzungen in den Unterabschnitten 3 und 4. Es liegt zwar grundsätzlich kein Eingriff in das allgemeine Persönlichkeitsrecht vor, wenn eine staatliche Stelle öffentlich zugängliche Informationen erhebt (s.o.). Ein Eingriff kann allerdings gegeben sein, wenn allgemein zugängliche Informationen gezielt zusammengetragen, gespeichert gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich hieraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07, Rn. 309). Damit in solchen Fällen nicht in jedem Fall eine Einzelfallentscheidung getroffen werden muss, ob diese Voraussetzungen vorliegen, werden die in Absatz 2 genannten Daten, die im Einzelfall einen Eingriff in das Persönlichkeitsrecht darstellen können, von der Übermittlungsbefugnis nach Absatz ausgenommen.

Diese Einordnung gilt auch für die Übermittlung von Daten aus dem Ankauf z.B. von umfänglichen Werbedatenbanken und anderen Datenbanken mit vergleichbarer Eingriffsintensität. Auch bei diesen Daten handelt es sich um allgemein verfügbare Daten, die in der Regel von kommerziellen Anbietern verkauft werden. Die Erhebung und Weiterveräußerung dieser Daten durch die kommerziellen Anbieter geschieht in der Regel mit der Zustim-

mung des Nutzers, da diese Bestandteil der jeweiligen allgemeinen Geschäfts- und Nutzungsbedingungen sind. Da die Datenqualität solcher Daten jedoch mit den systematisch durch den Bundesnachrichtendienst erhobenen oder gezielt zusammengeführten Daten vergleichbar ist, entfällt die Privilegierung des Absatz 1 und die Übermittlung solcher Daten durch den Bundesnachrichtendienst richtet sich nach den Regelungen der Unterabschnitte 3 und 4.

Zu Nummer 9

Zu Unterabschnitt 3 (Übermittlung von personenbezogenen Daten aus nicht allgemein zugänglichen Quellen an inländische Stellen)

Unterabschnitt 3 enthält Regelungen für die Übermittlung von personenbezogenen Daten aus nicht allgemein zugänglichen Quellen durch den Bundesnachrichtendienst an inländische Stellen. Hierbei werden die o.a. Vorgaben des Bundesverfassungsgerichts aus den Entscheidungen vom 26. April 2022 (1 BvR 1619/17) und vom 28. September 2022 (1 BvR 2354/13) Bundesnachrichtendienst-spezifisch umgesetzt.

Personenbezogene Daten, die aus Maßnahmen der strategischen Fernmeldeaufklärung stammen, unterfallen nunmehr dem allgemeinen Übermittlungsregime. Das Bundesverfassungsgericht qualifiziert Erkenntnisse, die von Nachrichtendiensten mit nachrichtendienstlichen Mitteln erhoben wurden, generell als so schutzwürdig, dass eine Übermittlung nur zum Schutz besonders gewichtiger Rechtsgüter zulässig ist (vgl. BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 238-242; BVerfG, Beschluss vom 28. September 2022, 1 BvR 2354/13, Rn. 117-120). Eine Differenzierung nach dem Eingriffsgewicht der jeweiligen Einzelmaßnahme kommt wegen der Besonderheit nachrichtendienstlicher Aufgabenwahrnehmung nicht in Betracht (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 238). Die strategische Fernmeldeaufklärung nimmt in diesem Kontext keine Sonderrolle ein. Maßgeblich ist vielmehr allgemein - auch für Erkenntnisse, die aus Maßnahmen der strategischen Fernmeldeaufklärung erlangt wurden -, dass Daten nur dann übermittelt werden dürfen, wenn ihre Erhebung nach allgemeinen rechtsstaatlichen Anforderungen für die Übermittlungszwecke gerechtfertigt wäre (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 233). Dieser Anforderung wird nach der neueren Rechtsprechung des Gerichts durch die hohen Anforderungen an das durch die Übermittlung zu schützende Rechtsgut und - im Falle operativ tätiger Empfänger - einer qualifizierten Übermittlungsschwelle Rechnung getragen (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 231 ff.; BVerfG, Beschluss vom 28. September 2022, 1 BvR 2354/13, Rn. 124 ff.). Dadurch kann allgemein, alle Erhebungsarten einschließend, ein hoher Grundrechtsschutz sichergestellt werden.

Zu Nummer 10

Zu § 11 (Übermittlung an inländische Nachrichtendienste)

Die Regelung gestattet dem Bundesnachrichtendienst, personenbezogene Daten an andere Nachrichtendienste des Bundes oder der Länder zu übermitteln. Dies trägt dem Erfordernis des schnellen und effektiven Datenaustausches innerhalb der Nachrichtendienste Rechnung. Diese Vorschrift privilegiert die Übermittlung von personenbezogenen Daten innerhalb des Nachrichtendienstverbundes. Die Regelung unterscheidet daher auch nicht nach dem Erhebungszweck der Daten. Nachrichtendienste haben von vornherein die Aufgabe, besonders gewichtige Rechtsgüter zu schützen (ständige Rechtsprechung des Bundesverfassungsgerichts, vgl. BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 320, BVerfG, Beschluss vom 27. Mai 2020, 1 BvR 1873/13, Rn. 151). Zudem verfügen die empfangenden Nachrichtendienste – wie auch der Bundesnachrichtendienst als die übermittelnde Behörde – nicht über operative Anschlussbefugnisse; insoweit kann die Übermittlung nicht die für den Betroffenen damit verbundenen typischen eingriffsintensiven Folgen haben (BVerfG, Beschluss vom 28. September 2022, 1 BvR 2354/13, Rn. 120). Dies rechtfertigt

die hier zugrunde gelegten privilegierten Übermittlungsvoraussetzungen. Die Übermittlung muss zur Erfüllung eigener Aufgaben des Bundesnachrichtendienstes oder zur Erfüllung der Aufgaben des Übermittlungsempfängers erforderlich sein. Durch diese Hürde soll insbesondere im Rahmen des Verhältnismäßigkeitsgrundsatzes sichergestellt werden, dass nur die jeweils erforderlichen personenbezogenen Daten übermittelt werden.

Zu Nummer 11

Zu § 11a (Übermittlung an inländische Strafverfolgungsbehörden)

Der Bedarf einer Neuregelung der Übermittlungsvorschriften an Strafverfolgungsbehörden ergibt sich insbesondere aus dem Urteil des Bundesverfassungsgerichts vom 26. April 2022, 1 BvR 1619/17, Rn. 251, sowie dem Beschluss vom 28. September 2022, 1 BvR 2354/13, Rn. 136. Danach ist die Übermittlung personenbezogener Daten an Strafverfolgungsbehörden nur zum Schutz eines herausragenden öffentlichen Interesses und damit nur zur Verfolgung besonders schwerer Straftaten zulässig und erfordert eine gewisse Verdachtsverdichtung (BVerfG, Beschluss vom 28. September 2022, 1 BvR 2354/13, Rn. 137).

Den Vorgaben des Bundesverfassungsgerichts entsprechend erfolgt die nähere Konkretisierung der besonders schweren Straftaten im Rahmen eines enumerativen und abschließenden Katalogs von Straftaten, die im Zusammenhang mit dem Auftrag des Bundesnachrichtendienstes stehen. Hierdurch wird die vom Bundesverfassungsgericht geforderte Normenklarheit umgesetzt (BVerfG, Beschluss vom 28. September 2022, 1 BvR 2354/13, Rn. 144).

Dabei wurde bei den Übermittlungsvoraussetzungen das Gewicht der Straftaten berücksichtigt. Für die Bewertung der besonders schweren Straftat wurde in erster Linie der Strafrahmen in den Blick genommen (Absatz 1 Nummer 1). In Nummer 2 werden weitere besonders schwere Straftaten abschließend aufgezählt, die mit einer Freiheitsstrafe, die im Höchstmaß mit fünf Jahren bedroht sind und zu denen der Bundesnachrichtendienst im Rahmen seiner Aufklärungstätigkeit Informationen erhalten kann.

Voraussetzung für die Übermittlung ist weiter, dass für die Straftat zumindest hinreichend verdachtsbegründende Tatsachen vorliegen. Bei Übermittlungen zu bereits laufenden Strafverfahren ist dies per se der Fall. Es ist aber keine Voraussetzung, dass bereits Strafermittlungen geführt werden, folglich ist auch unmaßgeblich, in welchem Verfahrensstadium sich etwaige staatsanwaltliche oder polizeiliche Prüfungen befinden. Maßgeblich ist die Einschätzung der übermittelnden Stelle. Unschädlich ist, wenn in diese Einschätzung auch Informationen der empfangenden Stelle einbezogen werden, die von dort etwa im Rahmen der Prüfung der Übermittlungsvoraussetzungen übermittelt werden.

Zu Absatz 1

Zu Nummer 1

Der Strafrahmen (im Höchstmaß mit Freiheitsstrafe von mindestens zehn Jahren) bestimmt sich nach dem jeweiligen Strafrahmen des Delikts. Maßgebend für die Deliktsnatur ist alleine der gesetzlich festgelegte abstrakte Strafrahmen. Danach kommt es für die Einordnung weder auf die Berücksichtigung von Erschwerungs- oder Milderungsgründen im Einzelfall, sondern alleine darauf an, welche Höchstfreiheitsstrafe der jeweilige Tatbestand vorsieht.

Zu Nummer 2

Nummer 2 erfasst einzelne Straftaten mit einem Strafrahmen im Höchstmaß mit Freiheitsstrafe von fünf Jahren, die einen Bezug zur Aufgabe des Bundesnachrichtendienstes zur Sammlung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer

Bedeutung für die Bundesrepublik Deutschland sind, aufweisen können. Für die Bestimmung der besonders schweren Straftaten gibt der Strafrahmen einen ersten Anhaltspunkt, kann aber nicht alleiniger Maßstab sein. Das Bundesverfassungsgericht hat hierfür noch keine abschließende Entscheidung getroffen, wie bei Straftaten mit einem Strafrahmen im Höchstmaß mit Freiheitsstrafe von fünf Jahren umzugehen ist. Einbezogen werden muss auch die Gesamtumstände einer Tatbegehung, um das herausragende öffentliche Interesse zu bestimmen. Bei Nummer 2 ist als zusätzliche Voraussetzung ein Bezug zu Aufgaben des Bundesnachrichtendienstes erforderlich, d.h. die Straftaten müssen im Einzelfall eine außen- und sicherheitspolitische Bedeutung aufweisen. Das herausragende öffentliche Interesse an der Strafverfolgung liegt daher bei den in Nummer 2 aufgezählten Straftaten vor.

Zu Nummer 2

Zu Buchstabe a

Zu Buchstabe a

Buchstabe aa) enthält Straftaten nach dem ersten und zweiten Abschnitt des Besonderen Teils des Strafgesetzbuches. Diese Straftaten richten sich direkt gegen den Bestand der Bundesrepublik Deutschland bzw. gefährden unmittelbar die Sicherheit der Bundesrepublik Deutschland.

Zu Buchstabe b

Buchstabe bb) enthält Straftaten nach dem dritten und vierten Abschnitt des Besonderen Teils des Strafgesetzbuches. Diese Straftaten gefährden unmittelbar die freiheitlich demokratische Grundordnung der Bundesrepublik Deutschland.

Zu Buchstabe c

Buchstabe cc) enthält Straftaten nach dem fünften Abschnitt des Besonderen Teils des Strafgesetzbuches (Straftaten gegen die Landesverteidigung), die sich dadurch auszeichnen, dass sie zielgerichtet die Tätigkeit der Bundeswehr stören oder auf andere Weise die Sicherheit der Bundesrepublik Deutschland gefährden.

Zu Doppelbuchstabe dd

Buchstabe dd) erfasst besondere Straftaten gegen die öffentliche Ordnung. Es handelt sich um typische Straftaten, die mit Aufklärungsthemen des Bundesnachrichtendienstes in Zusammenhang stehen. 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 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.

Zu Doppelbuchstabe ee

Buchstabe ee) umfasst Straftaten gegen die sexuelle Selbstbestimmung, die oft in Zusammenhang mit illegaler Migration, Menschenhandel und Organisierter Kriminalität stehen, aber aufgrund des niedrigeren Strafrahmens nicht von Nummer 1 erfasst sind (Förderung sexueller Handlungen Minderjähriger, Zuhälterei, sexueller Missbrauch von Jugendlichen).

ENTWURF

Zu Doppelbuchstabe ff

Buchstabe ff) erfasst spezifische Alternativen von Straftaten gegen die persönliche Freiheit, die typischerweise im Zusammenhang mit illegaler Migration und Organisierter Kriminalität stehen, aber aufgrund des niedrigeren Strafrahmens nicht von Nummer 1 erfasst sind (Menschenhandel, Zwangsprostitution, Verschleppung, Entziehung Minderjähriger, Kinderhandel, Zwangsheirat).

Zu Doppelbuchstabe ff

Die Buchstaben gg) bis hh) erfassen die Straftaten der genannten Abschnitte, die im Höchstmaß mit Freiheitsstrafe von fünf Jahren bedroht sind und mit den Aufgaben des Bundesnachrichtendienstes im Zusammenhang stehen.

Zu Doppelbuchstabe ii

Buchstabe ii) erfasst den Tatbestand der Erpressung, welcher im Bereich der Cyberkriminalität einen Großteil der Fälle ausmacht. Der Bundesnachrichtendienst leistet im Verbund der Sicherheitsbehörden einen erheblichen Beitrag zur Abwehr von Cyberangriffen, da er die Befugnis und die technischen Möglichkeiten zur strategischen Erfassung internationaler Datenverkehre besitzt. Somit kann der Bundesnachrichtendienst Cyberangriffe ausgehend von informationstechnischen Strukturen im Ausland und z.B. gegen kritische Infrastrukturen in Deutschland gerichtet sind, frühzeitig erkennen. So wird vermehrt Ransomware, also ein Schadprogramm, das auf die Blockade des informationstechnischen Systems oder die Verschlüsselung der Betriebs- und Nutzerdaten abzielt, von ausländischen Akteuren eingesetzt, um Lösegeld zu erpressen. Da die Täter in der Regel eine Vielzahl von informationstechnischen Systemen oder besonders bedeutende informationstechnische Systeme angreifen, um hohe Lösegeldsummen erpressen zu können, bergen diese Fälle ein solches Gefährdungspotential, dass die Übermittlung bereits zu einzelnen Straftaten in diesem Bereich erforderlich ist.

Ebenfalls wird die Übermittlung bei tatsächlichen Anhaltspunkten der Straftat der Geldwäsche geregelt. Die Geldwäsche ist ein typisches Delikt, dass durch Mitglieder der Organisierten Kriminalität begangen wird, häufig mit Schwerpunkt im Ausland. Die Mitglieder begehen die Straftat im Inland, mit Geldern, die im Ausland durch illegale Aktivitäten im Zusammengang mit der Organisierten Kriminalität erworben wurden.

Zu Doppelbuchstabe jj

Der Buchstabe kk) umfasst bestimmte Straftaten der Urkundenfälschung, insbesondere Fälschung von amtlichen Ausweisen. Auch diese Straftaten werden häufig durch Mitglieder der Organisierten Kriminalität begangen, die den Schwerpunkt im Ausland haben und beispielsweise die Illegale Migration oder den Menschenhandel unterstützen.

Zu Doppelbuchstabe kk

Auch die Straftat der Computersabotage im Buchstaben j) ist eine der Cyberkriminalität und stehen daher im unmittelbaren Zusammenhang mit den Aufgaben des Bundesnachrichtendienstes (vgl. Begründung zu Buchstabe g)). Umfasst sind die Fälle der Störung der Datenverarbeitung auf Betriebe, Unternehmen oder Behörden von wesentlicher Bedeutung sowie der besonders schwerere Fall (gewerbsmäßige Begehung, Gefährdung von KRITIS oder Beeinträchtigung der Sicherheit der Bundesrepublik Deutschland).

Zu Buchstabe l bis °oo

Die Buchstaben gg) bis hh) erfassen die Straftaten der genannten Abschnitte, die im Höchstmaß mit Freiheitsstrafe von fünf Jahren bedroht sind und mit den Aufgaben des Bundesnachrichtendienstes im Zusammenhang stehen.

Zu Buchstabe e

Auch bei Straftaten nach dem Außenwirtschaftsgesetz können über den Einzelfall hinaus schwerwiegende Gefährdungen innen- und außenpolitische Belange der Bundesrepublik Deutschland auftreten. Diese Straftaten sind aufgrund ihrer besonderen Relevanz auch nach dem bisher geltenden BNDG in § 29 Absatz 3 und § 38 Absatz 3 aufgenommen.

Zu Buchstabe f

Im Rahmen der Aufklärungstätigkeit des Bundesnachrichtendienstes zur Proliferation, zum Handel mit Kriegswaffen sowie zur Organisierten Kriminalität können auch Informationen zu Straftaten aus dem Kriegswaffenkontrollgesetz anfallen.

Zu Buchstabe o

Mit Buchstaben d werden Straftaten im Zusammenhang mit Waffen aufgenommen, die im Rahmen des organisierten Waffenhandels, der Aufklärung von Proliferationssachverhalten und der Organisierte Kriminalität auftreten.

Zu Buchstabe pe

Der im Aufenthaltsgesetz geregelte Straftatbestand des Einschleusens von Ausländern, steht im Zusammenhang mit den vom Bundesnachrichtendienst aufzuklärenden Gefährdungen durch illegale Migration und ist eine typische Schleusungskriminalität.

Zu Buchstabe q

Mit Buchstaben f werden Straftaten im Zusammenhang mit Waffen aufgenommen, die im Rahmen des organisierten Waffenhandels, der Aufklärung von Proliferationssachverhalten und der Organisierte Kriminalität auftreten.

Zu Buchstabe g

Im Zusammenhang mit der Wirtschaftsspionage können Straftaten gegen die deutsche Wirtschaft im Sinne des § 23 Geschäftsgeheimnisgesetzes begangen werden, zu denen eine Übermittlung an Strafverfolgungsbehörden geboten ist.

Zu Absatz 2

Im Zusammenhang mit sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten ist die Übermittlung zum Zweck der Verfolgung weiterer, über Absatz 1 hinausgehender Straftaten zulässig. Hierbei ist zu berücksichtigen, dass insbesondere Spionageakte nicht isolierte Einzeltaten sind, sondern ein spezifischen Gefährdungspotenzial weiterer solcher Taten gegen die Bundesrepublik Deutschland erwarten lassen. Wegen der Zeitenwende bedarf es des angestrebten Informationsaustausches.

Zu Absatz 3

Absatz 3 regelt die Fälle, in denen eine Übermittlungspflicht des Bundesnachrichtendienstes an Strafverfolgungsbehörden besteht. Die diesbezügliche bisherige Regelung verwies

ENTWURF

auf § 20 BVerfSchG, welcher mit Beschluss des Bundesverfassungsgerichts vom 28. September 2022, 1 BvR 2354/13, für verfassungswidrig erklärt wurde. Die jetzige Regelung zählt die jeweiligen Straftaten normenklar auf, jeweils beschränkt auf Straftaten, die im Höchstmaß mindestens mit Freiheitsstrafe von fünf Jahren bedroht sind.

Zu § 11b (Übermittlung an inländische öffentliche Stellen)

Das Bundesverfassungsgericht fordert für die Übermittlung von mit nachrichtendienstlichen Mitteln erhobenen personenbezogenen Daten an Gefahrenabwehrbehörden, dass diese dem Schutz eines besonders gewichtigen Rechtsguts dient, für das wenigstens eine hinreichend konkretisierte Gefahr besteht (Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 235).

Der Bundesnachrichtendienst übermittelt auch an Behörden, deren Aufgaben auch die Gefahrenabwehr ist. Entsprechend der verfassungsrechtlichen Gebotenheit setzen daher Übermittlungen an inländische öffentliche Stellen mit Ausnahme der Nachrichtendienste und der Bundeswehr grundsätzlich die vom Bundesverfassungsgericht geforderten Übermittlungsschwellen voraus.

Zu Absatz 1

Grundsätzliche Voraussetzung für Übermittlungen an inländische öffentliche Stellen ist das Vorliegen einer konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut.

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 zugrunde liegenden 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“ (BVerfGE 141, 220, 272). In der Folge hat das Bundesverfassungsgericht diese Rechtsprechung weiter konsolidiert und auch auf nachrichtendienstliche Sachverhalte angewendet (BVerfGE 154, 152, 266, 269; BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 245 ff., 261; BVerfG, Beschluss vom 28. September 2022, 1 BvR 2354/13, Rn. 132 ff.). Diese Rechtsprechung wurde schließlich von den Fachgerichten aufgegriffen und weiterentwickelt (vgl. nur BGHSt 66, 1 ff.; 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.

Der jüngeren Rechtsprechung des Bundesverfassungsgerichts zum Sicherheitsrecht lassen sich Anhaltspunkte für eine verfassungsrechtlich angeleitete Systematisierung von Rechtsgütern entnehmen. So zählt das Bundesverfassungsgericht in mittlerweile gefestigter Rechtsprechung zum Kreis der „besonders gewichtigen Rechtsgüter“ (die teilweise auch

als „überragend wichtige“, „hochrangige“ oder „Rechtsgüter von herausragendem öffentlichem Interesse Gewicht“ bezeichnet werden) 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, 254 f.; 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, die Übermittlung rechtfertigen. Eine abschließende Benennung der besonders gewichtigen Rechtsgüter ist damit 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 Subjekten und solchen des Völkerrechts eine systemische Bedeutung zu. Diese Bedeutung wird in den Nummern 1 bis 11 für die Tätigkeitsbereiche des Rechtsgüterschutzes, zu denen der Bundesnachrichtendienst Erkenntnisse beitragen kann, weiter konturiert.

Die genannten Rechtsgüter können jeweils durch verschiedene Bedrohungen berührt sein.

Zu Nummer 1

Leib, Leben und Freiheit der Person sind die unverzichtbaren Grundlagen jeder individuellen Existenz und zählen unbestritten zu den besonders gewichtigen Rechtsgütern. Die Regelung ist nicht auf eine Gefährdung deutscher Staatsangehöriger begrenzt. Der Schutz von Leib, Leben und Freiheit natürlicher Personen muss eine der vordringlichsten Aufgaben aller staatlichen Stellen sein (Artikel 1 Absatz 1 Satz 2 GG). Das Rechtsgut kann durch verschiedene Bedrohungen berührt sein, z.B. durch Terrorismus oder Extremismus, Organisierte Kriminalität wie beispielsweise im Bereich des Menschhandels oder auch durch grenzüberschreitende Verbreitung von Kriegswaffen.

Zu Nummer 2

Der Bestand und die Sicherheit des Bundes oder eines Landes betrifft die Existenz der Völkerrechtssubjekte und die unverzichtbaren Rahmenbedingungen für ein Leben des Staatsvolkes in Freiheit und Sicherheit. Beides ist konstitutiv für die Bundesrepublik Deutschland. Dieses Rechtsgut betrifft beispielsweise auch die Funktionsfähigkeit des Bundesnachrichtendienstes als Teil der staatlichen Sicherheitsstruktur. Beispiele für mögliche Bedrohungen sind hybride Bedrohungen, Bedrohungen durch die Entwicklung disruptiver Technologien, gewichtige Bedrohungen der Sicherheit des Weltraums aus der militärischen und nachrichtendienstlichen Nutzung von Weltraumsystemen sowie sicherheitsgefährdende oder geheimdienstliche Aktivitäten fremder Nachrichtendienste.

Auch die Organisierte Kriminalität (z.B. internationaler Rauschgifthandel, internationale Geldwäsche) kann dem besonders gewichtigen Rechtsgut des Bestandes und der Sicherheit des Bundes oder eines Landes unterfallen, da das gezielte Unterlaufen staatlicher Strukturen geeignet ist, die Funktionsfähigkeit des Bundes oder eines Landes zu gefährden.

Zu Nummer 3

In einer zunehmend globalisierten Welt sind die Existenzbedingungen einzelner Staaten in hohem Maße miteinander verschränkt und voneinander abhängig und werden als zentrale

gemeinsame Interessen durch Bündnisse und supranationale Einrichtungen wahrgenommen. Der Bestand und die Sicherheit verbündeter Staaten sowie der Bündnisse selbst besitzt 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.

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 insbesondere durch hybride Bedrohungen (z.B. die systematische, zielgerichtete Verbreitung von Fake-News und Desinformationen) beeinträchtigt sein. Unter hybriden Bedrohungen ist die interessensgeleitete Einflussnahme auf Staaten oder Staatenverbünde, insbesondere zentrale Akteure, deren Netzwerke und die von ihnen genutzten Instrumente zu verstehen. Ziel ist die Störung des gesamtgesellschaftlichen und politischen Gefüges eines Staates durch die Anwendung konventioneller und nicht konventioneller Mittel unter gezielter Verschleierung der eigenen Urheberschaft, in deren Folge eine möglicherweise einsetzende Destabilisierung der Gesellschaft von anderen Staaten für eigene, insbesondere machtpolitische Zwecke genutzt werden kann.

Zu Nummer 5

Die Bundeswehr und die ihr verbündeten Streitkräfte sichern die physische Existenz der Bundesrepublik Deutschland und ihrer Bündnispartner im Verteidigungsfall sowie höchstrangige Rechtsgüter wie Leib, Leben und Freiheit von Personen im Rahmen von Auslandseinsätzen oder im Rahmen der Landes- oder Bündnisverteidigung. Auch dieses Rechtsgut kann durch verschiedene Bedrohungen berührt werden, z.B. durch wehrtechnische Technologien und -programme oder krisenhafte Entwicklungen im Ausland.

Befindet sich die Bundeswehr in einem Einsatz oder steht ein solcher unmittelbar bevor, ist in der Regel vom Vorliegen einer konkretisierten Gefahr für dieses Rechtsgut auszugehen.

Zu Nummer 6

Die Sicherheits- und Arbeitsfähigkeit staatlicher Einrichtungen und anderer wesentlichen Infrastrukturen Deutschlands im Sinne der Nummer 6, von Mitgliedstaaten sowie Einrichtungen der Europäischen Union, des Nordatlantikvertrages und der Europäischen Freihandelsassoziation ist ein besonders gewichtiges Rechtsgut im Sinne der Rechtsprechung des Bundesverfassungsgerichts. Jeder Staat benötigt zur Herstellung und Aufrechterhaltung seiner Funktionsfähigkeit wesentliche Einrichtungen, die daher eine staatstragende Funktion besitzen. Hierzu gehören neben staatlichen Einrichtungen, wie etwa die Verkehrsnetze, auch solche, die von privater Seite betrieben werden, wie zum Beispiel Kritische Infrastrukturen auf dem Gebiet der Energie- oder Wasserversorgung. Es handelt sich hier typischerweise um Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist. Häufig ginge mit einer Störung der Funktionsfähigkeit auch eine Gefahr für Leib und Leben einer Person oder den Bestand oder die Sicherheit des Bundes oder eines Landes einher. Auch dieses Rechtsgut kann durch verschiedene Bedrohungen berührt werden, z.B. durch die Beeinträchtigung der Versorgung mit Rohstoffen, Energien oder kritischen Technologien, durch Terrorismus oder Extremismus, durch den Handel und die Verbreitung von wehrtechnischen Technologien und Programmen, aufkommende disruptive Technologien einschließlich Technologien der Künstlichen Intelligenz, durch internationale kriminelle, terroristischen oder staatlichen Angriffen, insbesondere mittels Schadprogrammen auf die Vertraulichkeit, Integrität oder Verfügbarkeit von informationstechnischen Systemen.

Zu 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, die den unmittelbaren Grenzübertritt betreffen, sondern auch Fragen, die den Aufenthalt im Bundesgebiet betreffen. Auch hier können verschiedene Bedrohungen zu Beeinträchtigungen führen, z.B. Auswirkungen durch illegale Migration und Menschenhandel sowie sonstige Bevölkerungs- und Migrationsbewegungen und Migrationspotenziale.

Zu Nummer 8

Die Sicherheit von informationstechnischen Systemen, d.h. die 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), aber beispielsweise auch für die Bedrohung durch weiträumig orchestrierte Cyberangriffe oder -kampagnen, 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. Derartige 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 vor dem Hintergrund der Aufklärung von internationalen terroristischen, staatlichen oder weiträumig orchestrierten Angriffen als besonders gewichtiges Rechtsgut anzusehen ist. Cyberangriffen ist die Gefahr des Eintritts von Großschadenslagen immanent. Angriffe auf, ggf. sogar eine Störung der Verfügbarkeit von informationstechnischen Systemen, können insbesondere bei einer Vielzahl betroffener informationstechnischen Systeme oder der Betroffenheit von Kritischen Infrastrukturen erhebliche Auswirkungen auf die öffentliche Sicherheit und Ordnung, bis hin zu einer Bedrohung von Leib und Leben oder dem Bestand 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. Es können verschiedene Bedrohungen auf das Rechtsgut einwirken, z.B. kann ein Angriff mittels Schadprogrammen vor dem Hintergrund des Terrorismus oder Extremismus, wie auch vor dem Hintergrund der Organisierten Kriminalität, oder nachrichtendienstlichen Aktivitäten ausländischer staatlich gesteuerter Akteure erfolgen.

Zu Nummer 9

Der Umstand, dass die Bundesrepublik Deutschland einer der weltweit führenden Wirtschafts- und Wissenschaftsstandorte ist, gehört zum ihrem ökonomischen Wesenskern. Ein Leben in Freiheit und Sicherheit bedarf der wirtschaftlichen Absicherung. Zugleich ist diese

Grundlage durch Wirtschaftsspionage und andere Formen der Einflussnahme zunehmend Angriffen ausgesetzt. Bei der wesentlichen Funktionsfähigkeit des inländischen und europäischen Wirtschafts- und Wissenschaftsstandortes handelt es sich daher um ein Rechtsgut im Sinne der Rechtsprechung des Bundesverfassungsgerichts. Gefährdungen des europäischen Wirtschafts- und Wissenschaftsstandortes und diesem zugeordneter Wirtschaftssubjekte können immensen volkswirtschaftlichen Schaden begründen und in der Folge eine Gefährdung der Sicherheit von Mitgliedstaaten der Europäischen Union bedeuten. Das Rechtsgut umfasst u.a. den Schutz der deutschen Wirtschaft vor unerlaubtem Außenwirtschaftsverkehr mit Waren und technischen Unterstützungsleistungen in Fällen von erheblicher Bedeutung (Beispiel: §§ 17, 18 AWG).

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.

Verschiedene Bedrohungen können auf dieses Rechtsgut wirken, z.B. Beeinträchtigungen der Geldwertstabilität im Euro-Währungsraum oder nachrichtendienstliche Aktivitäten ausländischer staatlicher Akteure, dies gerade auch mit Blick auf den Wissenschaftsstandort Deutschland. 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 kritische Infrastruktur in eine Abhängigkeit zu zwingen.

Zu Nummer 10

Ein Wesenselement staatlicher Souveränität ist das Vertreten eigener Interessen gegenüber anderen Völkerrechtssubjekten. Auf die Befähigung der Regierung hierzu zielt der Auftrag des Bundesnachrichtendienstes (vgl. Gusy, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 1 BNDG Rn. 28: „Es geht um die Aufklärung der Bedingungen eigener Handlungsmöglichkeiten der Bundesrepublik wie auch möglicher Handlungen Anderer.“). Das Bundesverfassungsgericht hat das überragende Gewicht dieses Rechtsguts anerkannt (BVerfGE 154, 152, 248 ff.). Die Herausforderungen der globalisierten, multipolaren Welt, die von neuen Gestaltungsmächten wie beispielsweise China und Russland zunehmend bestimmt werden, schaffen neue Rahmenbedingungen und Gefährdungspotenziale durch Destabilisierung politischer und wirtschaftlicher Systeme. Der Schutz der außenpolitischen Handlungsfähigkeit der Bundesrepublik Deutschland ist damit ein besonders gewichtiges Rechtsgut im Auftragskatalog des Bundesnachrichtendienstes als einzigem Auslandsnachrichtendienst der Bundesrepublik (zivil und mit der militärischen Auslandsaufklärung betraut), insbesondere als spezifische Ausprägung des Rechtguts des Bestands und der Sicherheit der Bundesrepublik Deutschland wie auch mit Blick auf Leib, Leben und Freiheit von Personen sowie auch der Sachen von bedeutendem Wert für die Allgemeinheit.

Zu Nummer 11

Das Bundesverfassungsgericht hat 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 BundesVerfassungsgericht dabei wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen (siehe hier Nummer 5). Die Subsumtion unter Nummer 11 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). Im Hinblick auf Nummer 6 kommt der Regelung eine Auffangfunktion zu, die zum Beispiel bedeutende Gegenstände von kulturellem Wert betreffen kann.

Zu Absatz 1 Satz 3

Satz 3 eröffnet die Möglichkeit zur Datenübermittlung, wenn dies in anderen Rechtsvorschriften des Bundesrechts für den Bundesnachrichtendienst vorgesehen ist.

Verschiedene Gesetze sehen die Möglichkeit vor, dass inländische öffentliche Stellen in einem Verwaltungsverfahren unter den jeweils gesetzlich geregelten Voraussetzungen beim Bundesnachrichtendienst anfragen können, ob zu dem Antragsteller nachrichtendienstliche Erkenntnisse vorliegen. Die Norm stellt klar, dass der Bundesnachrichtendienst die Anfragen der Behörden beantworten darf.

Die Festlegung weiterer Übermittlungsvoraussetzungen im BNDG für diese Fälle ist nicht geboten. Oftmals liegen den Anfragen an den Bundesnachrichtendienst Verwaltungsverfahren zugrunde, denen ein Antrag der betroffenen Person vorausgeht. Ein solcher Antrag bzw. die darin enthaltene Einwilligung hat häufig bereits eine den Eingriff ausschließende Wirkung. In Konstellationen, in denen dies nicht der Fall ist, wie z.B. bei Zuverlässigkeitsüberprüfungen, reduziert die Einwilligung der betroffenen Person zumindest die Eingriffsintensität der Datenverarbeitung (vgl. BayVGH GSZ 2022, 196 ff.). In solchen Fällen kann die betroffene Person aufgrund ihres Antrags oder ihrer Zustimmung absehen, dass und nach welchen Kriterien ihr Antrag geprüft wird. Gleichfalls gerechtfertigt ist in der Folge eine Datenübermittlung, mit der als actus contrarius die Aufhebung einer antragsgebundenen Erlaubnis vorbereitet wird.

Eine Übermittlungsbefugnis wie in Absatz 1 Satz 3 vorgesehen ist darüber hinaus auch in Konstellationen relevant, in denen der Bundesnachrichtendienst zur Erfüllung seiner Aufgaben durch die Übermittlung der personenbezogenen Daten weitere Informationen zu der betroffenen Person generieren möchte.

Beispielhaft kann hier eine Übermittlung von personenbezogenen Daten zum Abgleich mit den im Fluggastdaten-Informationssystem gespeicherten Daten nach § 4 Absatz 5 des Fluggastdatengesetzes genannt werden. Gleiches gilt für die Übermittlung von personenbezogenen Daten nach dem Aufenthaltsgesetz zur Unterstützung der Ausländerbehörden bei der Prüfung, ob Versagungsgründe oder sonstige Sicherheitsbedenken nach § 73 Absatz 3 Aufenthaltsgesetz (AufenthG) vorliegen. Übermittlungen nach dieser Norm umfassen ebenso Datenübermittlungen des Bundesnachrichtendienstes im Rahmen von Konsultationsverfahren nach §§ 73 Absatz 3, 3a, 3b AufenthG sowie die Übermittlung von Behördenerklärungen beispielsweise im Sinne von § 99 der Verwaltungsgerichtsordnung, § 4 Verwaltungsverfahrensgesetz oder § 256 Strafprozessordnung. Erfasst sind ferner Datenübermittlungen im Rahmen des Verfahrens nach Artikel 36 der Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen. Zu nennen sind auch Übermittlungen nach § 5 Absatz 2 Satz 2 Sanktionsdurchführungsgesetz.

Zu Absatz 2

Nach Maßgabe der Rechtsprechung des Bundesverfassungsgerichts dürfen mit nachrichtendienstlichen Mitteln erhobene personenbezogene Daten an Behörden mit operativen Anschlussbefugnissen nur übermittelt werden, wenn tatsächliche Anhaltspunkte für eine

konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut vorliegen. Das Erfordernis dieser strengen Voraussetzungen folgt daraus, dass operative Befugnisse besonders tief in Grundrechte betroffener Personen eingreifen. Vorbild für diese Systembildung ist das Gefahren abwehrende, Kausalverläufe unterbrechende und unmittelbar mit Zwangsmitteln durchsetzbare polizeiliche Handeln.

Die Vielfalt der zwischenbehördlichen Kooperationen lässt sich jedoch nicht ohne weiteres in den vom Bundesverfassungsgericht aufgezeigten Dualismus operativer und nicht-operativer Behörden einordnen. So nehmen zahlreiche Sicherheitsbehörden, die über operative Befugnisse verfügen, zugleich auch Aufgaben wahr, die keine unmittelbare Außenwirkung entfalten. Auch der Begriff der operativen Anschlussbefugnisse selbst ist unscharf. Im hiesigen Kontext wird er in einem weiten Sinne verstanden, wonach ein operatives Tätigwerden die Qualität besitzt, Grundrechte über den mit der Datenverarbeitung verbundenen informationellen Eingriff hinaus zu beeinträchtigen.

Dieses weite, grundrechtsschonende Verständnis macht umgekehrt Ausnahmen für besondere Konstellationen erforderlich, in denen solche über die reine Datenverarbeitung hinausgehenden Folgeeingriffe weitgehend ausgeschlossen sind oder jedenfalls nicht dieselbe hohe Eingriffsintensität aufweisen wie polizeiliches Handeln. Alle diese Ausnahmen orientieren sich an praktisch hoch relevanten Bedarfen der Zusammenarbeit des Bundesnachrichtendienstes mit anderen inländischen öffentlichen Stellen. Dementsprechend ist in den geregelten Ausnahmen der Nachweis des Vorliegens einer konkretisierten Gefahr für eine Übermittlung von personenbezogenen Daten durch den Bundesnachrichtendienst entbehrlich. Den im Katalog abgebildeten Konstellationen ist dabei gemein, dass ein besonders gewichtiges Rechtsgut zu einem erhöhten Risiko durch eine nachrichtendienstspezifische Gefährdungslage ausgesetzt ist, die sich indes regelmäßig noch im Vorfeld einer konkretisierten Gefahr befindet. Es handelt sich um eine Aufzählung von spezifischen Belangen, in denen die Datenübermittlungen unabhängig von einer konkretisierten Gefahr zugelassen werden. Die in dieser Norm vorgesehenen Datenübermittlungen dienen Zwecken, hinsichtlich derer der Schutz der besonders gewichtigen Rechtsgüter es notwendig macht, der informationellen Zusammenarbeit des Bundesnachrichtendienstes mit den zuständigen – teilweise auch operativ handelnden Behörden – auch verfassungsrechtlich eine Sonderstellung zuzugestehen.

Die in Absatz 2 vorgesehenen Datenübermittlungen gründen jeweils in der besonderen Nähe des Übermittlungsanlasses zum gesetzlichen Auftrag des Bundesnachrichtendienstes, insbesondere auch vor dem Hintergrund des Alleinstellungsmerkmals als einzigem Auslandsnachrichtendienst der Bundesrepublik Deutschland. Die Informationen des Bundesnachrichtendienstes über das Ausland tragen zur Wirksamkeit der Maßnahmen anderer inländischer Behörden bei. Die Mitwirkung des Bundesnachrichtendienstes bei der Vorbereitung der Maßnahmen anderer Behörden gehört zu seinem gesetzlichen Auftrag. Die Beteiligung des Bundesnachrichtendienstes und die Übermittlung von Informationen über das Ausland an inländische Behörden gehört in den Fällen des Absatz 2 nicht nur im Einzelfall, sondern generell zu seinem Auftrag. Absatz 2 stellt somit spezifische Belange fest, die ein besonderes Näheverhältnis zu seinen Aufgaben aufweisen und deren Erfüllung innerhalb der Sicherheitsarchitektur der Bundesrepublik Deutschland auch von der Tätigkeit, den Informationen und Erkenntnissen des Bundesnachrichtendienstes abhängig ist.

Der Gesetzgeber berücksichtigt auch in Bezug auf die in Absatz 2 aufgeführten spezifischen Belange, dass die Übermittlungen von mit nachrichtendienstlichen Mitteln erhobenen Daten auf besonders gewichtige Rechtsgüter, mithin auf öffentliche Interessen von herausragender Bedeutung beschränkt sind.

Darüber hinaus ist eine Nutzung der übermittelten personenbezogenen Daten zur operativen Anwendung unmittelbaren Zwanges ausgeschlossen. Es handelt sich dabei um eine Folgenbegrenzung, die die abgesenkten Übermittlungsschwellen des § 11c Absatz 2 zulässt. Übermittlungsvoraussetzung ist hier keine bereits konkretisierte Gefahr, vielmehr ist

die Übermittlung hier durch spezifische Belange veranlasst, auf die zum vorbeugenden Rechtsgüterschutz bereits im Vorfeld einer konkretisierten Gefahr einzuwirken ist. Der Ausschluss der Nutzung der übermittelten Daten zur operativen Anwendung unmittelbaren Zwangs wahrt dabei die Verhältnismäßigkeit dieser auf spezifische Belange ausgerichteten Übermittlungsschwelle. Hierdurch bleiben hoheitliche Anschlussmaßnahmen mit unmittelbarer Außenwirkung zu Lasten der betroffenen Person möglich (und sind womöglich auch intendiert), bei der Gewichtung dieser Folgen ist hier aber wesentlich, dass in den Konstellationen des Absatz 2, in denen eine Anschlussmaßnahme droht, vorheriger Rechtsschutz effektiv verfügbar ist und die Verwaltung in einer Verwaltungsstreitsache die Darlegungs- und Beweislast für den Eingriffstatbestand trägt. Bei der operativen, unmittelbar situationsveranlassten Zwangsausübung drohen hingegen irreversible Schäden, die auch mit der Genugtuungs- und zukunftsgerichteten Vorbeugefunktion einer Fortsetzungsfeststellungsklage nicht auszugleichen sind. Dies unterscheidet die situationsbedingt operative Anwendung unmittelbaren Zwangs von einem Verwaltungsvollstreckungsverfahren, das auch bei einer Übermittlung nach § 11c Absatz 2 BNDG zur Durchsetzung eines Verwaltungsaktes möglich bleibt (vgl. dazu Unterreitmeier, GSZ 2023, 34/35).

Zu Nummer 1

Als Auslandsnachrichtendienst ist der Bundesnachrichtendienst zudem Informationsdienstleister für andere staatliche Stellen, die für die Erfüllung ihrer Aufgaben auf Hintergrundinformationen über Auslandssachverhalte angewiesen sind. Der Bundesnachrichtendienst übermittelt Informationen an inländische öffentliche Stellen in Form von Berichterstattungen für die Vervollständigung der Lagebilder der empfangenden Stelle oder zum Zweck des Abgleichs der Lagebilder sowie zur Sensibilisierung inländischer öffentlicher Stellen (z.B. im Vorfeld von Veranstaltungen, beim Missbrauch von Fluchtbewegungen, Vernetzungsabsichten und -bemühungen von nachrichtendienstlich und polizeilich relevanten Gruppierungen (z.B. Internationale Organisierte Kriminalität), zum Erkennen von nachrichtendienstlich und polizeilich relevanten Kennverhältnissen und Netzwerken, Aufbau neuer und Weiterentwicklung nachrichtendienstlich und polizeirelevanter Strukturen, Verwicklung von Personen in Geldwäsche, Sanktionsumgehungen, Proliferations- oder Terrorfinanzierung), die sich noch im Vorfeld einer konkretisierten Gefahr befinden. Diese Hintergrundinformationen tragen zur besseren Einordnung und Interpretation eigener Erkenntnisse der anderen Stellen bei. Sie finden beispielweise Verwendung bei der Erstellung polizeilicher Lagebilder, Analysen und Berichte (vgl. BVerfGE 154, 152, Rn. 212, 223 ff.). Zum Beispiel im Vorfeld von Großveranstaltungen, die heute typischerweise auch Reisebewegungen aus dem Ausland beinhalten. Gegenstand solcher Übermittlungen sind überwiegend Strukturerkenntnisse, im Einzelfall kann aber auch die Übermittlung personenbezogener Daten erforderlich sein, um eine sachgerechte Lagebeurteilung zu ermöglichen, was eine Rechtsgrundlage erforderlich macht. Ein Beispielsfall für die ausnahmsweise Übermittlung von Daten zu bestimmten Personen kann etwa die Anreise eines bekannten ausländischen Agitators zu einer rechtsextremistischen Großveranstaltung sein. Solche Informationen sind jedoch nicht unmittelbar Grundlage operativer Maßnahmen, sondern ermöglichen die sachgerechte Einordnung einer Sachlage durch die empfangende Stelle selbst. Bei den übermittelten Informationen handelt es sich um nachrichtendienstliche Erkenntnisse, d.h. vom Bundesnachrichtendienst ausgewertete Informationen.

Wichtige Lagebilder, die eine Zusammenarbeit im Bund-Länder-Verhältnis unterstützen sollen, entstehen beispielsweise im Bundeskriminalamt (z.B. Bundeslagebilder Menschenhandel, Organisierte Kriminalität, Cyberkriminalität). In diesem Zusammenhang ergänzen die nachrichtendienstlichen Milieu- und Strukturerkenntnisse ein Gesamtlagebild, ohne dass daraus konkrete Folgemaßnahmen für Betroffene resultieren. Ohne die Übermittlung von Informationen im Vorfeld einer konkretisierten Gefahr in diesen Ausnahmefällen entstünden risikobehaftete Lücken in Lagebildern der jeweils zuständigen inländischen öffentlichen Stellen. Ebenso kann sich aus diesen Übermittlungen für den Empfänger die Erforderlichkeit ergeben, die Schwerpunkte der eigenen Arbeit aufgrund erkennbarer Veränderungen in den betreffenden Themenfeldern anzupassen.

Dazu müssen Informationen unabhängig vom Vorliegen einer konkretisierten Gefahr übermittelt werden dürfen. Um den o.g. Anforderungen des Bundesverfassungsgerichts zu entsprechen, wird in diesen Fällen eine Übermittlung unter der Voraussetzung zugelassen, dass die Informationen nicht zur operativen Anwendung unmittelbaren Zwangs genutzt werden dürfen (vgl. zutreffend Unterreitmeier, GSZ 34, 37; Gärditz, GSZ 2022, 161, 164 f.). Sollte die empfangende Stelle die Daten zur operativen Anwendung unmittelbaren Zwangs nutzen wollen, handelt es sich nicht mehr um eine Übermittlung zum Zweck der Erstellung eines Lagebildes und ist damit nicht zulässig.

Der im Regelfall geringe Anteil personenbezogener Daten bei solchen Übermittlungen und die Distanz zu operativen Maßnahmen reduziert die Eingriffstiefe. Im Zusammenspiel mit der Bedeutung der Übermittlung der Informationen rechtfertigt dies die hier festgelegte Ausnahme.

Zu Nummer 2

Eine strategische Einflussnahme auf und Ausspähung deutscher Interessen durch fremde Mächte erfolgt nicht nur gegenüber staatlichen Einrichtungen, Kritischer Infrastruktur oder wesentlichen Funktionsträgern des deutschen Wirtschafts- und Wissenschaftsstandorts. Zunehmend sind von solchen Aktivitäten auch andere Einrichtungen, die dem Schutz der deutschen Hoheitsgewalt unterstehen, wie zum Beispiel Glaubensgemeinschaften, Entwickler neuer Technologien oder Hochschulen betroffen. In solchen Konstellationen ist es ein Gebot hoheitlicher Fürsorge, die betroffenen Stellen von dem Versuch ihrer Infiltrierung in Kenntnis zu setzen, damit sie selbst Vorkehrungen treffen und Abwehrmaßnahmen ergreifen können. Die Norm erlaubt die Datenübermittlung an die zuständigen inländischen öffentlichen Stellen zum Zweck der Unterrichtung der betroffenen Einrichtungen. In diesen Fällen agiert der deutsche Staat nicht operativ gegenüber den fremden Akteuren und hinter der Infiltration steht zudem eine fremde Staatsgewalt oder vergleichbare Macht („durch fremde Mächte“). Beides rechtfertigt eine Ausnahme von dem Erfordernis des Vorliegens einer konkretisierten Gefahr.

So gibt der Bundesnachrichtendienst beispielsweise im Rahmen der Initiative Wirtschaftsschutz insbesondere an das Bundeskriminalamt, Landeskriminalämter und Landespolizeien Informationen über die Risiken und Bedrohungen für deutsche Unternehmen oder die Wirtschaft im Allgemeinen weiter. Dies erfolgt u.a. in den Themenfeldern Wirtschaftsspionage, illegale oder illegitime Einflussnahme ausländischer Akteure auf deutsche Unternehmen (z.B. als Element hybrider Aktivitäten). Im Bereich Wissenschaftstransfer (d.h. der Abfluss von Wissen aus Universitäten und Forschungseinrichtungen, insb. im Dual Use-Bereich) informiert der Bundesnachrichtendienst z.B. Universitäten und unterrichtet das Bundesministerium für Bildung und Forschung.

Zu Nummer 3

Mitteilungen über Umstände, die für die Einhaltung von Beschränkungen des Außenwirtschaftsverkehrs von Bedeutung sind, dienen der Sensibilisierung von Teilnehmern des Außenwirtschaftsverkehrs und stellen eine präventive Maßnahme der Proliferationsbekämpfung dar, die auch dem Schutz betroffener Unternehmen dient (vgl. Huber, in: Schenke/Graulich/Ruthig, Sicherheitsgesetze des Bundes, 2. Aufl. 2019, § 7 Artikel 10-Gesetz Rn. 9; zum Hintergrund BT-Drs. 14/5655 S. 21). Eine vergleichbare Regelung, die eine Übermittlung von aus Maßnahmen der strategischen Aufklärung internationaler Fernmeldeverkehre erlangten Daten an das Bundesamt für Ausfuhrkontrolle erlaubt, fand sich bisher bereits in § 7 Absatz 3 G 10. Der dieser Regelung zugrundeliegende Gedanke wird nunmehr auf alle Erhebungsmethoden des Bundesnachrichtendienstes ausgeweitet, weil diese Erkenntnisse über proliferationsrelevante Sachverhalte nicht nur aus Maßnahmen der strategischen Fernmeldeaufklärung stammen können. Die Norm erlaubt die Datenübermittlung an die zuständigen inländischen öffentlichen Stellen (insbesondere an das Bundesamt für Ausfuhrkontrolle) zum Zweck der Unterrichtung der betroffenen Unternehmen.

Damit gehen unmittelbar keine operativen hoheitlichen Maßnahmen gegenüber den betroffenen Unternehmen einher, so dass ist eine Ausnahme vom strengen Übermittlungsregime geboten ist.

Zu Nummer 4

Die Sicherheit der Informationstechnologie, d.h. die Verfügbarkeit, Integrität und Vertraulichkeit informationstechnischer Systeme, besitzt für den Wirtschafts- und Wissenschaftsstandort Deutschland sowie für den Erhalt der freiheitlichen demokratischen Grundordnung überragende systemische Bedeutung. Dies gebietet es, Maßnahmen zum Schutz der informationstechnischen Infrastruktur auch schon unterhalb der Schwelle einer konkretisierten Gefahr zu ergreifen. So ist es Aufgabe des Bundesnachrichtendienstes, Bestrebungen oder Tätigkeiten, die die Sicherheit in der Informationstechnologie beeinträchtigen, aufzuklären und dabei mitzuwirken, die Verwundbarkeit in diesem Bereich zu mindern und die Resilienz zu stärken. Die Ausnahmevorschrift ermöglicht es, entsprechende Erkenntnisse an die zuständigen inländischen öffentlichen Stellen (etwa das Bundesamt für die Sicherheit in der Informationstechnik) frühzeitig zu übermitteln, welche ihrerseits notwendige Maßnahmen ergreifen, insbesondere betroffene Betreiber von informationstechnischen Systemen von Bedrohungslagen in Kenntnis setzen können. Internationale terroristische, staatliche oder weiträumig orchestrierte Angriffe auf informationstechnische Systeme oder Angriffsstrukturen bergen in sich bereits ein solch immenses Gefährdungspotential, dass die Verarbeitung und auch die Übermittlung von Daten zu laufenden Cyberangriffen und -kampagnen bereits in einem frühen Stadium zum Zeitpunkt der Erstentdeckung geboten ist. Je frühzeitiger Erkenntnisse gewonnen und ausgetauscht werden, desto mehr Schäden (z.B. Vertraulichkeitsverlust, Datenveränderung, Verfügbarkeitsstörungen, Zerstörung) können im weiteren Verlauf bestenfalls abgewendet werden. Würde mit der Übermittlung der Erkenntnisse gewartet werden, bis durch den Angriff eine bestimmte Schadensschwelle überschritten ist, bedeutete dies die bewusste Hinnahme erhöhter Schäden (z.B. im Fall von Ransomwareangriffen auf kritische Infrastrukturen deren völlige Ausschaltung auf unbestimmte Zeit).

Die Nationale Sicherheitsstrategie der Bundesregierung für die Bundesrepublik Deutschland legt dazu fest, dass die Aufklärungs- und Frühwarnsysteme der Nachrichtendienste gestärkt werden sollen. Zum Ziel der gesamtstaatlichen Resilienz und Aufrechterhaltung der staatlichen Reaktions- und Wehrhaftigkeit sollen alle maßgeblichen Akteure zu einem ganzheitlichen Cyberlagebild beitragen (vgl. Nationale Sicherheitsstrategie, Stand Juni 2023, Seite 61).

Bei Erkennen eines laufenden Cyberangriffs auf Basis technischer Merkmale in der eigenen Erfassung des Bundesnachrichtendienstes oder durch den Hinweis eines Dritten ist im Regelfall zunächst nur die IP-Adresse des Opfers erkennbar und ggf. das verwendete Eindringmittel. Dies bedeutet, es ist zunächst nicht klar erkennbar, von wem die Angriffe ausgehen, gegen wen sie sich richten und was das Ziel des Cyberangriffs ist. Die weitere Aufklärung erfolgt dabei typischerweise auch mittels des Informationsaustausches mit anderen Stellen, um laufenden Cyberangriffen möglichst effektiv und zeitgerecht begegnen zu können. In Anbetracht des den Angriffen innwohnenden Gefährdungspotentials erscheint es sogar naheliegend, in derartigen Cyberangriffen bereits in einem sehr frühen Stadium des Erkenntnisgewinns eine konkretisierte Gefahr für ein gewichtiges Rechtsgut zu sehen, auch wenn in einem frühen Stadium der Aufklärung möglicherweise noch nicht eindeutig erkennbar ist, dass es sich um einen Fall von herausgehobener Bedeutung für die Allgemeinheit handelt (vgl. dazu auch die Begründung zu Absatz 1 Nummer 8). Absatz 2 Nummer 6 dient insofern insbesondere dazu, die Übermittlungsvoraussetzungen im Fall von Cyberangriffen eindeutig zu regeln, für den Anwender eine eindeutige Handlungs- und Rechtssicherheit herzustellen und so die frühzeitige Übermittlungsmöglichkeit beim Erkennen von Cyberbedrohungen sicherzustellen.

Daten, die im Rahmen der Aufklärung von Cyberangriffen erhoben werden, werden im Rahmen des § 11b in der Regel an folgende inländische öffentliche Stellen übermittelt: Bundeskriminalamt, insbesondere zum Austausch zur Vorgehensweise der Cyberakteure und zur Opferfläche, Bundes- und Landespolizeien, Bundesamt für Sicherheit in der Informationstechnik, Bundesamt für Katastrophenschutz und Bevölkerungshilfe sowie im Rahmen des Nationalen Cyber Abwehrzentrums.

Zu Nummer 5

Zur Vorbereitung oder Durchführung eigener Maßnahmen darf der Bundesnachrichtendienst im Vorfeld konkretisierter Gefahrenlagen personenbezogene Daten an inländische öffentliche Stellen übermitteln. Bei eigenen Maßnahmen des Bundesnachrichtendienstes kann es sich auch um solche handeln, die gemeinsam mit anderen inländischen öffentlichen Stellen vorbereitet werden und bei denen im konkreten Fall die Übermittlung personenbezogener Daten erforderlich ist. Eine Datenübermittlung kann etwa auch erforderlich sein, um festzustellen, ob und in welchem Umfang eine technische Unterstützungsleistung erfolgen kann.

Zu Nummer 6

Die Norm ist Ausdruck der besonderen Zusammenarbeit des Bundesnachrichtendienstes als einzigem Auslandsnachrichtendienst der Bundesrepublik Deutschland, dem somit auch die Funktion eines mit der militärischen Aufklärung betrauten Auslandsnachrichtendienstes zukommt. 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 wichtigen Informationen, insbesondere zur Landes- und Bündnisverteidigung sowie zu Einsätzen im Ausland, aber auch zu sonstigen Aufgabenwahrnehmungen der Bundeswehr.

Bei der Wahrnehmung ihrer Aufgaben, insbesondere bei der Vorbereitung und Durchführung der Landes- oder Bündnisverteidigung sowie von Auslandseinsätzen, wird die Bundeswehr 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, zum Schutz hochrangiger Rechtsgüter tätig. Der Bundesnachrichtendienst darf daher auch ohne Vorliegen einer hinreichend konkretisierten Gefahr personenbezogene Daten an die Bundeswehr übermitteln, wenn tatsächliche Anhaltspunkte vorliegen, dass die Übermittlung zur Vorbereitung und Durchführung der Landes- oder Bündnisverteidigung sowie von Auslandseinsätzen erforderlich ist. Hiervon sind insbesondere Übermittlungen an die Bundeswehr erfasst, die im Vorfeld von eventuellen, nicht auszuschließenden Einsätzen erforderlich sind.

Die Vorschriften des § 24 BNDG bleiben unberührt.

Zu Nummer 7

Übermittlungen nach Nummer 7 liegt das auch für die vorausgegangenen Nummern geltende Kriterium der Reduktion des Gefährdungspotenzials durch ein Einwirken auf gefährdungssteigernde Risikofaktoren im Aufgabenbereich des Bundesnachrichtendienstes zugrunde. Es liegt dabei ein qualitativ mit den vorausgegangenen Nummern vergleichbarer besonderer Risikosachverhalt vor, der ein administratives Einwirken konkret erfordert. Die in den Nummern 1 bis 6 für den Bundesnachrichtendienst gebildeten Fallgruppen werden in Nummer 7 durch den Bezug auf die Gefahrenbereiche des § 19 Absatz 4 ergänzt. Der Bezug auf die in § 19 Absatz 4 genannten Gefahrenbereiche stellt sicher, dass es sich bei Nummer 7 um Übermittlungen handelt, die in einem besonderen Näheverhältnis zu den Kernaufgaben des Bundesnachrichtendienstes stehen und durch einen den Nummern 1 bis 6 vergleichbaren besonderen Risikosachverhalt gefährdet sind. Durch § 11b Absatz 2 Satz

2 ist überdies sichergestellt, dass die übermittelten personenbezogenen Daten nicht zur operativen Anwendung unmittelbaren Zwangs genutzt werden dürfen.

Zu Absatz 3

Die Bundeswehr ist insbesondere im Rahmen der „Force Protection“ bei Auslandseinsätzen und deren Vorbereitung, aber auch in anderen Fällen auf valide und schnelle Datenübermittlung angewiesen. Diese kann in vielen Fällen nur durch eine automatisierte Datenübermittlung gewährleistet werden. Der Bundesnachrichtendienst darf Daten aus der technischen Aufklärung auch automatisiert an die Bundeswehr übermitteln, wenn sie auf Grundlage von Suchbegriffen erhoben wurden, die strategischen Aufklärungsmaßnahmen nach § 19 Absatz 4 Nummer 1 Buchstabe a – zur Landes- oder Bündnisverteidigung sowie Einsätzen der Bundeswehr oder verbündeter Streitkräfte im Ausland, Buchstabe b – zu krisenhaften Entwicklungen im Ausland und deren Auswirkungen, Buchstabe e – zur Organisierten Kriminalität in ihrer Ausprägung Piraterie, Buchstabe f – zur internationalen Verbreitung von Kriegswaffen, Buchstabe g – zu Gefährdungen kritischer Infrastruktur, Buchstabe h – zu hybriden Bedrohungen und Nummer 2 Buchstabe a – Leib, Leben oder Freiheit, Buchstabe b – Bestand oder Sicherheit des Bundes oder eines Landes sowie Buchstabe c – Bestand oder Sicherheit von Einrichtungen der EU, EFTA oder NATO oder Bestand oder Sicherheit eines Mitgliedsstaates der EU, EFTA oder NATO, zugeordnet sind.

Zu Nummer 1

Die Neuaufnahme des Buchstaben b ermöglicht die automatisierte Übermittlung personenbezogener Daten, welche auf der Grundlage von Suchbegriffen zu dem Gefahrenbereich krisenhafte Entwicklungen im Ausland und deren Auswirkungen erhoben wurden, da auch die Bundeswehr personenbezogene Daten zur Krisenfrüherkennung benötigt. Durch die Erweiterung der bestehenden Regelung um den Buchstaben e können personenbezogene Daten zu Piraterie an die Bundeswehr übermittelt werden, wenn es um Gebiete geht, in denen (noch) kein bestehender Einsatz der Bundeswehr gegeben ist. Buchstabe f ermöglicht Angaben zu legalen und illegalen Rüstungstransporten außerhalb bestehender Einsätze der Marine sowie in Gebieten, die an definierte Einsatzgebiete angrenzen. Die Erweiterung um den Buchstaben g ermöglicht die automatisierte Übermittlung von personenbezogenen Daten zum Gefahrenbereich Kritischer Infrastrukturen. Da hybride Bedrohungen auch den Aufgabenbereich der Bundeswehr betreffen, findet auch insoweit eine Erweiterung statt.

Die Notwendigkeit der Aufnahme des § 19 Absatz 4 Nummer 2 b und c erfolgt mit Blick auf die Aufgabe der Bundeswehr, für den Schutz und den Bestand der Bundesrepublik Deutschland und ihrer Bündnispartner sowie gemeinsamer Institutionen einzutreten.

Soweit die Bundeswehr dem Bundesnachrichtendienst zur Datenerhebung konkrete Suchbegriffe zur Verfügung gestellt hat, erfolgt auch die Prüfung dieser Suchbegriffe durch den Bundesnachrichtendienst vor deren Verwendung automatisiert.

Zu Nummer 2

Die automatisierte Übermittlung von personenbezogenen Daten erstreckt sich auch auf solche, die im Rahmen von individuellen Aufklärungsmaßnahmen nach § 34 Absatz 1 mit Bezug zu den in § 19 Absatz 4 Nummer 1 Buchstabe a, b, f, g, h oder Buchstabe e in der Ausprägung Piraterie sowie Nummer 2 Buchstabe a, b oder c genannten Gefahren erhoben wurden.

Zu Absatz 4

Es wird die Übermittlung der Daten geregelt, die zum Zweck der politischen Unterrichtung erhoben wurden, d.h. es handelt sich um eine gesonderte Regelung für Daten aus der strategischen Ausland-Fernmeldeaufklärung nach § 19 BNDG und Daten aus dem Eingriff in informationstechnische Systeme von Ausländern im Ausland nach § 34 BNDG. Die Erhebungsvoraussetzungen knüpfen hier an den Zweck der Nutzung der Daten an. Die Regelung in Absatz 3 eröffnet als Ausnahmevorschrift die Möglichkeit, Daten die lediglich zum Zweck der politischen Unterrichtung erhoben wurden, dennoch an inländische öffentliche Stellen zu übermitteln.

Eine solche Übermittlung scheidet grundsätzlich aus, da die personenbezogenen Daten allein zur politischen Information der Bundesregierung erhoben wurden. Ausnahmsweise ist eine Übermittlung dieser personenbezogenen Daten an andere Stellen möglich, wenn eine unmittelbar bevorstehende Gefahr für die in dem Absatz aufgezählten Schutzgüter von höchster Gewichtigkeit abgewendet werden soll. Die verfassungsrechtliche Unbedenklichkeit der Ausnahmevorschrift ergibt sich aus dem Urteil des Bundesverfassungsgerichts, das eine solche Verwendung ausdrücklich als zulässig ansieht (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 228).

Zu Absatz 5

Absatz 4 regelt die Übermittlungspflicht des Bundesnachrichtendienstes an inländische öffentliche Stellen. Liegen tatsächliche Anhaltspunkte vor, dass die Übermittlung zu Abwehr einer unmittelbar bevorstehenden Gefahr für ein besonders gewichtiges Rechtsgut erforderlich ist, muss der Bundesnachrichtendienst die entsprechenden personenbezogenen Daten an die zuständige inländische öffentliche Stelle übermitteln.

Der bestehende § 18 Absatz 1 BVerfSchG (Übermittlungspflicht an das Bundesamt für Verfassungsschutz) wurde nicht in das BNDG übernommen. Es besteht daher kein Bedarf der Kodifizierung einer Übermittlungspflicht für den Bundesnachrichtendienst an das Bundesamt für Verfassungsschutz im BNDG. Die Übermittlungspflicht an das Bundesamt für den Militärischen Abschirmdienst wird in § 10 MADG geregelt. Im Interesse der Normenklarheit bedarf es auch hier keiner zusätzlichen Regelung im BNDG.

Die Regelungen des Allgemeinen Teils der Übermittlungen gelten auch bei einer Übermittlungspflicht.

Zu § 11c (Übermittlung an nicht öffentliche inländische Stellen)

Zu Absatz 1

Die Übermittlung von personenbezogenen Daten an nicht öffentliche inländische Stellen stellt eine Ausnahme dar. Die materiellen und formellen Übermittlungshürden berücksichtigen dies, und sind entsprechend hoch.

Die Nummer 5 wurde im Vergleich zur bisher geltenden Regelung ergänzt. Die Bedeutung der Cyberangriffe und -kampagnen und deren Schadenspotential wächst stetig. So ist es Aufgabe des Bundesnachrichtendienstes, Bestrebungen oder Tätigkeiten, die die Sicherheit in der Informationstechnologie beeinträchtigen, aufzuklären und dabei mitzuwirken, die Verwundbarkeit in diesem Bereich zu mindern und die Resilienz zu stärken. Beim Erkennen eines laufenden Cyberangriffs – hier können zunächst nur Zeitstempel, Opferadresse, Muster von Schadprogrammen oder Eindringmittel erkennbar sein - müssen so frühzeitig wie möglich Informationen weitergegeben und die weitere Aufklärung angestrebt werden, um mögliche Schäden (Vertraulichkeitsverlust, Datenveränderung, Zerstörung) möglicherweise letztlich abwenden zu können. Cyberangriffe bergen in sich ein derart großes Schadenspotential, welches eine frühzeitige Übermittlung von Daten zur weiteren Aufklärung

rechtfertigt (vgl. dazu auch die Begründung zu § 11c Absatz 2 Nummer 5). Dabei ist auch die Übermittlung von – möglicherweise auch – personenbezogenen Daten an nicht öffentliche inländische Stellen geboten. Denn erlangt der Bundesnachrichtendienst nachrichtendienstliche Informationen über Cybervorfälle bei z.B. Unternehmen oder Behörden, bedarf dieser Sachverhalt der weiteren Abklärung auch mit nicht öffentlichen Stellen. Insbesondere ist zur notwendigen weiteren Verdichtung von Informationen zu einer Cyberbedrohung die Übermittlung technischer Indikatoren zwingend erforderlich. Durch einen bilateralen Austausch mit inländischen Unternehmen (z.B. mit dem betroffenen Unternehmen selbst oder mit Cybersicherheitsdienstleistern) werden über diesen Weg weitere nützliche und notwendige Informationen erlangt, um das Cyberlagebild zu verdichten und die eigenen Erkenntnisse anzureichern sowie zur Sachverhaltsaufklärung und ggf. Schadensbeseitigung beizutragen.

In formeller Hinsicht ist nach Satz 2 eine vorherige Zustimmung durch die Präsidentin oder den Präsidenten des Bundesnachrichtendienstes oder deren oder dessen Vertretung einzuholen. Im Eilfall (Gefahr im Verzug) kann die Übermittlung ohne vorherige Zustimmung erfolgen, diese ist allerdings unverzüglich nachzuholen. Erfolgt letztlich keine Zustimmung zur Datenübermittlung, ist die empfangende Stelle zur unverzüglichen Löschung der Daten aufzufordern.

Zu Absatz 2

Um dem besonderen Schutzbedürfnis der Betroffenen Rechnung zu tragen, ist eine Unterrichtungspflicht an das Bundeskanzleramt vorgesehen.

Zu Absatz 3

Auf die Ausführungen zu § 11c Absatz 3 wird verwiesen. Die Aufnahme der Nummer 2 stellt eine Erweiterung gegenüber den bisherigen Regelungen dar. Private Unternehmen sind insbesondere auch für den Betrieb von kritischer Infrastruktur zuständig, eine Übermittlung bei Gefährdung dieser Infrastruktur ist daher erforderlich. Die Gefährdungslage nimmt insbesondere durch Cyberangriffe zu, war die Ergänzung erforderlich macht.

Zu Absatz 4

Dieser Absatz regelt einen Sonderfall der Übermittlung im Kontext einer Anfrage. Auch Anfragen des Bundesnachrichtendienstes, in denen er einer anderen Stelle personenbezogene Daten übermittelt, um sich zu erkundigen, ob zu dieser Person Informationen vorliegen, stellen eine Übermittlung dar.

Absatz 4 gestattet ausnahmsweise eine Datenübermittlung an andere inländische Stellen über die Vorgaben in Absatz 1 hinaus, wenn diesen die Daten bereits bekannt sind und der Bundesnachrichtendienst mit der Anfrage eine Vervollständigung oder Konkretisierung seiner Daten erreichen möchte. Da der anderen inländischen Stelle in diesem Fall durch die Übermittlung keine zusätzlichen personenbezogenen Daten bekannt werden, sind die datenschutzrechtlichen Auswirkungen für die betroffenen Personen gering.

Zu § 11d (Übermittlung von personenbezogenen Daten aus einer Vertraulichkeitsbeziehung an inländische Stellen)

Die Regelung schützt besonders sensible Daten, die Journalistinnen und Journalisten, Rechtsanwältinnen und Rechtsanwälten oder Geistlichen in ihrer Funktion als Seelsorger anvertraut wurden und die ausnahmsweise nach § 21 BNDG im Rahmen von Maßnahmen der technischen Aufklärung erhoben wurden. Hierdurch soll sichergestellt werden, dass die Schutzfunktion des § 53 StPO in Bezug auf die benannten Personengruppen nicht unterlaufen wird. Anders als im Strafprozess gilt im aufklärenden Vorfeldbereich der Nachrichtendienste nicht der Maßstab des Strengbeweises.

Daher ist eine Ausnahmeregelung auch im Hinblick auf gegebenenfalls zu veranlassende gefahrenabwehrrechtliche oder strafprozessuale Maßnahmen grundsätzlich möglich. Die Frage der Verwertbarkeit solcher Erkenntnisse ist hiervon zu unterscheiden und obliegt primär den Strafverfolgungsbehörden.

Zu Absatz 1

Die derzeit geltende materielle Schwelle wird dahingehend erhöht, dass die Übermittlung zur Abwendung einer konkretisierten Gefahr für die abschließend aufgezählten Rechtsgüter erforderlich sein muss.

Zu Absatz 2 und 3

Der Unabhängige Kontrollrat prüft vor der Übermittlung das Vorliegen der Voraussetzungen nach Absatz 1. Die Möglichkeit der Übermittlung nach vorläufiger Bestätigung der Rechtmäßigkeit durch ein Mitglied des Unabhängigen Kontrollrats ist vorgesehen, wenn die Gefahr besteht, dass das Ziel der Übermittlung durch die Verzögerung aufgrund des zusätzlichen Verfahrens ansonsten vereitelt oder wesentlich erschwert wird.

Sofern eine Übermittlung nach vorläufiger Bestätigung der Rechtmäßigkeit durch ein Mitglied des Unabhängigen Kontrollrats an den Empfänger übersandt wurde und im Anschluss durch den Unabhängigen Kontrollrat für rechtswidrig erklärt wird, ist der Empfänger durch den Bundesnachrichtendienst aufzufordern, die übermittelten Daten unwiederbringlich zu löschen.

Zu Unterabschnitt 4 (Übermittlung von personenbezogenen Daten aus nicht allgemein zugänglichen Quellen an ausländische Stellen sowie an über- oder zwischenstaatliche Stellen)

Die Regelungen ermöglichen dem Bundesnachrichtendienst einen Austausch mit ausländischen Nachrichtendiensten und anderen ausländischen öffentlichen Stellen, sofern diese nachrichtendienstliche oder ähnlich gelagerte, sicherheitliche Aufgaben wahrnehmen. Unter ausländischen öffentlichen Stellen im Sinne dieses Gesetzes sind ausländische Dienststellen zu verstehen, die zu einer für den Schutz der nationalen Sicherheit im Empfängerland verantwortlichen Verwaltung gehören.

In einem wechselseitig bestehenden, von gemeinsamen oder zumindest miteinander verbundenen Sicherheitsinteressen gekennzeichneten nachrichtendienstlichen Arbeitsumfeld ist die Berücksichtigung von Interessen des ausländischen Partners häufig Bedingung dafür, dass der Bundesnachrichtendienst auch seinerseits Informationen erhält. Daher sind Datenübermittlungen an ausländische öffentliche Stellen und über- oder zwischenstaatliche Stellen zur Erfüllung der gesetzlichen Aufgaben des Bundesnachrichtendienstes regelmäßig erforderlich, um im Gegenzug von diesen nachrichtendienstlich relevante Informationen zu erhalten.

Dieser Austausch nachrichtendienstlich erlangter personenbezogener Daten ist vor dem Hintergrund begrenzter finanzieller und personeller Ressourcen ein unverzichtbarer Bestandteil der Tätigkeit des Bundesnachrichtendienstes. Zudem werden durch den Austausch Synergieeffekte in der internationalen Zusammenarbeit genutzt, ohne die der Bundesnachrichtendienst viele Themen nicht in der für die angemessene Aufgabenerfüllung erforderlichen Intensität und Tiefe bearbeiten könnte. In verfassungsrechtlicher Hinsicht kann eine internationale Zusammenarbeit insofern an die internationale Offenheit des Grundgesetzes anknüpfen.

Zu § 11e (Übermittlung an ausländische öffentliche Stellen und an über- oder zwischenstaatliche Stellen)

Der Bundesnachrichtendienst arbeitet zur Aufgabenerfüllung auch mit ausländischen öffentlichen Stellen zusammen und übermittelt in diesem Zusammenhang auch Daten an diese Stellen. Ansprechpartner für den Bundesnachrichtendienst im Ausland sind in der Regel öffentliche Stellen, die auch nachrichtendienstliche Befugnisse wahrnehmen. Das Bundesverfassungsgericht verlangt in mittlerweile gefestigter Rechtsprechung, dass bei einer Übermittlung personenbezogener Daten an ausländische Stellen dieselben materiellen Schwellen einzuhalten sind, wie bei einer Übermittlung an inländische Stellen (BVerfGE 141, 220, 343; BVerfGE 154, 152 Rn. 232; BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 261). Diese Vorgabe stellt den Gesetzgeber vor Herausforderungen, denn die für das Regelungsregime des deutschen Verfassungsrechts geltenden Maßstäbe lassen sich nicht ohne weiteres auf ausländische Rechtsordnungen übertragen. Das Bundesverfassungsgericht hat jedoch die Problematik der Verschiedenheit der aufeinandertreffenden Rechtsordnungen erkannt und gebilligt, diesem Umstand bei der Ausgestaltung der einzelnen Ermächtigungen Rechnung zu tragen (BVerfGE 141, 220, 344; BVerfGE 154, 152 Rn. 232; BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 263).

Zu Absatz 1

Die Übermittlung von Daten an ausländische oder über- oder zwischenstaatliche Strafverfolgungsbehörden nimmt auf den Straftatenkatalog des § 11b Absatz 1 Bezug. Allerdings hängt insbesondere die Bestimmung besonders schwerer Straftaten und besonders gewichtiger Rechtsgüter maßgeblich von souveränen Entscheidungen des jeweiligen ausländischen Gesetzgebers und dem dortigen Regelungskontext ab. In besonderem Maße gilt dies für die Frage, welche Rechtsgüter in welchem Maße durch das Steuerungsinstrument des Strafrechts geschützt werden. Namentlich das System der Strafrahmen unterscheidet sich in ausländischen Staaten erheblich vom deutschen. Das Bundesverfassungsgericht hat anerkannt, dass das (formelle und materielle) Strafrecht wie auch das Polizeirecht in hohem Maße von nationalen Besonderheiten geprägt sind (vgl. BVerfGE 123, 267, 359 ff.). Insofern stellt Absatz 1 auf in Art und Schwere vergleichbare Straftaten ab. Da sich die mit der Breite und Vielfalt der Beziehungen zu anderen Staaten einhergehende Heterogenität der jeweiligen staatstragenden Grundsätze gesetzgebungstechnisch weder abschließend noch exemplarisch abbilden lässt, verfolgt der gegenständliche Entwurf den Ansatz einer eher abstrakt-generellen Regelung. Danach müssen die für die empfangenden ausländischen öffentlichen Stellen den Anlass der Übermittlung bildenden Straftaten ihrer Art und Schwere nach vergleichbar mit den für inländische öffentliche Stellen maßgeblichen besonders schweren Straftaten sein. Für die Rechtsanwendung bedeutet dies, dass zum Beispiel der Strafrahmen einer Straftat nach ausländischem Recht im Kontext des dortigen Strafrahmensystems am oberen Ende der zeitigen Freiheitsstrafen liegen müsste (in Deutschland: im Höchstmaß mindestens über fünf Jahre). Auch das zu schützende Rechtsgut müsste vergleichbar sein. Das würde es zum Beispiel von vornherein - ungeachtet der ohnehin erforderlichen Vergewisserung über den rechtsstaatlichen Mindeststandard, vgl. § 9e - ausschließen, Daten an andere Staaten zur Verfolgung von bloßen Äußerungsdelikten (etwa Beleidigung des Staatsoberhaupts) zu übermitteln, da Äußerungsdelikte in Deutschland der Strafdrohung nach keine besonders schweren Straftaten sind.

Zu Absatz 2

Absatz 2 bestimmt die grundsätzlichen Voraussetzungen für die Übermittlung von Daten an ausländische öffentliche oder über- oder zwischenstaatliche Stellen. Entsprechend der Inlandsregelung muss als Übermittlungsvoraussetzung auch hier eine konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut vorliegen. D.h. eine Übermittlung an ausländische öffentliche Stellen kann auch zum Schutz von Rechtsgütern nach der Verfasstheit der Bundesrepublik Deutschland erfolgen. Das ist etwa der Fall, wenn der Schutz eines in

§ 11c Absatz 2 genannten Rechtsguts die Einbindung anderer Staaten erfordert. In Nummer 2 ist als weiteres besonders gewichtiges Rechtsgut auch die Sicherheit des Empfängerstaates aufgeführt und entspricht damit der bisherigen Regelung in § 30 Absatz 3 Nummer 2 BNDG. Insbesondere bei der Übertragung der für das deutsche Verfassungsrecht geltenden Maßstab bei der Bestimmung besonders gewichtiger Rechtsgüter hängt dies maßgeblich von souveränen Entscheidungen des jeweiligen ausländischen Gesetzgebers und dem dortigen Regelungskontext ab. Auch die Definition von besonders gewichtigen Rechtsgütern unterscheidet sich im Ausland - abgesehen von einem unscharfen völkergewohnheitsrechtlich konsentierten Mindeststandard - erheblich vom deutschen. Beispielsweise kommt in Staaten an den Außengrenzen des Schengenraums der Grenzsicherung naturgemäß ein noch höheres Gewicht zu als in den innenliegenden Staaten. Umgekehrt ist etwa der Bestand und Umfang der freiheitlichen demokratischen Grundordnung stark historisch und national geprägt und wird nicht von allen Staaten, mit denen die Bundesrepublik Deutschland kooperiert, geteilt. Derzeit unterhält der Bundesnachrichtendienst Kooperationen mit einer Vielzahl ausländischer Nachrichtendienste in mehr als 160 Staaten (Kahl, in: Dietrich et al. [Hrsg.], Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, S. 153 „über 450 ausländische Nachrichtendienste“). Auch hier muss der Verschiedenheit der aufeinandertreffenden Rechtsordnungen bei der Ausgestaltung der Ermächtigungen Rechnung getragen werden. Auch hier lassen sich die mit der Breite und Vielfalt der Beziehungen zu anderen Staaten einhergehende Heterogenität der jeweiligen staatstragenden Grundsätze gesetzgebungstechnisch weder abschließend noch exemplarisch abbilden, es wird hier auf die bereits bestehende Formulierung der Sicherheit des Empfängerstaates abgestellt.

Zu Absatz 3

Um den Gleichlauf mit den Übermittlungsregelungen im Inland herzustellen, in denen dem Informationsaustausch zwischen Nachrichtendiensten eine Sonderstellung zukommt, sowie den Bedarfen der internationalen Zusammenarbeit im Bereich der Nachrichtendienste nachzukommen, muss die Übermittlung nach Absatz 3 zum Schutz eines besonders gewichtigen Rechtsgutes mithin für ein überragend wichtiges Interesse erforderlich sein: Der Nachweis des Vorliegens einer konkretisierten Gefahrenlage ist jedoch entbehrlich, eine Übermittlung ist auch im Vorfeld einer konkretisierten Gefahrenlage möglich.

Die Übertragung der verfassungsgerichtlichen Vorgaben auf Auslandskooperationen berücksichtigt insbesondere, dass ausländische Sicherheitsarchitekturen in anderer Weise strukturiert sind als die deutsche. So ist das Trennungsgebot in seinen verschiedenen Dimensionen einerseits ein grundlegendes Ordnungselement für die deutsche Sicherheitsarchitektur, andererseits aber auch ein historisch bedingtes deutsches Spezifikum. Eine große Zahl ausländischer Nachrichtendienste verfügt über Zwangsbefugnisse, die sehr unterschiedlich ausgeprägt sein können. Der systembildende Anspruch des Bundesverfassungsgerichts knüpft gerade an diese Besonderheit des deutschen Rechts an und differenziert zwischen empfangenden Stellen mit und ohne „operative Anschlussbefugnisse“. Das Bundesverfassungsgericht anerkennt andererseits zurecht, dass eine Übermittlung an Staaten, in denen die Sicherheitsbehörden nicht in gleicher Weise organisatorisch getrennt sind, nicht ausgeschlossen ist (BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 267). Eine strenge Unterscheidung aller empfangenden Stellen entlang des Kriteriums „operativer Befugnisse“ ist für ausländische Stellen gesetzgeberisch nicht zu leisten. Eine solche Einteilung wäre - auch angesichts sich ändernder Zuständigkeiten und Befugnisse bei den ausländischen Stellen - weder praktikabel noch im Sinne eines wirksamen Grundrechts- und Rechtsgüterschutzes zielführend, da eine klare Zuordnung häufig nicht möglich ist. Hintergrund des hier in Absatz 3 verfolgten Ansatzes ist das im Bereich des internationalen nachrichtendienstlichen Informationsaustauschs etablierte Prinzip der Gegenseitigkeit („do ut des“-Prinzip) und des gegenseitigen Vertrauens (sog. „Third Party Rule“). Die Wirksamkeit dieses informellen Prinzips, ohne das ein internationaler nachrichtendienstlicher Austausch unmöglich ist, steht der eines formellen, mit rechtsstaatlichen Sicherungen versehe-

nen Verfahrens nicht nach. Brüche dieses Prinzips werden in der sog. Intelligence Community unmittelbar mit der Einschränkung oder dem Ausschluss weiteren Informationsaustausches sanktioniert, mit für den betroffenen Staat weitreichenden Folgen. Vor diesem Hintergrund ist es gerechtfertigt, eine Übermittlung zum Schutz von besonders gewichtigen Rechtsgütern zuzulassen, wenn eine Verwendung der Daten durch die empfangende Stelle für Folgemaßnahmen mit unmittelbarer Außenwirkung gegenüber Dritten ausgeschlossen ist. Materiell entspricht das einer Verwendung durch Stellen ohne operative Anschlussbefugnisse im Inland.

Um dem Umstand zu begegnen, dass Übermittlungen ins Ausland ein besonders hohes Risiko für betroffene Personen bergen, weil Rechtsschutz gegen hoheitliche Maßnahmen dort möglicherweise nur eingeschränkt verfügbar ist und staatliche Stellen mitunter noch weitreichendere Eingriffsbefugnisse besitzen, wird der Schutz der von der Übermittlung betroffenen Personen gegenüber der Regelung in § 11c Absatz 2 Satz 2 ausgeweitet auf den Ausschluss der Verwendung der Daten für Folgemaßnahmen mit unmittelbarer Außenwirkung. Anders als § 11c Absatz 2 Satz 2 findet sich hier also eine weiter gefasste Folgenbegrenzung. Erfasst sind hier sämtliche hoheitliche Anschlussmaßnahmen mit unmittelbarer Folgewirkung zu Lasten der betroffenen Person und sogar Dritter. Diese Ausweitung gegenüber der Regelung des § 11c Absatz 2 Satz 2 beachtet damit die möglichen Folgen einer Übermittlung ins Ausland im Unterschied zu einer Übermittlung im Inland. Die Ausweitung wahrt demgemäß die Verhältnismäßigkeit der Schwelle unter besonderer Berücksichtigung der Auslandskonstellation. Die Überzeugung, dass solche Folgemaßnahmen ausgeschlossen sind, wird dabei häufig auf Erfahrungswissen beruhen. In Zweifelsfällen kann der Bundesnachrichtendienst auch eine Zusicherung der empfangenden Stelle einholen. Im Übrigen ist eine etwaige Unzuverlässigkeit der empfangenden Stelle auch in der Folgenabschätzung nach § 9e zu berücksichtigen.

Der Bundesnachrichtendienst macht bei der Übermittlung die einschränkende Folgenbegrenzung kenntlich.

Der Bundesnachrichtendienst darf ferner personenbezogene Daten an ausländische öffentliche Stellen übermitteln, wenn dies zur Vorbereitung und Durchführung seiner eigenen Maßnahmen erforderlich ist. Diese Regelung umfasst insbesondere Anfragen des Bundesnachrichtendienstes an ausländische öffentliche Stellen, die mit einer Übermittlung personenbezogener Daten einhergehen. Bei eigenen Maßnahmen des Bundesnachrichtendienstes kann es sich auch um solche handeln, die gemeinsam mit ausländischen Nachrichtendiensten durchgeführt werden und bei denen die Übermittlung personenbezogener Daten erforderlich ist (z.B. gemeinsame Zielerkundung, sog. Targeting).

Zu Absatz 4

Entsprechend der Regelung in § 11c Absatz 3 ist eine Übermittlung von ausschließlich mit dem Erhebungszweck der politischen Unterrichtung gekennzeichneten personenbezogenen Daten und deren Weiterverarbeitung durch die empfangende Stelle nur dann gestattet, wenn eine unmittelbar bevorstehende Gefahr für die in dem Absatz aufgezählten essentiellen Schutzgüter von höchstem Gewicht gegeben ist. Auf die Ausführungen zu § 11c Absatz 3 wird verwiesen.

Zu § 11f (Übermittlung an nicht öffentliche ausländische Stellen)

Eine Übermittlung von personenbezogenen Daten an nicht öffentliche ausländische Stellen ist grundsätzlich unzulässig. Eine Ausnahme von diesem Übermittlungsverbot sieht Satz 2 vor, der eine Übermittlung von personenbezogenen Daten an nicht öffentliche ausländische Stellen ermöglicht, wenn Rechtsgüter von besonders schwerem Gewicht betroffen sind. Die Ausnahmetatbestände orientieren sich hierbei an Vorgaben des Bundesverfassungsgerichts (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 313).

Zu Absatz 1

Für die Übermittlung an ausländische nicht öffentliche Stellen gelten erhöhte Formvorgaben. Sie bedürfen einer vorherigen Befassung der Behördenleitung, hiervon kann – abweichend zur Regelung für inländische nicht öffentliche Stellen, auch bei Gefahr im Verzug nicht abgewichen werden.

Zu Absatz 2 bis 4

Die Regelungen entsprechen § 11d Absatz 2 bis 4; insoweit wird auf die dortigen Ausführungen verwiesen.

Zu § 11g (Übermittlung von personenbezogenen Daten aus einer Vertraulichkeitsbeziehung an ausländische Stellen oder über- oder zwischenstaatliche Stellen)

§ 11h Absatz 1 entspricht § 11e; insoweit wird auf die dortigen Ausführungen verwiesen.

Zu Nummer 12

Die Einfügung der Überschrift dient der Übersichtlichkeit des Gesetzes.

Zu Unterabschnitt 5 (Gemeinsame Dateien)

Zu Nummer 13

Die Streichung ist Folge der Entkoppelung der Übermittlungsvorschriften des BNDG vom BVerfSchG.

Zu Nummer 14

Die Anpassungen sind Folge der neuen Übermittlungsvorschriften im BNDG.

Zu Buchstabe a (§ 21 Absatz 1 Nummer 1)

Die Anpassung ist Folge der neuen Übermittlungsvorschriften des BNDG. Die für den Bundesnachrichtendienst in Zusammenhang mit Übermittlungen spezifischen Straftaten sind in § 11b Absatz 1 geregelt.

Zu Buchstabe b (§ 25 Absatz 3 und 4)

Die Anpassung der Aufzählung in Absatz 3 und 4 ist Folge der Ziffer II. des Organisationserlasses des Bundeskanzlers vom 8. Dezember 2021 (BGBl I 5176).

Die neue Datumsangabe nebst Verweis berücksichtigt die Novellierung der VSA Bund in 2023.

Zu Buchstabe c (§ 28 Absatz 3)

Die Änderung berücksichtigt die Überführung des § 30 in den überarbeiteten Abschnitt 3 Unterabschnitt 4.

Zu Buchstabe d

Die Anpassungen sind Folgen der überarbeiteten Übermittlungsvorschriften in Abschnitt 3, Übermittlungen von personenbezogenen Daten, die nach § 19 erhoben werden, sind durch die Regelungen in Abschnitt 3 umfasst.

ENTWURF

Zu Buchstabe e

Es handelt sich bei der Anpassung um eine Folgeänderung.

Zu Buchstabe f

Auch die bisherigen §§ 38 und 39 wurde in die neu geregelten Übermittlungsvorschriften im Abschnitt 3 überführt.

Zu Buchstabe g

Es handelt sich bei der Anpassung um eine Folgeänderung.

Zu Buchstabe h

Es handelt sich bei der Anpassung um eine Folgeänderung.

Zu Nummer 15

Die Anpassung der Aufzählung in Absatz 3 und 4 ist Folge der Ziffer II. des Organisationserlasses des Bundeskanzlers vom 8. Dezember 2021 (BGBl I 5176).

Zu Nummer 16 (§ 65 Politische Berichterstattung und Information der Öffentlichkeit)

Zu Buchstabe a

Die politische Unterrichtung der Bundesregierung ist Aufgabe des Bundesnachrichtendienstes. Daneben ist er beauftragt, seine Informationen und Erkenntnisse auch an andere inländische öffentliche Stellen weiterzugeben und so auch zur Wirksamkeit von deren Tätigkeit beizutragen (vgl. hierzu Abschnitt 3 des BNDG, der mit diesem Gesetzentwurf grundlegend überarbeitet wird). Auch spielt der internationale Austausch von Informationen eine immer größere Rolle, um den außenpolitischen sowie den zunehmend globalisierten sicherheitspolitischen Herausforderungen Rechnung zu tragen. In der Regel erwächst erst aus dem Zusammenspiel der verschiedenen Stellen untereinander ein Gesamtbild, mit dem die Bundesregierung befähigt werden kann, ihre Regierungstätigkeit im außen- und sicherheitspolitischen Bereich wirksam wahrzunehmen.

Zu Buchstabe b

Die Berichterstattung des Bundesnachrichtendienstes dient der Information der Bundesregierung zur Wahrnehmung ihrer außen- und sicherheitspolitischen Verantwortung (vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 223). Es handelt sich hierbei um den primären Zweck der Auslandsaufklärung, wobei dies nicht den Schluss zulässt, dass ein größerer Teil der Daten des Bundesnachrichtendienstes aus Maßnahmen zur politischen Unterrichtung erhoben werden (Erhebungszweck politische Unterrichtung, vgl. § 19 Absatz 1 Nummer 1, § 34 Absatz 1 Nummer 1). Häufig ergibt sich eine Information für die Bundesregierung zur Wahrnehmung ihrer außen- und sicherheitspolitischen Verantwortung gerade aus Daten, die sich unabhängig von diesem Erhebungszweck, gerade auch im Zusammenspiel und dem Austausch des Bundesnachrichtendienstes mit anderen Stellen – sowohl im nationalen wie auch internationalen Bereich – ergeben. Übermittlungsschwellen sind bei der Information der Bundesregierung zur Wahrnehmung ihrer außen- und sicherheitspolitischen Verantwortung verfassungsrechtlich nicht geboten (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 224). Die Informationen im Rahmen der Berichterstattung werden zum Zweck der Regierungsarbeit, zum Zweck der Vorbereitung von Entscheidungen in Fragen der Außen- und Sicherheitspolitik genutzt und sind Teil der Beratung der Bundesregierung. Die Unterrichtung weiterer, auch nachgeordneter öffentlicher Stellen, setzt voraus, dass die Daten zum Zweck der Regierungsarbeit, zum Zweck von Entscheidungen in Fragen der

außen- und Sicherheitspolitik genutzt werden; eine Nutzung zu anderen Zwecken, insbesondere zu operativen Zwecken, ist nicht zulässig (vgl. BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 226). Die Zustimmung des Bundenachrichtendienstes zu einer Zweckänderung im Sinne von § 9a Absatz 1 Satz 2 2. Halbsatz ist ausgeschlossen.

Eine weitere inländische öffentliche Stelle kann beispielsweise das Bundespräsidialamt sein. Die Aufgabe des Bundespräsidenten ist u.a. die Repräsentation der Bundesrepublik Deutschland nach innen und außen sowie deren völkerrechtliche Vertretung (Artikel 59 Absatz 1 GG). Auch hier werden Entscheidungen getroffen, die u.a. Auswirkungen auf die Wahrnehmungen der Bundesrepublik Deutschland auch im Ausland haben. Um solche Entscheidungen treffen zu können, benötigt auch das Bundespräsidialamt umfassende Informationen, insbesondere auch aus dem Aufgabenbereich des Bundesnachrichtendienstes.

Die politische Unterrichtung auch unmittelbar nachgeordneter inländischer öffentlicher Stellen im Rahmen der Berichterstattung ist notwendig, da Regierungsarbeit und Entscheidungen auf Regierungsebene die Einbeziehung nachgeordneter – in den entsprechenden Themenbereichen zuständigen – inländischer öffentlicher Stellen bedingen. Nur durch die Einbeziehung auch nachgeordneter Stellen kann sichergestellt werden, dass die Bundesregierung in der Lage ist, in ihrer Regierungsarbeit sachlich fundierte Entscheidungen zu treffen. Die Vorbereitung von Regierungsentscheidungen erfolgt nicht allein auf Ebene der Bundesregierung, sondern muss die Fachkenntnisse ihrer nachgeordneten Behörden und deren wechselseitige Einschätzungen eines Sachverhalts einbeziehen. Die nachgeordneten Behörden müssen dazu in der Lage sein, die Informationen anderer Behörden einzuordnen, die Bundesregierung zu beraten, um gemeinsam der Bundesregierung die wirksame Wahrnehmung ihrer außen- und sicherheitspolitischen Verantwortung zu ermöglichen. Beispielhaft dafür sind auch hochrangige Gesprächsformate oder schriftliche Informationsformate – sowohl Regelformate wie auch anlassbezogene Termine – die gerade zum Ziel haben, einen Sachverhalt aus verschiedenen Perspektiven unterschiedlicher nachgeordneter Behörden zu beleuchten, um sich einer Regierungsentscheidung anzunähern. Es handelt sich dabei typischerweise um den Ressorts unmittelbar nachgeordnete Behörden. Eine Weitergabe von Informationen z.B. an Bezirksbehörden oder an bestimmte Ausländerbehörden ist unzulässig, da diese keine unmittelbare Rolle in der Vorbereitung der Regierungsentscheidungen einnehmen.

Die politische Unterrichtung ist keine Übermittlung im Sinne der §§°11 bis°11g. Das Bundesverfassungsgericht hat ausdrücklich erklärt, dass Übermittlungsschwellen bei der politischen Unterrichtung nicht geboten sind (BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 211, 224). Insbesondere kann auch auf den Schutz von Vertraulichkeitsbeziehungen verzichtet werden, soweit dies erforderlich ist (BVerfG, aaO. Rn. 198). Der Gesetzgeber hat sich daher entschieden, die politische Unterrichtung klar von der Übermittlung zu trennen. Die §§ 11ff. BNDG finden keine Anwendung. Nur in Ausnahmefällen dürfen Daten, die ausschließlich zum Zweck der politischen Unterrichtung erhoben wurden, an andere Stellen nach den §§°11 bis°11g übermittelt werden (siehe § 11b Absatz 4, § 11c Absatz 3, § 11e Absatz 4 sowie § 11f Absatz 3).

Zu Buchstabe c

Da sich die Bundesrepublik Deutschland in den genannten Staatenbündnissen oder zwischenstaatlichen Organisationen beteiligt, hat die Bundesrepublik Deutschland insbesondere auch eine Verantwortung, sicherheitspolitisch relevante Informationen insbesondere mit der Europäischen Union oder der Organisation des Nordatlantikvertrages zeitnah auszutauschen. Durch die Teilnahme an Staatenbündnissen entstehen der Bundesrepublik verschiedene Bündnispflichten, so dass auch insoweit die Möglichkeit der politischen Berichterstattung gegeben sein muss. Abweichend von Absatz 1 besteht insoweit jedoch keine Berichtspflicht.

Zu Buchstabe d

Die Norm ist unverändert im Vergleich zum geltenden Recht.

Zu Nummer 17

Zu Abschnitt 6 (Sicherung von Verschlusssachen im Bundesnachrichtendienst)

Abschnitt 6 enthält Regelungen für Maßnahmen im Bundesnachrichtendienst zur Sicherung von Verschlusssachen. Diese dienen der Verstärkung und Optimierung des Schutzes der durch den Bundesnachrichtendienst erhobenen sensiblen Informationen und in Ergänzung zu § 2 BNDG und § 4 Sicherheitsüberprüfungsgesetz (SÜG) dem Schutz des Bundesnachrichtendienstes und seiner Beschäftigten selbst. Der Bundesnachrichtendienst ist dauerhaft Ziel der Spionage durch fremde Nachrichtendienste. Mit der Ergänzung der Regelungen ist beabsichtigt, den Informationsabfluss aus dem Bundesnachrichtendienst auszuschließen. Mögliche Spionagetätigkeiten anderer Nachrichtendienste sollen durch die Kontrollen frühzeitig erkannt werden. Dieser Abschnitt enthält daher präzise Befugnisse, um den ordnungsgemäßen Umgang mit Verschlusssachen im Bundesnachrichtendienst verstärkt zu kontrollieren.

Die vorgesehenen Kontrollen dienen der präventiven Spionageabwehr im Nachgang der Sicherheitsüberprüfung, der sich alle Mitarbeiterinnen und Mitarbeiter des Bundesnachrichtendienstes unterziehen. Die Durchführung der Kontrollen soll unmittelbar durch den Bundesnachrichtendienst selbst ausgeführt werden. Er hat bessere Möglichkeiten, sicherheitsgefährdende oder geheimdienstliche Tätigkeiten in seinem Inneren frühzeitig zu bemerken und mit Kontrollen auf diese zu reagieren (vgl. Ader, in: Dietrich/Fahrner/Gazeas/von Heintschel-Heinegg, Handbuch Sicherheits- und Staatsschutzrecht, 2022, § 19 Rn. 75).

Die Verpflichtung entsprechende Kontrollen durchzuführen ergibt sich aus § 4 Absatz 4 Satz 1 SÜG, wonach Bundesbehörden verpflichtet sind, Versuche zur Durchbrechung des Verschlusssachenschutzes zu erkennen und aufzuklären. Zur Umsetzung der Verpflichtung nach § 4 Absatz 4 Satz 1 SÜG sind insbesondere folgende Maßnahmen zur Sicherung vorgesehen: Verwahrgelasse für Verschlusssachen, Aktensicherungsräume, Verschlusssachen-Registraturen, jährliche Belehrungen zum Umgang mit Verschlusssachen oder das Errichten besonderer Sicherheitsbereiche sowie das Vorhalten von Schließfächern für private Mobiltelefone innerhalb der Dienststellen des Bundesnachrichtendienstes. Die Kontrollausrichtung wird in den nach § 35 Absatz 4 SÜG erlassenen internen Verwaltungsvorschriften beschrieben, die den §§ 6, 63 VSA Bund 2023 entsprechen.

Eine Regelung der Befugnisse im Wege einer Verordnung ist nicht ausreichend, da durch die Maßnahmen zum Schutz von Verschlusssachen unmittelbar auch die Grundrechte der betroffenen Personen berührt werden (vgl. Franck, NVwZ 2021, 430, 431). Aus diesem Grund werden die Maßnahmen nunmehr in einem Parlamentsgesetz geregelt.

Die Regelungen im Abschnitt 6 betreffen Maßnahmen zur Sicherung von Verschlusssachen (v.a. Personen-, Taschen-, Fahrzeug- und Raumkontrollen sowie Auswertung von Geräten der Informations- und Kommunikationstechnik) sowie die weitere Verarbeitung der im Rahmen dieser Maßnahmen erhobenen Informationen einschließlich personenbezogenen Daten.

Neu zu regelnde Befugnisse zur Sicherung von Verschlusssachen sind:

- verdachtsunabhängige Personen-, Taschen- und Fahrzeugkontrollen innerhalb der Dienststellen, insbesondere an Ein- und Ausgängen; Befugnis zur Durchsuchung nur, wenn tatsächliche Anhaltpunkte vorliegen, dass dies zur Sicherung von Verschlusssachen erforderlich ist.

- verdachtsunabhängige Raumkontrollen; verdachtsabhängige Befugnis zur Öffnung und Durchsuchung von in Räumen befindlichen Gegenständen nur, soweit tatsächliche Anhaltspunkte vorliegen, dass dies zur Sicherung von Verschlusssachen erforderlich ist.

- Kontrollen von privatdienstlichen Geräten der Informations- und Kommunikationstechnik sowie privaten Geräten, wenn tatsächliche Anhaltspunkte vorliegen, dass die betroffene Person Verdächtige oder Verdächtiger einer sicherheitsgefährdenden oder geheimdienstlichen Straftat oder Nachrichtenmittlerin oder Nachrichtenmittler für die verdächtige Person ist. Für sich genommen genügt das einmalige oder auch unregelmäßig wiederholte Einbringen privater Geräte in die Dienststellen des Bundesnachrichtendienstes nicht, um als tatsächlicher Anhaltspunkt für eine Straftat die beschriebenen Kontrollen zu begründen.

Nicht geregelt ist die Befugnis, die Berechtigung des Aufenthalts der sich in den Dienststellen des BND befindlichen Personen zu kontrollieren oder von Personen, die die Dienststellen betreten möchten. Die Dienststellen des Bundesnachrichtendienstes sind Sicherheitsbereiche i.S.d. § 1 Absatz 2 Nummer 3 SÜG und damit gegen Zutritte besonders gesichert. Die Zutrittskontrolle ist schon aus diesem Grund erforderlich und zulässig. Dies umfasst auch die Befugnis, die Berechtigung der Person zum Aufenthalt in gesondert geschützten Bereichen innerhalb der Dienststellen des Bundesnachrichtendienstes zu kontrollieren.

Zu Unterabschnitt 1 (Befugnisse, Durchführung und Anordnung)

Zu § 65a (Maßnahmen zur Sicherung von Verschlusssachen)

Die einzelnen Kontrollmaßnahmen dieses Abschnitts werden in Ergänzung zum SÜG geregelt, welches durch die nach § 35 Absatz 4 SÜG erlassenen internen Verwaltungsvorschriften konkretisiert wird.

Soweit verdachtsunabhängige Kontrollen durchgeführt werden, wird der Bundesnachrichtendienst durch interne Vorgaben sicherstellen, dass diese verhältnismäßig und willkürfrei eingesetzt werden. Zu berücksichtigen ist u.a. das Zufallsprinzip, es darf keine unangemessene zeitliche Beanspruchung der betroffenen Personen erfolgen, Kontrollen sollten gleichmäßig in allen für den Umgang mit Verschlusssachen vorgesehenen Gebäuden bzw. Gebäudeteilen durchgeführt werden und auch auf allen Grundstücken. Eingriffsintensivere Maßnahmen werden an einen Verdacht geknüpft und finden damit nicht „ins Blaue hinein“ statt, da dies unzulässig wäre (vgl. BAG, Urteil vom 29.6.2017 – 2 AZR 597/16, NJW 2017, 2853, 2856 Rn. 32; Löffelmann/Zöller, Nachrichtendienstrecht, 2022, Teil C Rn. 30; Maschmann, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, § 26 BDSG Rn. 47; Stück, CCZ 2018, 88, 89). Bei kernbereichsrelevanten Vorgängen findet § 65h Anwendung.

Bei Kontrollen zum Verschlusssachenschutz handelt es sich nicht um eine originäre nachrichtendienstliche Befugnis. Es findet ein spezifisch dafür vorgesehenes Verfahren statt, welches durch Abschnitt 6 für den Bundesnachrichtendienst konkretisiert wird.

Zu Absatz 1

Die Vorschrift beschreibt die Zielrichtung der Maßnahmen zum Verschlusssachenschutz.

Zu Absatz 2

In Absatz 2 wird festgelegt, welcher Personenkreis durch die Maßnahmen zur Sicherung von Verschlusssachen betroffen sein kann.

Von Nummer 1 sind Beamtinnen und Beamte, Soldatinnen und Soldaten und Beschäftigte als Mitarbeiterinnen und Mitarbeiter des Bundesnachrichtendienstes erfasst. Die einzelnen Vorschriften finden laufbahnunabhängig für alle Statusgruppen gleichmäßig Anwendung und sind grundrechtsschonend ausgestaltet. Umfasst sind auch solche Personen, die nicht

in einem auf Dauer angelegten Beschäftigungsverhältnis, beispielsweise auf Grundlage von Werkverträgen oder Honorarverträgen, für den Bundesnachrichtendienst tätig sind. Sofern die Kontrollen in Anwesenheit der betroffenen Personen durchgeführt werden, ist dies Dienstzeit (restriktiver LAG Hessen, Urteil vom 10. August 2011, 8 Sa 1945/10, BeckRS 2011, 78545; Chwalisz, in: Oberthür/Seitz, Betriebsvereinbarungen, 3. Aufl. 2021, II Rn. 8 Anm. 169, danach können Kontrollen außerhalb der Dienstzeit vorgenommen werden).

Von Nummer 2 sind Mitarbeiterinnen und Mitarbeiter inländischer und ausländischer öffentlicher Stellen, auch anderer Nachrichtendienste, erfasst.

Nummer 3 betrifft Mitarbeiterinnen und Mitarbeiter externer Unternehmen sowie sonstige Besucherinnen und Besucher. Sofern sich Personen in den Dienststellen des Bundesnachrichtendienstes ohne dessen Erlaubnis aufhalten, handelt es sich um eine strafbewehrte Handlung (Hausfriedensbruch). Die Polizei wird in diesen Fällen eingeschaltet.

Die in Satz 1 aufgeführten Personen sind zur Mitwirkung bei der Durchführung von Maßnahmen zur Sicherung von Verschlusssachen verpflichtet. Weigern sich Personen nach Nummer 1, an der Durchführung von Maßnahmen zur Sicherung von Verschlusssachen mitzuwirken, kann dies statusrechtliche, disziplinarrechtliche oder arbeitsrechtliche Maßnahmen nach sich ziehen.

Zu Absatz 3

Alle Personen, die Dienststellen des Bundesnachrichtendienstes betreten, sind in geeigneter Weise über die durchzuführenden Kontrollen zu belehren, etwa durch Schreiben an Mitarbeiterinnen und Mitarbeiter, durch Hinweise bei Anmeldungsbestätigungen oder Piktogramme im Umfeld der Kontrollmaßnahmen oder durch mündliche Hinweise.

Zu § 65b (Kontrolle und Durchsuchung von Personen, Taschen und Fahrzeugen zur Sicherung von Verschlusssachen)

Die Personen-, Taschen- und Fahrzeugkontrollen sind zweistufig aufgebaut. Die Norm differenziert zwischen der Kontrolle in Nummer 1 und der Durchsuchung in Nummer 2.

Auf der ersten Stufe darf der Bundesnachrichtendienst verdachtsunabhängige Kontrollen durchführen. Damit können Verschlusssachenverstöße von Personen unabhängig davon erkannt werden, ob sie zuvor auffällig geworden sind.

Die eingriffsintensivere Durchsuchung auf der zweiten Stufe kann durchgeführt werden, wenn als zusätzliche Voraussetzung tatsächliche Anhaltspunkte vorliegen, dass dies zur Sicherung von Verschlusssachen erforderlich ist. Die Durchsuchung bedarf gemäß § 65e einer vorherigen Anordnung durch den Geheimschutzbeauftragten oder einer von ihr oder ihm bestimmten Vertretung. In Eilfällen kann die Maßnahme ohne Anordnung erfolgen, diese ist unverzüglich nachzuholen, vgl. § 65e Absatz 2.

Das Kontrollpersonal kann sich bei beiden Maßnahmen technischer Hilfsmittel bedienen. In Betracht kommen unter anderem Geräte zur Detektion von Mobilfunkgeräten, Torbogensonden, Durchgangsdetektoren oder Handmetalldetektoren. Sofern bei Kontrollen aus gesundheitlichen Gründen der betroffenen Person keine entsprechende Technik eingesetzt werden darf, müssen alternative Mittel eingesetzt werden, z.B. ein Handdetektor.

Zu Nummer 1

Die Kontrolle umfasst nicht die Durchsuchung von Gegenständen oder Personen. Umfasst ist lediglich eine Sichtkontrolle, d.h. eine oberflächliche Betrachtung, beispielsweise der Blick in die geöffnete Aktentasche oder Jackentasche oder das Durchblättern eines Stapels Papiere sowie das Öffnen von Innentaschen in einer Hand- oder Aktentasche oder das

Handschuhfach in einem Fahrzeug. Taschen in Kleidungen (z.B. Hosentaschen, Jackentaschen) sind auf Verlangen zu entleeren. In Abgrenzung zur Durchsuchung kann aber z.B. das Futter einer Tasche nicht auf etwaige eingenähte Gegenstände durchsucht werden. Führt die Mitarbeiterin oder der Mitarbeiter Verschlusssachen genehmigt mit sich, so umfasst die Kontrolle auch die Durchsicht dieser Unterlagen, soweit die Mitnahmegenehmigung dies vorsieht. Die betroffene Person kann auch in eine über die bloße Sichtkontrolle nach Nummer 1 hinausgehende Maßnahme einwilligen. Allein die Verweigerung einer solchen Einwilligung stellt jedoch keinen tatsächlichen Anhaltspunkt im Sinne von Nummer 2 dar, der für sich genommen bereits eine Durchsuchung rechtfertigen würde. Von Nummer 1 ist auch die Befugnis umfasst, die betroffene Person zu verpflichten, die die Sichtkontrolle behindernden Gegenstände abzulegen. Die Schwelle einer Durchsuchung bei Personen ist erreicht, wenn als entscheidendes Kriterium ein Körperkontakt stattfindet, vgl. § 65f Absatz 2. Dem Begriff „Personenkontrolle“ ist schon das Verständnis immanent, dass eine Kontrolle der Person erfolgt und die zu kontrollierende Person zumindest die Grundvoraussetzungen dafür schafft. Daher ist die Aufforderung an die betroffene Person, z.B. Mantel, Schal, Mütze, Handschuhe abzulegen von Nummer 1 mitumfasst. Andernfalls liefe die Befugnis leer, da eine sinnvolle Kontrolle nach Nummer 1 unmöglich wäre. Die betroffene Person ist nach § 65a Absatz 2 Satz 2 zur Mitwirkung verpflichtet.

Zu Nummer 2

Bei Nummer 2 handelt es sich um eine verdachtsabhängige Maßnahme. Die Durchsuchung ist gemäß § 65f Absatz 3 die zielgerichtete und planmäßige Suche am äußeren Körper (z.B. Abtasten der Person), sowie an Kleidung und Gegenständen, die zur Verbringung von Verschlusssachen geeignet sind. Die Kontrolle ist als weniger eingriffsintensive Maßnahme von der Durchsuchung mitumfasst. Zur Wahrung des Verhältnismäßigkeitsgrundsatzes sind Kontrollen nach Nummer 1 auch im Verdachtsfall nach Nummer 2 selbstverständlich zunächst als milderes Mittel möglich.

Tatsächliche Anhaltspunkte für das Erfordernis einer Durchsuchung sind konkrete Tatsachen, die dafür sprechen, dass gerade der zu untersuchende Lebenssachverhalt einen Verschlusssachenverstoß enthält (vgl. BGH NStZ 1994, 499 m.w.N.). Bloße, nicht durch konkrete Umstände belegte Vermutungen oder reine denktheoretische Möglichkeiten reichen nicht aus (vgl. nur BVerfG, NJW 2022, 3070; zur Rolle von Vorurteilen vgl. Ricker, Anfangsverdacht und Vorurteile, 2021). Bei anonymen Hinweisen ist vom Kontrollpersonal besondere Vorsicht walten zu lassen (vgl. LG Augsburg wistra 2018, 96; BeckOK StPO/Beukelmann, 47. Ed., § 152 Rn. 4). In den nachfolgenden Fallgruppen lassen sich tatsächliche Anhaltspunkte annehmen, die eine Durchsuchung rechtfertigen:

1. Fallgruppe:

Die hier erforderlichen tatsächlichen Anhaltspunkte können sich aus den zuvor durchgeführten Kontrollhandlungen nach Nummer 1 ergeben, die dafür sprechen, dass

- Geräte der Informations- und Kommunikationstechnik oder sonstige Geräte nach § 65a Absatz 1 Nummer 1 unbefugt eingebracht wurden oder

- Verschlusssachen unbefugt aus Dienststellen ausgebracht wurden (§ 65a Absatz 1 Nummer 2).

Klassischerweise wäre dies also z.B. das Anschlagen des „Handydetektors“ bei einer verdachtsunabhängigen Kontrollhandlung nach Absatz 1 Nummer 1 oder aber das Erkennen eines Mobiltelefons oder einer Verschlusssache während der Kontrolle.

Auch Torbogensonden sind bei deren Anschlagen als ein tatsächlicher Anhaltspunkt zu werten. Vor einer Durchsuchung muss der Mitarbeiterin oder dem Mitarbeiter die Gelegen-

heit gegeben werden, glaubhaft zu machen, dass sie oder er eine Verschlusssache zulässigerweise mitführt (insbesondere ausbringt). Dies geschieht regelmäßig durch Vorlage und Abgabe einer sogenannten Mitnahmegenehmigung für Verschlusssachen, die durch den Bundesnachrichtendienst für seine Mitarbeiterinnen und Mitarbeiter ausgestellt werden kann, die aus dienstlichen Gründen Verschlusssachen ausführen müssen.

2. Fallgruppe:

Darüber hinaus können sich tatsächliche Anhaltspunkte (wieder mit Blick auf Handlungen nach § 65a Absatz 1) aus einer anderen Erkenntnisquelle ergeben. Ein solcher Fall liegt zum Beispiels vor, wenn Mitarbeiter A sich an das Kontrollpersonal wendet und glaubhaft schildert, dass Mitarbeiter B regelmäßig an seinem Arbeitsplatz mit seinem Mobiltelefon telefoniert. Ein solcher Vortrag bedarf jedoch einer gewissen Substanz.

Ob in solchen Fällen nicht zunächst eine Kontrolle als milderes Mittel zu erwägen ist, ist von einer Einzelfallbetrachtung abhängig. Im geschilderten Beispiel käme etwa eine Kontrolle mit technischen Mitteln in Betracht.

Als weitere Erkenntnisquelle kommen Hinweise aus anderen Kontrollmaßnahmen in Frage (also Raum- und IT-Kontrollen) oder aber auch Hinweise Dritter, zum Beispiel ausländischer Nachrichtendienste.

3. Fallgruppe:

Außerdem könnten wiederholt festgestellte Sicherheitsverstöße im Rahmen von Kontrollen nach Nummer 1 tatsächliche Anhaltspunkte darstellen, wobei die Gesamtumstände des Einzelfalles zu berücksichtigen sind und dem Kontrollpersonal ein Beurteilungsspielraum zusteht.

Zu § 65c (Kontrolle und Durchsuchung von Räumen zur Sicherung von Verschlusssachen)

Die vorgesehenen Maßnahmen greifen nicht in den Schutzbereich des Artikel 13 GG ein. Nach der Rechtsprechung des Bundesverfassungsgerichts unterliegen nicht sämtliche behördlichen Amtsräume dem Schutz des Artikel 13 GG (BVerfGE 103, 142 (150) und Beschluss vom 12. Februar 2004 – 2 BvR 1687/02, BVerfGK 2, 310, 314 jeweils zu Einzeldienstzimmern von Polizeibeamten; BeckOK/Kluckert, 53. Ed. 2022 Artikel 13 Rn. 4; Jarass/Pieroth, GG, 17. Aufl. 2022, Artikel 13 Rn. 6; v. Münch/Kunig/Berger, GG, 7. Aufl. 2021, Artikel 13 Rn. 22; BK/Herdegen, Artikel 13 GG Rn. 36; Dreier/Hermes, GG, Bd. 1, 3. Aufl. 2013, Artikel 13 Rn. 23; Rensen/Brink/Wild, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 282; Hasenstab, IWRZ 2019, 3, 4). Die räumliche Privatsphäre ist vielmehr substanziiert im jeweiligen Einzelfall zu prüfen. Dabei sind Weisungen des Dienstherrn zur Büronutzung einzubeziehen.

Büros im Bundesnachrichtendienst fungieren nicht als individuelle Rückzugsbereiche. Zwar sind sie der Öffentlichkeit nicht allgemein zugänglich und enthalten zum Teil auch persönliche Gegenstände. Bereits die umfassende Einstufung als Sicherheitsbereich im Sinne des § 1 Absatz 2 Nummer 3 SÜG führt zu erheblichen Einschränkungen der räumlichen Privatsphäre im Vergleich zu Behörden ohne derartige Restriktionen. Auch bei ausschließlicher Nutzung durch eine Person ist der Dienstherr verpflichtet darauf zu achten, dass es in den Räumen keine räumlich geschützte Privatsphäre mit individuellen Rückzugsbereichen gibt, um Sicherheitsrisiken zu minimieren. Zudem haben für Einzelbüros regelmäßig auch Vorgesetzte und der Arbeitsschutz eine Schließberechtigung. Die in den Büros vorhandenen Schränke dienen der sicheren Aufbewahrung von Verschlusssachen und stellen keine persönlichen Schränke der Mitarbeiterinnen und Mitarbeiter dar. Dennoch ist auch bei der Kontrolle und Durchsuchung von Räumen das Grundrecht auf informationelle Selbstbestimmung in erforderlichem Maße zu achten.

Zu Absatz 1

Zu Nummer 1

Die Vorschrift regelt die verdachtsunabhängigen Raumkontrollen. Schon heute können Sichtkontrollen in behördlichen Büros zur Verwaltungspraxis von Sicherheitsbehörden gehören. Die Vorschrift stellt diese nunmehr auf eine gesetzliche Grundlage für den Bundesnachrichtendienst. Die Befugnis erlaubt keine fortlaufende akustische oder optische Überwachung der Büros der Mitarbeiterinnen und Mitarbeiter. Die Regelung erlaubt eine Sichtkontrolle. Das Öffnen verschlossener Behältnisse, die von der betroffenen Person selbst verschlossen wurden, stellt eine Durchsuchung nach Absatz°1 Nummer°2 dar.

Zu Nummer 2

Nach Nummer 2 darf der Bundesnachrichtendienst Räume einschließlich der in den Räumen befindlichen Gegenstände öffnen und diese durchsuchen, wenn Tatsachen die Annahme rechtfertigen, dass dies zur Sicherung der Verschlusssache erforderlich ist. Bei den sich in den Räumen befindlichen Gegenständen kann es sich z.B. um einen Büroschrank oder einen Rollkoffer handeln. Das Erfordernis von „Tatsachen, die die Annahme rechtfertigen“ stellt dabei eine höhere Schwelle dar und beinhaltet ein qualitatives Mehr gegenüber den tatsächlichen Anhaltspunkten (Vgl. BT-Drs. 19/26103, S. 96). So können verdichtete und weiter konkretisierte Anhaltspunkte zum Merkmal „Tatsachen, die die Annahme rechtfertigen“ führen. Zudem ist dieses Merkmal auch dann gegeben, wenn die Tatsachen den Rückschluss auf ein konkretisiertes und zeitnahes Geschehen zulassen und Rückschlüsse auf eine bestimmte oder hinreichend bestimmbare Person oder Personenkreis möglich sind. Im Rahmen der Raumkontrollen erhalten die Kontrollpersonen Zugriff auf und Einsicht in Verschlusssachen, die der zu kontrollierende Mitarbeitende auch zulässigerweise im Büro aufbewahrt. Dabei muss sichergestellt werden, dass der zu kontrollierenden Mitarbeitenden nicht missbräuchlich ein Verstoß gegen die Regelungen zur Sicherung von Verschlusssachen angelastet wird. Dieser Schutz kann beispielsweise durch ein 4-Augen-Prinzip bei der Kontrolle oder durch eine entsprechende Dokumentation der Kontrollmaßnahme erreicht werden.

Zu Absatz 2

Absatz 2 ermöglicht eine verdachtsunabhängige optische Überwachung von allgemein zugänglichen Bereichen des Bundesnachrichtendienstes. Dabei kann es sich um gemeinschaftlich genutzte Flure und Korridore, aber auch um allgemein zugängliche Arbeitsräume handeln, deren Beschaffenheit die Begehung von Verstößen gegen Vorschriften zum Schutz von Verschlusssachen begünstigt, wie z.B. Kopier- oder Druckerräume. Die Regelung erlaubt keine Überwachung von Büros der Mitarbeiterinnen und Mitarbeiter. Eine Überwachung höchstpersönlicher Räume, z.B. von Toiletten, Umkleideräumen oder Pausenräumen, ist unzulässig.

Zu § 65d (IT-Kontrollen zur Sicherung von Verschlusssachen)

§ 65d befugt den Bundesnachrichtendienst dazu, Geräte der Informations- und Kommunikationstechnik sicherzustellen und auszuwerten. Hierzu gehören alle Geräte sowie auch Zubehör, die eine elektronische Speicherung von Informationen ermöglichen und/oder in der Lage sind, eine Kommunikationsverbindung zu ermöglichen. Umfasst sind insbesondere alle Geräte, die geeignet sind, Informationen in Bild (Kamera) und Ton oder in sonstigen Darstellungsformen (z.B. digital) aufzunehmen, zu speichern oder zu übertragen. Hierbei ist das Übertragungsmedium unwesentlich. Eigenschaften solcher Geräte sind Möglichkeiten von Bild- und Tonaufnahmen, die Möglichkeit zur Abspeicherung von Dateien und die Ausstattung mit Funkschnittstellen oder kabelgebundenen Schnittstellen. Dies können insbesondere Mobiltelefone, Smartwatches und Fitnesstracker (sofern diese über eine

Speicherfunktion verfügen), Personal Digital Assistants (PDA), portable Navigationssysteme, Bildaufzeichnungsgeräte, Tonaufzeichnungsgeräte, IT-Speichermedien (z.B. Speicherkarten, USB-Sticks, CDs, Blu Rays, DVDs, Festplatten, Bluetooth-Kopfhörer, E-Book-Reader, Tablets oder Notebooks) sein. Die genannten Geräte zeichnen sich dadurch aus, dass sie durch eine manipulative Vorbereitungshandlung genutzt werden können, um etwa Schadsoftware (z.B.: Ausschalten der behördlichen IT-Infrastruktur durch DDoS-, Botnet- oder Virenangriffe) oder Abhörtechnik in den Bundesnachrichtendienst einzubringen bzw. Verschlusssachen auszubringen.

Zu Absatz 1

Der Bundesnachrichtendienst darf auf zu dienstlichen Zwecken überlassenen Geräten der Informations- und Kommunikationstechnik auch personenbezogene Daten zum Schutz der Verschlusssachen erheben und auswerten (vgl. ErfK/Franzen, 23. Aufl. 2023, § 26 BDSG Rn. 22 ff.; OVG Magdeburg, Urteil vom 30. Mai 2013 – 11 L 1/12). Hierfür ist keine gesetzliche Befugnis erforderlich. Von den Geräten der Informations- und Kommunikationstechnik umfasst sind zum einen solche, die in den Dienststellen verortet sind. Mitarbeitende des Bundesnachrichtendienstes bekommen aber auch –sofern für die zugewiesenen Aufgaben erforderlich – Informations- und Kommunikationstechnik zur dienstlichen Verfügung gestellt. Dies können Laptops, dienstliche Mobiltelefone und sonstige Geräte und Zubehör sein. Diese Überprüfungen dienen auch dazu, mögliche Sabotagehandlungen im Sinne des § 65a Absatz 1 Nummer 1 aufzuspüren. Absatz 1 berechtigt den Bundesnachrichtendienst, die entsprechenden Geräte herauszuverlangen und sicherzustellen, sofern sie sich nicht im Besitz des Bundenachrichtendienstes befinden.

Zu Absatz 2

Zu Satz 1

Absatz 2 Satz 1 umfasst die Geräte der Informations- und Kommunikationstechnik, die den Mitarbeitenden zwar vom Bundenachrichtendienst zur Verfügung gestellt werden, aber auch zu Zwecken genutzt werden dürfen, die den privaten Bereich des Mitarbeiters oder der Mitarbeiterin berühren können, z.B. bestimmte Laufwerke zum Speichern von Personalsachen (BVerwG Urteil vom 31. März 2011 – 2 A 11.08, NVwZ-RR 2011, 698, 699 Rn. 16). Das personengebundene Mail-Postfach und der Chatdienst dienen ebenfalls „privatdienstlichen“ Zwecken. Da bei diesen Überprüfungen auch private Daten betroffen sein können, sind diese eingriffsintensiver als die Auswertung rein dienstlicher Laufwerke. Die materiellen und formalen Schwellen sind daher erhöht. Es müssen tatsächliche Anhaltspunkte für den Verdacht einer Straftat vorliegen, die im unmittelbaren Bezug zu sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten steht, und die betroffene Person muss Verursacherin oder Verursacher dieser Straftat oder Nachrichtenmittlerin bzw. Nachrichtenmittler für die betroffene Person sein.

Zu Satz 2

In Satz 2 werden Straftaten aufgezählt, die typischerweise im Zusammenhang mit Verstößen gegen das SÜG begangen werden. Es handelt sich hierbei um Regelbeispiele. Möglicherweise hinzukommende Straftaten sind nicht auf solche begrenzt, die ergänzend in das Strafgesetzbuch aufgenommen werden, sondern auch gerade solche, die nicht typischerweise im Zusammenhang mit Verstößen gegen das SÜG begangen werden, gleichwohl in diesem Zusammenhang im Einzelfall begangen wurden.

Zu Satz 3

Auch Geräte der Informations- und Kommunikationstechnik von Nachrichtenmittlern können nach Satz 3 umfasst sein, wenn diese für die verdächtige Person bestimmte oder von ihm herrührende Informationen entgegennehmen und für ihn weitergeben. Dabei ist nicht

erforderlich, dass zwischen dem Verdächtigen und der Nachrichtenmittlerin oder dem Nachrichtenmittler eine Absprache besteht. Es muss sich auch nicht um eine Partnerschaft handeln, um die Nachrichtenmittlerin oder den Nachrichtenmittler als Verursacher zu qualifizieren. Zudem bedarf es auch nicht einer gemeinsamen Tatbegehung aufgrund eines gemeinsamen Tatentschlusses. Ein arbeitsteiliges Vorgehen zwischen dem Verdächtigen und der Nachrichtenmittlerin oder dem Nachrichtenmittler im Sinne einer mittäterschaftlichen Begehungsweise ist nicht erforderlich. Das reine Entgegennehmen von Informationen genügt hingegen nicht, da es auch Fälle geben kann, bei denen Empfängern gegen ihren Willen Informationen übermittelt werden. In diesen Fällen wäre eine Auswertung der privatdienstlichen Informations- und Kommunikationstechnik der Nachrichtenmittlerin oder des Nachrichtenmittlers unverhältnismäßig.

Zu Absatz 3

Nach Absatz 3 ist die Sicherstellung vorschriftswidrig eingebrachter privater Geräte zulässig, wenn zusätzlich zum vorschriftswidrigen Einbringen noch tatsächliche Anhaltspunkte vorliegen, dass die betroffene Person entweder selbst Verdächtige oder Verdächtiger einer Straftat nach Absatz 2 oder Nachrichtenmittlerin oder Nachrichtenmittler eines Verdächtigen einer solchen Straftat ist. Allein das – ggf. auch wiederholte – Einbringen des privaten Geräts führt daher ohne weiteres noch nicht zur Verwirklichung der erhöhten Schwelle. Vorschriften, die das Einbringen von Geräten der Informations- und Kommunikationstechnik untersagen, können sich aus Dienstvorschriften und Konkretisierungen des Präsidenten des Bundesnachrichtendienstes. Mitarbeitende und Dritte werden auf diese Regelungen deutlich vor Betreten einer Dienststelle des Bundesnachrichtendienstes aufmerksam gemacht.

Das Sicherstellen und das Auslesen der privaten Geräte der Informations- und Kommunikationstechnik stellt einen eingriffsintensiven Vorgang dar, der einem einfachen Gesetzesvorbehalt unterliegt. Die Befugnis ist für den Bundesnachrichtendienst von großer Bedeutung, um Straftaten, die die Sicherheit der Verschlusssachen gefährden, zu erkennen. Das private Gerät der Informations- und Kommunikationstechnik ist ein geeignetes Mittel, um Verschlusssachen unkompliziert und unerkannt aus dem Bundesnachrichtendienst heraus zu transportieren. Hierdurch entsteht eine hohe Gefahr für die Sicherheit vertraulicher Informationen; ein Datenabfluss kann enormes Schadenspotential aufweisen. Die Maßnahme wird auf dasjenige Maß beschränkt, das für die Kontrolle des Verschlusssachenschutzes erforderlich ist. Die Kontrolle bezweckt das Erkennen von abgespeicherten behördlichen Daten. Der Bundesnachrichtendienst könnte ohne die entsprechenden Beweise, die er im Rahmen einer Maßnahme nach Absatz 3 sichert, auch nicht personaldienstlich gegen die entsprechenden Mitarbeiter vorgehen und wäre gehalten, diese weiter zu beschäftigen und ggf. auch den Zugang zu VS-Material zu ermöglichen. Auch der Entzug eines Sicherheitsbescheides ist nicht ohne das Vorliegen bestimmter Voraussetzungen möglich. Daher kann auf eine entsprechende Befugnis nicht verzichtet werden.

Die Kontrolle ist angemessen. Die vorgesehenen Schwellen, das Verursacherprinzip sowie die verfahrenssichernden Bestimmungen wie etwa Anordnung (§ 65e Absatz 1), Kennzeichnung und Protokollierung tragen den Rechten der betroffenen Personen und dem Kontrollzweck Rechnung. Es handelt sich bei Verschlusssachen um Informationen des Bundesnachrichtendienstes, die besonders sensibel und schutzbedürftig sind. Die in einer Kontrolle von privaten Geräten der Informations- und Kommunikationstechnik liegende Härten sind mit Rücksicht auf die Besonderheiten der vom Bundesnachrichtendienst wahrzunehmenden Aufgaben hinzunehmen. Im Hinblick auf die selbst gegenüber anderen Sicherheitsbehörden exponierte Lage des Bundesnachrichtendienstes ist hier sogar ein besonders strenger Maßstab anzulegen (vgl. zu diesem Maßstab in Bezug auf Sicherheitsüberprüfungen bereits BVerwG, Beschluss vom 1. Oktober 2009, 2 VR 6.09, BeckRS 2009, 39914, Rn. 15).

Das Verursacherprinzip enthält eine weitere materielle Schwelle aufgrund der gesteigerten Grundrechtsintensität. Auch wenn keine Situation denkbar wäre, dass sich die Maßnahme gegen eine andere Person richten könnte, wirkt diese materielle Voraussetzung grundrechtsschonend. Hierdurch wird auch der Anlass des Kontrollvorgangs weiter konkretisiert, da ein Verantwortlicher bereits identifiziert werden kann bzw. identifizierbar ist (Anlehnung an BVerfG, Urteil vom 27. Februar 2008, Az. 1 BvR 370/07, 1 BvR 595/07, Rn. 251).

Das private informationstechnische Gerät ist nach höchstens zwei Wochen an die betroffene Person zurückzugeben, es sei denn, es muss zur Einleitung eines strafrechtlichen Ermittlungsverfahrens an die Strafverfolgungsbehörden weitergegeben werden. In diesen Fällen richtet sich die Herausgabe nach den für das Ermittlungsverfahren geltenden Bestimmungen (§ 111n, § 111o StPO).

Zu Absatz 4

Absatz 4 enthält eine Regelung für den Fall, dass die betroffene Person darlegt, dass sie auf die Erreichbarkeit mittels ihres privaten Mobiltelefons oder dessen Nutzung angewiesen ist (nachvollziehbare private Gründe, etwa zur Nutzung des Gerätes aus familiären oder gesundheitlichen Gründen). In diesen Fällen kann vor der Rückgabe des privaten informationstechnischen Geräts ein Abzug zur Sicherung der Daten erstellt werden, damit dieses schnellstmöglich (höchstens binnen 48 Stunden) an die betroffene Person zurückgegeben werden kann. Eine Auswertung der Daten darf aber erst nach der Anordnung der Auswertung erfolgen. An die Darlegung der Gründe für die Unzumutbarkeit der Aufrechterhaltung der Sicherstellung sind keine erhöhten Anforderungen zu stellen. Legt der Mitarbeitende dar, dass er auf das Mobiltelefon nicht verzichten kann und aus diesen Gründen einen Datenabzug bevorzugt, ist dem in der Regel nachzukommen. Etwas anderes kann sich nur ergeben, wenn Hinweise dafür vorliegen, dass die betroffene Person plant, im Anschluss Beweise vernichten zu wollen oder die Begründung gänzlich fernliegend ist.

Zu Absatz 5

Absatz 5 betrifft Zufallsfunde innerhalb der Dienststellen des Bundesnachrichtendienstes (z.B. liegen gelassenes Mobiltelefon in Besprechungsraum oder Kantine) und regelt eine Auswertung des Gerätes zur Identifizierung der Inhaberin oder des Inhabers, wenn die oder der Berechtigte nicht ausfindig gemacht werden kann. Meldet sich der Betroffene, kann festgestellt werden, ob es sich um ein dienstliches, privat-dienstliches oder privates Gerät der Informations- und Kommunikationstechnik handelt. Für die Feststellung, ob es sich um ein dienstliches, privat-dienstliches oder vorschriftswidrig eingebrachten privates Mobiltelefon handelt, können neben den Angaben der betroffenen Person auch sonstige weiteren Erkenntnisse herangezogen werden, die dem Bundesnachrichtendienst hierzu vorliegen. Die weitere Vorgehensweise richtet sich dann entsprechend nach Absatz 1 bis 3.

Zu Absatz 6

Die Vorschrift betrifft Fälle der unvermeidbaren Betroffenheit von Dritten wie sie das geltende Recht vergleichbar bereits in § 34 Absatz 6 BNDG enthält (vgl. dazu BT-Drs. 19/26103, S. 96). Es handelt sich um sachlich zwingend notwendige Fälle. Die Erfassung ist auf den zur Umsetzung der Maßnahme notwendigen Umfang beschränkt. Eine Mitbetroffenheit kann z.B. eintreten, wenn sich auf dem Mobiltelefon einer verdächtigen Person Fotos oder Nachrichten Dritter befinden.

Zu Absatz 7

Satz 1 ist an den geltenden § 34 Absatz 4 Satz 1 angelehnt. Satz 2 orientiert sich § 34 Absatz 7 und regelt grundrechtsschonend das Verfahren zur Prüfung der erhobenen Daten, indem sie auf Relevanz zu prüfen und ggf. unverzüglich zu löschen sind.

Zu Absatz 8

Die Vorschrift regelt die Befugnis zur Durchsuchung, falls das vorschriftenwidrig eingebrachte private Gerät nicht freiwillig übergeben wird. Die Durchsetzung richtet sich nach § 65f Absatz 6.

Zu § 65e (Anordnung von Maßnahmen zur Sicherung von Verschlusssachen)

Zu Absatz 1

Für die verdachtsunabhängigen Kontrollen nach § 65b Nummer 1 ist kein Anordnungsverfahren erforderlich. Sie können dauerhaft durchgeführt werden und betreffen unterschiedslos alle Personen, die die Dienststellen des Bundesnachrichtendienstes betreten. Dies entbindet den Bundesnachrichtendienst nicht von ggf. erforderlichen dienstinternen Anweisungen zur Art und Weise der Durchführung solcher Kontrollen.

Für Maßnahmen nach § 65c Nummer 1 (verdachtsunabhängige Raumkontrollen) muss nicht in jedem Fall eine Einzelanordnung erfolgen. Da die Kontrollen zu unterschiedlichen Zeitpunkten und in vielen Dienststellen des Bundesnachrichtendienstes stattfinden, besteht die Möglichkeit, eine allgemeine Anordnung zur Durchführung mehrerer gleichgelagerter Maßnahmen innerhalb eines in der Anordnung definierten Zeitraums von höchstens sechs Monaten zu erteilen.

Für Maßnahmen nach § 65d kann eine Anordnung erlassen werden, die sowohl die Sicherstellung als auch die anschließende Auswertung des Gerätes umfasst.

Die Anordnung hat eine verfahrenssichernde Funktion. Sie dient der behördeninternen Kontrolle zum Schutz des Betroffenen und wirkt dem Risiko entgegen, dass verdachtslose Kontrollen dazu missbraucht werden, Mitarbeiterinnen und Mitarbeiter unter Druck zu setzen. Dies ist u.a. geboten, um die Unabhängigkeit und Unparteilichkeit von Beamten gegenüber ihrem Dienstherrn abzusichern (hergebrachter Grundsatz des Berufsbeamtentums, Artikel 33 Absatz 5 GG).

Für sämtliche Kontrollen mit Ausnahme der verdachtsunabhängigen Kontrollen nach § 65b Nummer 1 ist ein Anordnungsverfahren vorgesehen. Die Anordnungskompetenz knüpft an die Rolle des Geheimschutzbeauftragten oder der von ihm beauftragten Personen an, die ihnen zugewiesen ist nach § 3a Absatz 1 SÜG und der behördeninternen Verschlusssachenanweisung, deren Inhalt § 8, § 63 Absatz 1 VSA Bund entspricht. Bei den besonders eingriffsintensiven Maßnahmen des § 65d Absatz 2 und 3 hat die Anordnung durch die Behördenleitung oder ihre Vertretung zu erfolgen.

Die Anordnung hat sowohl eine Warn- als auch eine Schutzfunktion. Betroffene Mitarbeiter werden geschützt, da ein Anordnungsverfahren sicherstellt, dass BND-intern das Vorliegen der Voraussetzung sorgfältig geprüft und dokumentiert wurden. Auch dient das Anordnungsverfahren den durchführenden Mitarbeiter als Warnung, dass nunmehr eingriffsintensivere Maßnahmen durchgeführt werden. Das Anordnungsverfahren ermöglicht zudem durch die Dokumentationspflicht auch eine verbesserte Überprüfbarkeit der Maßnahmen.

Die in der erlassenden Anordnung typischerweise schriftlich präzise aufzunehmenden Angaben werden in Satz 3 genannt. Die Dokumentationspflicht dient ebenfalls dem Schutz der betroffenen Personen, v.a. bei verdachtslosen Raumkontrollen, die in Abwesenheit der betroffenen Personen durchgeführt werden. Sie schützt die betroffene Person u.a. davor, unverschuldet in Verdacht zu geraten bzw. erleichtert es ihr, sich gegen einen solchen Verdacht wehren zu können.

Zu Absatz 2

Absatz 2 regelt den Eilfall. Ein Eilfall liegt vor, wenn der Zweck der Maßnahme bei Einholung einer vorherigen Anordnung vereitelt oder wesentlich erschwert würde, was etwa bei Gefahr im Verzug angenommen werden. Diese kann beispielsweise eintreten, wenn das Kontrollpersonal im Rahmen seiner Tätigkeit zur Sicherung von Verschlusssachen entdeckt, dass ein Gerät der Informations- und Kommunikationstechnik unbefugt im BND eingesetzt wird. In diesem Fall darf das Kontrollpersonal die erforderlichen Maßnahmen (z.B. Durchsuchung der Person oder Sicherstellung eines Gerätes der Informations- oder Kommunikationstechnik) ohne vorherige Anordnung durchführen.

Im Fall der IT-Kontrolle ist ohne vorherige Anordnung lediglich das Herausgabeverlangen bzw. die Sicherstellung des Gerätes der Informations- oder Kommunikationstechnik möglich. Im Fall des § 65d Absatz 4 (Härtefall) erfolgt die Auswertung der Daten erst nachdem die Anordnung nachgeholt wurde. Für die Auswertung privater oder privatdienstlicher IT ist in jedem Fall eine Anordnung – ggf. nachgeholt – notwendig.

Das Anordnungsverfahren ist unverzüglich nachzuholen; hierzu sind organisatorische Vorkehrungen zu treffen. Die besondere Eilbedürftigkeit ist im Einzelfall zu begründen, pauschalisierte Begründungen reichen nicht. Wird das Anordnungsverfahren nicht nachgeholt, ist das private IT-Gerät unverzüglich an die betroffene Person zurückzugeben. Eventuell bereits erhobene Daten sind unverzüglich zu löschen. Eine Nutzung der Daten kommt nicht in Betracht.

Zu Absatz 3

Absatz 3 regelt die sofortige Vollziehbarkeit der Maßnahme nach Absatz 1. Ohne die sofortige Vollziehbarkeit droht ein Informationsverlust und in der Folge könnten in diesem Zusammenhang begangene Straftaten nicht verfolgt werden.

Bei möglichen Klageverfahren ist das Bundesverwaltungsgericht erstinstanzlich zuständig (vgl. § 50 Absatz 1 Nummer 4 VwGO). Die betroffenen Personen haben die Möglichkeit, eine gerichtliche Überprüfung der Maßnahmen zu veranlassen.

Zu § 65f (Durchführung von Maßnahmen zur Sicherung von Verschlusssachen)

§ 65f regelt erstmalig auch Vollstreckungsmaßnahmen des Bundesnachrichtendienstes für den eng umgrenzten Bereich der Maßnahmen zur Sicherung von Verschlusssachen (vgl. zum abweichenden geltenden Recht Ader, in: Dietrich/Fahrner/Gazeas/von Heintschel-Heinegg, Handbuch Sicherheits- und Staatsschutzrecht, 2022, § 19 Rn. 75). Ohne eine entsprechende Befugnis hinge die Durchführung der Kontrollen davon ab, ob die Beschäftigten mit der Kontrolle einverstanden sind. Sollten sie diese ablehnen, hat der Bundesnachrichtendienst keine Möglichkeiten, um einen Verschlusssachenbruch aufzuklären, sondern könnte lediglich auf disziplinar- oder strafrechtlichem Wege vorgehen. Eine Einschaltung der Strafverfolgungsbehörden würde bedeuten, dass sich das Kontrollpersonal bis zu deren Eintreffen auf das vorläufige Festnahmerecht nach § 127 StPO berufen könnte (vgl. allg. MKBGB/Spinner, 9. Aufl. 2023, § 611a Rn. 987; Koreng/Lachenmann/Huth, Formularhandbuch Datenschutzrecht, 3. Aufl. 2021, H IV.2 Anm. 12). Diese beiden Alternativen sind sehr zeit- und bürokratieaufwändig und können einen Verschlusssachenbruch nicht unmittelbar verhindern. Auch ist Voraussetzung eines Festnahmerechts nach § 127 StPO, dass die Person einer Straftat verdächtig ist; der Verstoß gegen das SÜG begründet aber nicht in jedem Fall eine Straftat. Deshalb ist es angesichts des Schadenspotentials und der generellen Gefährdungswahrscheinlichkeit erforderlich, dass der Bundesnachrichtendienst beim Vollzug von Maßnahmen zur Sicherung von Verschlusssachen auch unmittelbaren Zwang einsetzen darf, wenn eine kollegiale Ansprache nicht mehr weiterhilft.

Zu Absatz 1

In Absatz 1 wird klarstellend die Verhältnismäßigkeit der Kontrollmaßnahmen geregelt. Dabei darf eine Kontrollmaßnahme insbesondere nicht erkennbar außer Verhältnis zu dem beabsichtigten Erfolg, d.h. dem Erkennen von Verstößen gegen die Verschlusssachenanweisung stehen.

Zu Absatz 2 und Absatz 3

Die Vorschriften enthalten Durchführungsbestimmungen für die Kontrollen und Durchsuchung von Personen, Sachen und Räumen. Zur Abgrenzung der Kontrolle und der Durchsuchung, vgl. Begründung zu Nummer 26, § 65b Nummer 1. Soll die Durchsuchung gegen den Willen des Adressaten erfolgen, kann sie – beziehungsweise die darin enthaltene, konkludente Duldungsverfügung – mit Zwangsmitteln bis hin zur Anwendung von unmittelbarem Zwang (beispielsweise Festhalten gegenüber körperlichem Widerstand oder zwangsweises Öffnen am Körper getragener Taschen) durchgesetzt werden. Eine körperliche Untersuchung der betroffenen Person ist unzulässig; eine solche kann nur durch die Polizei nach den hierfür geltenden Vorschriften vorgenommen werden.

Zu Absatz 4

Absatz 4 stellt klar, dass im Rahmen der Maßnahmen zur Sicherung von Verschlusssachen aufgefundene Verschlusssachen sowie Geräte der Informations- und Kommunikationstechnik sichergestellt werden können. Da dies in Zusammenhang mit einer Kontrollmaßnahme nach § 65b bis § 65d erfolgt, sind die hierfür die hierfür vorgesehenen Eingriffsschwellen maßgeblich.

Zu Absatz 5

Absatz 5 regelt die Rechte der betroffenen Personen bei einer Durchsuchung nach Absatz 3. Die betroffene Person hat das Recht anwesend zu sein. Auf Wunsch ist eine Bescheinigung über die Durchsuchung und den Grund der Durchsuchung auszustellen, dies dient dem Betroffenen auch zur Durchsetzung von ggf. gewählten Rechtsmitteln gegen die Maßnahme. Damit wird die Position der betroffenen Personen gestärkt, individuellen Rechtsschutz anzustreben.

Zu Absatz 6

Die Befugnis zur Vollstreckung der Kontrollen ergibt sich aus Absatz 6. Dies gilt jedoch nicht für Kontrollen beim Betreten der Dienststellen an Eingängen zum Zweck der Verhinderung des Einbringens von Geräten der Informations- und Kommunikationstechnik oder sonstiger Gegenstände nach § 65b Nummer 1 zum Zwecke des § 65a Absatz 1 Nummer 1. Absatz 6 verweist auf die Regelungen zur Androhung, Festsetzung und Anwendung des Zwangsmittels nach dem Verwaltungs-Vollstreckungsgesetz (VwVG).

Der Einsatz von Zwangsmitteln ist nicht bei Kontrollen nach § 65a an Eingängen der Dienststellen des Bundesnachrichtendienstes zum Zweck der Verhinderung des unbefugten Einbringens von Geräten der Informations- und Kommunikationstechnik oder sonstigen Gegenständen zulässig. Dass eine Mitarbeiterin oder ein Mitarbeiter in diesem Fall unentschuldigt den Dienst nicht antritt, wäre 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 zulässig.

Das VwVG ist auch für den Bundesnachrichtendienst anwendbar, der Verweis ist insofern klarstellend.

ENTWURF

Zu Absatz 7

Da die Anwendung des Gesetzes über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes (UZwG des Bundes) nur für Vollzugsbeamte des Bundes anwendbar ist und die Mitarbeiterinnen und Mitarbeiter des Bundesnachrichtendienst nur für den Sonderbereich der Verschlusssachenkontrolle über Zwangsbefugnisse verfügen sollen (und mit Blick auf das Trennungsgebot auch nur für diesen Sonderbereich über Zwangsbefugnisse verfügen dürfen), bedarf es für die zwangsweise Durchsetzung der Maßnahmen die Sondervorschrift des Absatz 7 für den Bundesnachrichtendienst. Die Zwangsmittel für die Verschlusssachenkontrolle sind abschließend und enumerativ geregelt. Der Einsatz von Schusswaffen ist unzulässig. Die zwangsweise Durchsetzung der Kontrollbefugnisse darf nur durch Personen erfolgen, die über eine qualifizierte Ausbildung verfügen. Diese Personen sind hierfür durch die Behördenleitung gesondert zu ermächtigten. Der Bundesnachrichtendienst hat dafür Sorge zu tragen, dass die Mitarbeiter entsprechend ausgebildet werden.

Zu Unterabschnitt 2 (Verarbeitung und Übermittlung von personenbezogenen Daten aus Maßnahmen zur Sicherung von Verschlusssachen)

Zu § 65g (Kennzeichnung, Speicherung, Löschung und Zweckbindung)

Die Vorschrift trägt dem Umstand Rechnung, dass durch die vorgesehenen Kontrollen persönliche Informationen und insbesondere personenbezogene Daten bei den betroffenen Personen erhoben werden können. Deshalb bedarf es einer besonderen Kennzeichnung und gesonderter Lösch- und Überprüfungsvorschriften.

Zu Absatz 1

Absatz 1 regelt die Befugnis zur Verarbeitung personenbezogener Daten mit der Pflicht zur Kennzeichnung.

Zu Absatz 2

Absatz 2 regelt die Aufbewahrungs- und Löschpflichten.

Zu Absatz 3

Absatz 3 enthält eine besondere Zweckbindungsklausel für Daten die im Rahmen der Maßnahmen zur Sicherung von Verschlusssachen erhoben worden sind. Sofern diese Daten auf eine sicherheitsgefährdende oder geheimdienstliche Tätigkeit hinweisen, dürfen diese zu diesem Zweck nach § 2 Absatz 1 Nummer 1 oder Nummer 2 genutzt werden. Für die dann erforderlichen weiteren Maßnahmen im Bereich der Eigensicherung dürfen die nachrichtendienstlichen Mittel nach § 5 Satz 1 BNDG genutzt werden, da die Eigensicherung eine Annexaufgabe zu § 1 Absatz 2 BNDG ist (Gusy, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 2 BNDG Rn. 21; Dietrich, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, III, § 3 Rn. 62).

Zu § 65h (Schutz des Kernbereichs privater Lebensgestaltung)

Auch Maßnahmen zur Sicherung von Verschlusssachen haben den Kernbereich privater Lebensgestaltung der betroffenen Personen zu wahren (Richardi/Maschmann, BetrVG, 17. Aufl. 2022, § 75 Rn. 50 ff. m.w.N.). Bei der Ausgestaltung wurde dem Datenschutz hoher Wert beigemessen. Bei der Schulung der Mitarbeiter, die die Kontrollen durchführen, hat eine besondere Sensibilisierung in Bezug auf eine mögliche Verletzung des Kernbereichs zu erfolgen.

ENTWURF

Zu Absatz 1

Der Schutz des Kernbereichs privater Lebensgestaltung gewährleistet dem Individuum einen Bereich höchstpersönlicher Privatheit und sichert einen dem Staat nicht verfügbaren Menschenwürdekern grundrechtlichen Schutzes gegenüber sämtlichen staatlichen Eingriffen. Selbst überragende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Bereich privater Lebensgestaltung nicht rechtfertigen. 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 nicht öffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens, die in der berechtigten Annahme geführt wird, nicht überwacht zu werden. Es besteht daher ein umfassendes Verwertungsverbot. Demgegenüber gehören z.B. die Besprechung und Planung von Straftaten nicht zum Kernbereich privater Lebensgestaltung, selbst wenn sie auch Höchstpersönliches zum Gegenstand haben. Ob eine personenbezogene Kommunikation dem Kernbereich zuzuordnen ist, hängt von den Besonderheiten des jeweiligen Einzelfalls ab.

Zu Absatz 2

Kommt es trotz Absatz 1 zur Erhebung kernbereichsrelevanter Daten, schreibt Absatz 2 die unverzügliche Löschung vor.

Zu Absatz 3

Als eine im Konzept des Kernbereichsschutzes neue Norm wird das Gebot festgeschrieben, eine Kontrolle abzubrechen, wenn erkennbar wird, dass durch diese Maßnahme nicht nur am Rande Erkenntnisse über den Kernbereich privater Lebensgestaltung erlangt werden (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17-, Rn. 286).

Zu § 65i (Personenbezogene Daten aus Vertraulichkeitsbeziehungen)

Die Norm verweist auf § 21 BNDG. Vertraulichkeitsbeziehungen werden auch bei Maßnahmen zum Schutz von Verschlusssachen geschützt.

Es kann beispielsweise der Fall eintreten, dass eine Maßnahme zur Sicherung von Verschlusssachen auch Kommunikation aus Vertraulichkeitsbeziehungen betrifft (z.B. Korrespondenz eines Mitarbeiters oder einer Mitarbeiterin mit dessen/deren Rechtsanwalt bei der Auswertung eines Gerätes der Informations- oder Kommunikationstechnik, ärztliche Unterlagen). § 65i stellt klar, dass auch in dieser Konstellation diese Kommunikation besonders geschützt ist.

Zu § 65j (Schutz von minderjährigen Personen)

Die Vorschrift dient dem Minderjährigenschutz. Die Beurteilung der Minderjährigkeit einer Person richtet sich nach den Vorschriften des Bürgerlichen Gesetzbuchs.

Zu Absatz 1

Bei Maßnahmen zum Schutz von Verschlusssachen können personenbezogene Daten von Minderjährigen berührt sein. Grundsätzlich ist bei den Maßnahmen zum Schutz von Verschlusssachen darauf zu achten, eine Verarbeitung von Daten, die nicht zu den Personen nach § 65 Absatz 2 gehören, auf das erforderliche Maß zu beschränkten ist. Zum Teil sind aber andere Personen unvermeidbar mitbetroffen, vgl. § 65d Absatz 6. Bei der Auswertung von Daten auf einem Gerät der Informations- und Kommunikationstechnik können beispielsweise Kinderbilder enthalten sein. Grundsätzlich gilt ein Löschgebot. Sollte eine Löschung in Fällen der Datenverbindung ausscheiden, enthält Satz 2 hierfür die notwendigen

ENTWURF

Vorgaben mit einer eingeschränkten Verarbeitung, der etwa durch Kennzeichnung der Daten entsprochen werden kann.

Zu Absatz 2

Maßnahmen zur Sicherung von Verschlusssachen können sich auch gegen Mitarbeiter des BND unter 18 Jahren richten, beispielsweise Mitarbeiter, die sich in der Ausbildung befinden. Es dürfen sich auch Minderjährige, mit Erlaubnis des Bundesnachrichtendienstes in seinen Dienststellen aufhalten. Ein Beispiel hierfür wären minderjährige Mitarbeiter von Fremdfirmen wie z.B. Auszubildende. Sind diese Personen unter 16 Jahren, findet Absatz 1 Anwendung.

Zu § 65k (Protokollierung)

Zu Absatz 1

Die Vorschrift regelt entsprechend § 76 BDSG die Protokollierung der Verarbeitung von personenbezogenen Daten in automatisierten Dateien, um deren anschließende Kontrolle etwa durch den behördlichen Datenschutz oder gesetzlich vorgesehene Kontrollorgane sicherzustellen. Die Vorschrift dient der Umsetzung der datenschutzrechtlichen Kontrolle der Verarbeitung von personenbezogenen Daten, die im Rahmen von Maßnahmen zur Sicherung von Verschlusssachen erhoben wurden.

Zu Absatz 2

Die Löschung ist zu protokollieren. Die Protokolldaten unterliegen einer Zweckbindung und dürfen ausschließlich zur Durchführung von Kontrollen der Datenverarbeitung genutzt werden. Dies umfasst zum einen Datenschutzkontrollen des Behördlichen Datenschutzes und der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, aber auch ensprechende betriebstechnische Kontrollenhinsichtlich der Funktionsfähigkeit der behördlichen IT.

Zu Absatz 3

Die Vorschrift normiert Aufbewahrungsfristen zur Sicherstellung der Datenschutzkontrolle nach erfolgter Löschung.

Zu Absatz 4

Durch die begleitende Überprüfung durch den behördlichen Datenschutz des Bundesnachrichtendienstes ist eine weitere grundrechtssichernde Kontrollinstanz eingebunden, um auf die Einhaltung der Vorschriften hinzuwirken (vgl. § 7 Absatz 2 BDSG). Danach kann der behördliche Datenschutz jederzeit die Einhaltung der gesetzlichen Vorgaben kontrollieren. Die betroffenen Bereiche müssen so jederzeit mit einer Kontrolle rechnen.

Zu § 65l (Übermittlung von personenbezogenen Daten aus Maßnahmen zur Sicherung von Verschlusssachen)

Zu Absatz 1

Die von § 65l erfassten Daten wurden nicht nachrichtendienstlich erhoben, so dass die Vorgaben des Bundesverfassungsgerichts für Übermittlungen von mit nachrichtendienstlichen Mitteln erhobenen Daten an Strafverfolgungsbehörden keine Anwendung finden. § 65l Absatz 1 stellt keine eigenständige Rechtsgrundlage für die Übermittlung dar. Diese richtet sich nach § 25 Absatz 1 BDSG. Dessen Anwendung ist auch nicht durch § 64 Nummer 1 eingeschränkt.

ENTWURF

Zu Absatz 2

Die Übermittlung personenbezogener Daten, die im Rahmen von Maßnahmen zur Sicherung von Verschlusssachen erhoben wurden, an die herausgebende Stelle der Verschlusssache ist zulässig, wenn Anhaltspunkte für eine Gefährdung der Vertraulichkeit der Verschlusssache vorliegen und die Übermittlung für den Schutz der Verschlusssache erforderlich ist. Die herausgebende Stelle einer Verschlusssache trägt nach dem Sicherheitsüberprüfungsgesetz und der Verschlusssachenanweisung Bund in ihrer herausgehobenen Eigenschaft besondere Verantwortung und legt etwa den Geheimhaltungsgrad der Verschlusssache fest und weist die Verschlusssache in seinem Bestandsverzeichnis nach.

Zu Nummer 18 (geänderte Nummerierung der Abschnitte 6 und 7)

Die Regelung ist eine Folgeanpassung.

Zu Artikel 2 (Änderung des Artikel 10-Gesetzes)

Nummer 1 ergänzt eine Regelung zum Schutz zeugnisverweigerungsberechtigter Personen für Maßnahmen nach § 5 G10.

Die Änderungen in den Nummern 2 bis 4 beschränken die Übermittlungen zusätzlich auf den nach den neuen Übermittlungsvorschriften vorgegebenen, engeren Rahmen.

Zu Nummer 1

Zu Nummer 2

Zu Nummer 3

Zu Buchstabe a

Zu Buchstabe b

Zu Nummer 4

Zu Buchstabe a

Zu Buchstabe b

Zu Artikel 3 (Inkrafttreten)

Aufgrund der Vorgaben des Bundesverfassungsgerichts zur Umsetzung der novellierten Übermittlungsvorschriften tritt das Gesetz am 1. Januar 2024 in Kraft.

ENTWURF