

Referentenentwurf des Bundeskanzleramtes

Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts

A. Problem und Ziel

Das Bundesverfassungsgericht hat mit seiner Entscheidung vom 19. Mai 2020 - 1 BvR 2835/17 (Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes) die §§ 6, 7, 13 bis 15 des Gesetzes über den Bundesnachrichtendienst (BNDG) für mit Artikel 10 Absatz 1 des Grundgesetzes (GG) sowie mit Artikel 5 Absatz 1 GG nicht vereinbar erklärt und dem Gesetzgeber eine Frist für eine verfassungskonforme Neuregelung bis spätestens zum 31. Dezember 2021 gesetzt. Entsprechendes gilt für § 19 Absatz 1 und § 24 Absatz 1 Satz 1, Absatz 2 Satz 1 und Absatz 3 BNDG, soweit sie zur Verarbeitung personenbezogener Daten berechtigen.

Der gesetzliche Auftrag des Bundesnachrichtendienstes ist die Gewinnung von Erkenntnissen über das Ausland, die von außenpolitischer oder sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind. Hierdurch leistet der Bundesnachrichtendienst einen herausgehobenen Beitrag für die Sicherheitsarchitektur der Bundesrepublik Deutschland.

Die strategische Fernmeldeaufklärung stellt in diesem Zusammenhang ein wesentliches Element dar. Durch sie ist der Bundesnachrichtendienst in der Lage, ohne Zeitverzug aktuelle Geschehnisse zu erfassen und politische Bedarfsträger und auch internationale Partner hierüber zu informieren.

In einer globalisierten und technisch vernetzten Welt gewinnt die technische Aufklärung durch Nachrichtendienste eine zunehmend große Bedeutung. Um Gefahrenbereiche umfassend aufklären zu können, ist es für die Arbeit des Bundesnachrichtendienstes unerlässlich, mit den technischen Entwicklungen einer mehr und mehr vernetzten Welt mithalten zu können. Die genutzten Kommunikationsformen sind volatil und fortlaufenden Veränderungen unterworfen.

Schon im Zuge der letzten Novellierung des BND-Gesetzes im Jahr 2016 wurde versucht, dieser Entwicklung durch die Schaffung rechtssicherer und bestimmter Normen zu begegnen.

Stützte der Bundesnachrichtendienst zuvor die Durchführung der strategischen Ausland-Fernmeldeaufklärung allein auf die gesetzliche Aufgabenzuweisungsnorm des § 1 Absatz 2 BNDG, wurde im Rahmen der letzten Novelle die Rechtslage präzisiert und es wurden spezielle rechtliche Grundlagen für die strategische Ausland-Fernmeldeaufklärung vom Inland aus sowie für eine diesbezügliche Kooperation mit ausländischen öffentlichen Stellen anderer Staaten geschaffen. Auch die gemeinsame Datenhaltung mit ausländischen öffentlichen Stellen wurde auf eine spezielle Rechtsgrundlage gestellt.

Mit seinem Urteil vom 19. Mai 2020 (1 BvR 2835/17) hat das Bundesverfassungsgericht erstmals entschieden, dass sich auch Ausländer im Ausland auf den Schutzbereich des Artikels 10 Absatz 1 GG und des Artikels 5 Absatz 1 GG berufen können.

Um diesen verfassungsgerichtlichen Vorgaben gerecht zu werden, müssen die einschlägigen Normen des BNDG grundlegend überarbeitet werden. Dabei sollte der hervorgehobenen Rolle einer wirksamen Auslandsaufklärung und damit des Bundesnachrichtendienstes im Rahmen der Sicherheitsarchitektur der Bundesrepublik Deutschland Rechnung getragen werden.

Das Bundesverfassungsgericht betont in seiner Entscheidung vom 19. Mai 2020 das überragende öffentliche Interesse an einer wirksamen Auslandsaufklärung (BVerfG 1 BvR 2835/17, Randnummer 161). In diesem Zusammenhang wird unterstrichen, dass die Versorgung der Bundesregierung mit Informationen für ihre außen- und sicherheitspolitischen Entscheidungen, ihr hilft, sich im machtpolitischen Kräftefeld der internationalen Beziehungen zu behaupten, und folgenreiche Fehlentscheidungen verhindert werden können (BVerfG, a.a.O., Randnummer 162). Insoweit geht es nach Auffassung des Bundesverfassungsgerichtes mittelbar zugleich um die Bewahrung demokratischer Selbstbestimmung und den Schutz der verfassungsrechtlichen Ordnung – und damit um Verfassungsgüter von hohem Rang. In Frage stehe mithin ein gesamtstaatliches Interesse, das über das Interesse an der Gewährleistung der inneren Sicherheit als solcher deutlich hinausgeht (BVerfG, a.a.O., Randnummer 162).

Das Bundesverfassungsgericht betont zudem, dass im Zuge der Entwicklung der Informationstechnik und der internationalen Kommunikation, ebenso wie damit der engeren grenzüberschreitenden Verflechtung der Lebensbedingungen im Allgemeinen, Bedrohungen vom Ausland aus erheblich zugenommen haben. Die Früherkennung von Gefahrenlagen, die aus dem Ausland drohen, gewinnt dabei nach Einschätzung des Bundesverfassungsgerichtes auch für die Sicherheit eine besondere Bedeutung. Die Erweiterung und Internationalisierung der Kommunikationsmöglichkeiten und die damit gesteigerte Politisierung und Organisationsfähigkeit international agierender krimineller Gruppierungen führe dazu, dass innerstaatliche Gefahrenlagen oftmals durch Netzwerke international zusammenarbeitender Akteure begründet sind und leicht eine außen- und sicherheitspolitische Dimension erhalten können. Derartige Aktivitäten zielen zum Teil auf eine Destabilisierung des Gemeinwesens und können zur Bedrohung für die verfassungsmäßige Ordnung, den Bestand und die Sicherheit des Bundes oder der Länder sowie für Leib, Leben und Freiheit werden. Dies sind Rechtsgüter von überragendem verfassungsrechtlichem Gewicht, für deren Schutz der Gesetzgeber eine wirksame und zugleich rechtsstaatlich eingehegte Auslandsaufklärung als unverzichtbar ansehen kann (BVerfG, a.a.O., Randnummer 163).

Das Bundesverfassungsgericht betont darüber hinaus, dass dem ungleich weiteren Datenzugriff der strategischen Überwachung heute im Verhältnis zu der Situation der Entscheidung des Bundesverfassungsgerichtes im Jahr 1999 ein gesteigertes Gefahrenpotential gegenüberstehe. Vor allem aber hebt das Bundesverfassungsgericht hervor, dass ein wichtiger Gesichtspunkt für die Rechtfertigungsfähigkeit der strategischen Telekommunikationsüberwachung darin liege, dass die Folgen dadurch etwas abgemildert werden, dass sie durch eine Behörde vorgenommen wird, die selbst grundsätzlich keine operativen Befugnisse habe (BVerfG, a.a.O., Randnummer 164f.). Da die Daten gerade von einer Behörde erhoben werden, die keine eigenen operativen Befugnisse hat, ist eine weitere Datenverwendung zunächst von einer in Distanz zu eigenen Handlungsverantwortlichkeiten vorgenommenen Sichtung der Daten abhängig. Erst ihre Übermittlung zur operativen Nutzung muss daher durch qualifizierte Übermittlungsschwellen sichergestellt werden (BVerfG, a.a.O., Randnummer 165).

Gleichzeitig stellt das Bundesverfassungsgericht klar, dass die Befugnisse zur strategischen Überwachung, zur Übermittlung der mit ihr gewonnenen Erkenntnisse und zur diesbezüglichen Zusammenarbeit mit ausländischen Diensten nur dann mit den Anforderungen der Verhältnismäßigkeit vereinbar sind, wenn sie durch eine unabhängige objektivrechtliche Kontrolle flankiert sind. Diese Kontrolle ist als kontinuierliche Rechtskontrolle auszugestalten, die einen umfassenden Kontrollzugriff ermöglicht. Hierfür fordert das Bundesverfassungsgericht eine mit abschließenden Entscheidungsbefugnissen verbundene gerichtsähnliche Kontrolle, der die wesentlichen Verfahrensschritte der strategischen Fernmeldeaufklärung unterliegen, sowie eine administrative Kontrolle, die eigeninitiativ stichprobenmäßig den gesamten Prozess der strategischen Fernmeldeaufklärung auf seine Rechtmäßigkeit prüfen kann (BVerfG, a.a.O., Randnummer 272ff.). Zu gewährleisten ist eine Kontrolle in institutioneller Eigenständigkeit. Hierzu gehören ein eigenes Budget, eine eigene Personalhoheit sowie Verfahrensautonomie. Die Kontrollorgane sind personell wie sachlich so auszugestalten, dass sie ihre Aufgaben wirksam wahrnehmen können (BVerfG, a.a.O., Randnummer 282ff.). Sie müssen gegenüber dem Bundesnachrichtendienst alle für eine effektive Kontrolle erforderlichen Befugnisse haben und die Kontrolle darf nicht durch die „Third Party Rule“ behindert werden (BVerfG, a.a.O., Randnummer 292ff.).

Neben der Entscheidung des Bundesverfassungsgerichts setzt die Novellierung auch die Vorgaben zweier Entscheidungen des Bundesverwaltungsgerichts vom 13. Dezember 2017 (BVerwG 6 A 6.16 und 6 A 7.16) um. In diesen Verfahren hatte das Bundesverwaltungsgericht über zwei Klagen gegen das bis zu diesem Zeitpunkt durch den Bundesnachrichtendienst genutzte Verkehrsdatenanalysesystem (VERAS) zu entscheiden. In VERAS wurden Verkehrsdaten der Kommunikation von deutschen Staatsangehörigen, inländischen juristischen Personen oder sich im Bundesgebiet aufhaltende Personen mit dem Ausland gespeichert. Vor ihrer Speicherung wurden die Daten jedoch durch den Bundesnachrichtendienst anonymisiert, sodass diese nicht mehr individualisierbar waren. Das Bundesverwaltungsgericht hat hierin ungeachtet der vor der Speicherung vorgenommenen Anonymisierung einen Eingriff in den Schutzbereich des Artikels 10 Absatz 1 GG gesehen. Solche Eingriffe sind demnach nur zulässig, wenn sie auf eine spezielle gesetzliche Rechtsgrundlage gestützt werden könnten. Diese fehlte zum Zeitpunkt der Entscheidung des Bundesverwaltungsgerichts jedoch sowohl im BNDG wie auch im Artikel 10-Gesetz und wird nunmehr geschaffen.

Das Ziel dieser grundlegenden Novelle der bestehenden Rechtslage des Bundesnachrichtendienstes ist es somit – in Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts –, die Arbeit des Bundesnachrichtendienstes im Rahmen der technischen Aufklärung und der Weiterverarbeitung der so erhobenen Daten auf eine rechtssichere und bestimmte Rechtsgrundlage zu stellen. Damit soll auch für die Zukunft eine wirksame und zugleich rechtsstaatlich eingehegte Auslandsaufklärung mit technischen Mitteln ermöglicht werden.

B. Lösung

Die Novellierung des BNDG führt zu einer rechtskonformen Ausgestaltung der Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 19. Mai 2020 (1 BvR 2835/17) indem sie diese umsetzt und das Gesetz zudem in inhaltlicher und systematischer Hinsicht anpasst. Darüber hinaus dient die Novellierung der Umsetzung von zwei Entscheidungen des Bundesverwaltungsgerichts vom 13. Dezember 2017 (BVerwG 6 A 6.16 und 6 A 7.16).

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

[...]

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht kein zusätzlicher Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Ein über den bisher bestehenden Erfüllungsaufwand hinausgehenden weiterer Erfüllungsaufwand für die Wirtschaft entsteht nicht.

E.3 Erfüllungsaufwand der Verwaltung

[...]

F. Weitere Kosten

Keine.

Referentenentwurf des Bundeskanzleramtes

Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1 Änderung des BNDG

Das BND-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch Artikel 19 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:

1. In der Überschrift des Abschnitts 1 werden die Wörter „des Bundesnachrichtendienstes“ gestrichen.
2. In § 1 Absatz 2 Satz 2 werden die Wörter „nach den §§ 2 bis 15, 19 bis 21 sowie 23 bis 32“ durch die Wörter „nach Satz 1 sowie den §§ 2 bis 8, 10 bis 39, sowie 59 bis 63“ ersetzt.
3. § 3 Absatz 3 wird aufgehoben.
4. § 4 Satz 4 wird aufgehoben.
5. § 5 wird wie folgt geändert:
 - a) In Satz 1 werden die Wörter „die Mittel gemäß § 8 Absatz 2 des Bundesverfassungsschutzgesetzes“ durch die Wörter „nachrichtendienstliche Mittel“ ersetzt.
 - b) In Satz 2 werden die Wörter „Die §§ 9, 9a und 9b“ durch die Wörter „§ 8 Absatz 2 und die §§ 9, 9a und 9b“ ersetzt.
 - c) Folgender Satz wird angefügt:
„§ 1 Absatz 2 Satz 1 bleibt unberührt.“
6. In der Überschrift des Abschnitts 2 werden die Wörter „Ausland-Ausland-Fernmeldeaufklärung“ durch die Wörter „Weiterverarbeitung von Daten“ ersetzt.
7. Die §§ 6 bis 18 werden aufgehoben.
8. Die Überschrift des Abschnitts 3 wird gestrichen.
9. Die bisherigen §§ 19 bis 21 werden die §§ 6 bis 8.
10. Der bisherige § 22 wird § 9 und in Satz 1 wird die Angabe „§ 19“ durch die Angabe „§ 6“ ersetzt.

11. Die Überschrift des Abschnitts 4 wird durch folgende Überschrift ersetzt:

„Abschnitt 3
Übermittlung von Daten und gemeinsame Dateien“.

12. Der bisherige § 23 wird § 10 und wird wie folgt geändert:

- a) In der Überschrift wird das Wort „Informationen“ durch die Wörter „personenbezogenen Daten“ ersetzt.
- b) In Absatz 1 Satz 1 werden die Wörter „Informationen einschließlich personenbezogener“ durch das Wort „personenbezogenen“ ersetzt.
- c) In Absatz 2 wird wie folgt geändert:
 - aa) In Satz 1 werden die Wörter „Informationen einschließlich personenbezogener“ durch das Wort „personenbezogenen“ ersetzt.
 - bb) In Satz 2 werden die Wörter „Informationen einschließlich personenbezogener“ durch das Wort „personenbezogenen“ ersetzt.
- d) In Absatz 3 Satz 1 werden die Wörter „Informationen einschließlich personenbezogener“ durch das Wort „personenbezogenen“ ersetzt.

13. Der bisherige § 24 wird § 11 und wird wie folgt geändert:

- a) In der Überschrift wird das Wort „Informationen“ durch die Wörter „personenbezogenen Daten“ ersetzt.
- b) Absatz 1 wird wie folgt geändert:
 - aa) In Satz 1 werden die Wörter „Informationen einschließlich“ gestrichen und das Wort „personenbezogener“ durch das Wort „personenbezogene“ ersetzt.
 - bb) In Satz 2 werden die Wörter „Informationen einschließlich personenbezogener Daten“ durch die Wörter „Personenbezogene Daten“ ersetzt.
 - cc) In Absatz 2 Satz 1 werden die Wörter „Informationen einschließlich personenbezogener“ durch das Wort „personenbezogenen“ ersetzt und es wird die Angabe „§ 19 Abs. 2 bis 5“ die die Wörter „§ 19 Absatz 3 bis 5“ ersetzt.
- c) In Absatz 3 werden die Wörter „Informationen einschließlich personenbezogener“ durch das Wort „personenbezogene“ ersetzt.

14. Der bisherige § 25 wird § 12 und wird wie folgt geändert:

- a) Absatz 1 wird wie folgt geändert:
 - aa) In Satz 1 werden nach dem Wort „Zollkriminalamt“ die Wörter „und Dienststellen im Geschäftsbereich des Bundesministeriums der Verteidigung“ eingefügt.
 - bb) Satz 2 wird wie folgt geändert:
 - aaa) In Nummer 2 wird der Punkt am Ende durch ein Komma ersetzt.
 - bbb) Folgende Nummer 3 eingefügt:

„3. den Schutz der Funktionsfähigkeit der Bundeswehr für die Landes- oder Bündnisverteidigung sowie den Schutz der Funktionsfähigkeit der Bundeswehr bei Auslandseinsätzen.“
- b) Absatz 3 wird wie folgt geändert:

- aa) In Satz 1 werden nach dem Wort „Datei“ die Wörter „durch den Bundesnachrichtendienst“ eingefügt und es wird die Angabe „§§ 19 und 20“ durch die Angabe „§§ 6 und 7“ ersetzt.
- bb) In Satz 2 wird die Angabe „§ 22“ durch die Angabe „§ 9“ ersetzt.
- c) Dem Absatz 4 wird folgender Satz angefügt: „Soweit das Ziel der projektbezogenen Zusammenarbeit nach Absatz 1 Satz 2 Nummer 3 sich auf den Schutz der Funktionsfähigkeit der Bundeswehr bei Auslandseinsätzen bezieht und die Datei für die Erreichung dieses Ziels weiterhin erforderlich ist, kann die Frist über Satz 2 hinaus um jeweils ein weiteres Jahr, längstens jedoch bis zum Ende des Auslandseinsatzes verlängert werden.“
- d) Absatz 6 wird wie folgt geändert:
 - aa) In Satz 1 werden im Satzteil vor Nummer 1 vor den Wörtern „für die gemeinsame Datei“ die Wörter „im Fall des Absatzes 3“ eingefügt und es wird die Angabe „§ 21“ durch die Angabe „§ 8“ ersetzt.
 - bb) In Satz 3 werden die Wörter „Der Bundesbeauftragte für Datenschutz“ durch die Wörter „Die oder der Bundesbeauftragte für den Datenschutz“ ersetzt.

15. Der bisherige § 26 wird § 13 und wird wie folgt geändert:

- a) In Absatz 1 Satz 1 werden die Wörter „von nachrichtendienstlichen Informationen und Erkenntnissen“ durch die Wörter „von personenbezogenen Daten“ und es wird die Angabe „(§ 27)“ durch die Angabe „(§ 14)“ sowie die Angabe „(§ 30)“ durch die Angabe „(§ 17)“ ersetzt.
- b) In Absatz 3 Satz 1 werden die Wörter „des Europäischen Wirtschaftsraumes“ durch die Wörter „der Europäischen Freihandelsassoziation“ ersetzt.

16. Der bisherige § 27 wird § 14 und wird wie folgt geändert:

- a) Der Überschrift werden die folgenden Wörter „mit ausländischen öffentlichen Stellen“ angefügt.
- b) In Absatz 1 Satz 1 werden die Wörter „§ 26 Absatz 1 als eigene Datei, muss sich diese auf Informationen und Erkenntnisse“ durch die Wörter „§ 13 Absatz 1 als eigene Datei, muss sich diese auf personenbezogene Daten“ ersetzt.

17. Der bisherige § 28 wird § 15 und der Überschrift werden die Wörter „mit ausländischen öffentlichen Stellen“ angefügt.

18. Der bisherige § 29 wird § 16 und wird wie folgt geändert:

- a) Der Überschrift werden die Wörter „mit ausländischen öffentlichen Stellen“ angefügt.
- b) In Absatz 1 Satz 1 werden die Wörter „Informationen einschließlich personenbezogener Daten“ durch die Wörter „personenbezogenen Daten“ ersetzt und nach dem Wort „Dateien“ die Wörter „mit ausländischen öffentlichen Stellen“ eingefügt.
- c) Absatz 2 Satz 2 wird wie folgt gefasst:
„§ 32 Absatz 4 und 8 sowie § 33 Absatz 1 und 2 gelten entsprechend.“
- d) In Absatz 4 werden nach dem Wort „Durchführung“ die Wörter „von Kontrollen der Datenverarbeitung einschließlich“ eingefügt.

19. Der bisherige § 30 wird § 17 und wird wie folgt geändert:

- a) In Satz 1 wird die Angabe „§ 26“ durch die Angabe „§ 13“ ersetzt.
- b) In Satz 2 wird die Angabe „§ 29“ durch die Angabe „§ 16“ ersetzt.

20. Der bisherige § 31 wird § 18 und wie folgt geändert:

- a) In der Überschrift wird das Wort „Informationen“ durch die Wörter „personenbezogenen Daten“ ersetzt.
- b) Das Wort „Informationen“ wird durch die Wörter „personenbezogenen Daten“ und die Angabe „§ 23 und § 24“ durch die die Angabe „§ 10 und § 11“ ersetzt.

21. Nach dem neuen § 18 wird folgender Abschnitt 4 eingefügt:

„Abschnitt 4 Technische Aufklärung

Unterabschnitt 1

Verarbeitung von personenbezogenen Daten im Rahmen der strategischen Ausland-
Fernmeldeaufklärung

§ 19

Strategische Ausland-Fernmeldeaufklärung

(1) Der Bundesnachrichtendienst darf zur Erfüllung seiner Aufgaben mit technischen Mitteln personenbezogene Inhaltsdaten von Ausländern im Ausland auf der Grundlage zuvor angeordneter strategischer Aufklärungsmaßnahmen verarbeiten (strategische Ausland-Fernmeldeaufklärung), soweit dies erforderlich ist für den Zweck

1. der politischen Unterrichtung der Bundesregierung oder einer Landesregierung oder
2. der Früherkennung von aus dem Ausland drohenden Gefahren von internationaler Bedeutung.

(2) Eine strategische Aufklärungsmaßnahme begrenzt das jeweilige Ziel der strategischen Ausland-Fernmeldeaufklärung durch Angaben zu

1. Aufklärungszweck,
2. Aufklärungsthema,
3. geografischem Fokus und
4. Dauer.

(3) Strategische Aufklärungsmaßnahmen nach Absatz 1 Nummer 1 sind nur zulässig, wenn sie der Gewinnung von Informationen über das Ausland dienen, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind und zu deren Aufklärung das Bundeskanzleramt den Bundesnachrichtendienst beauftragt hat.

(4) Strategische Aufklärungsmaßnahmen nach Absatz 1 Nummer 2 sind nur zulässig, wenn sie der Gewinnung von Informationen über das Ausland dienen, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind und zu deren Aufklärung das Bundeskanzleramt den Bundesnachrichtendienst beauftragt hat sowie tatsächliche Anhaltspunkte dafür vorliegen, dass durch sie Erkenntnisse gewonnen werden können

1. mit Bezug zu den folgenden Gefahrenbereichen:
 - a) zur Landes- oder Bündnisverteidigung sowie Einsätzen der Bundeswehr oder verbündeter Streitkräfte im Ausland,

- b) zu krisenhaften Entwicklungen im Ausland und deren Auswirkungen,
 - c) zu Terrorismus oder Extremismus, der gewaltbereit oder auf die planvoll verborgen betriebene Durchsetzung politischer, religiöser oder ideologischer Ansichten ausgerichtet ist, oder dessen Unterstützung,
 - d) zu internationalen kriminellen, terroristischen oder staatlichen Angriffen mittels Schadprogrammen auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen,
 - e) zur organisierten Kriminalität,
 - f) zur internationalen Verbreitung von Kriegswaffen im Sinne des Gesetzes über die Kontrolle von Kriegswaffen sowie des unerlaubten Außenwirtschaftsverkehrs mit Waren und technischen Unterstützungsleistungen in Fällen von erheblicher Bedeutung,
 - g) zum Schutz kritischer Infrastrukturen oder
 - h) zu hybriden Bedrohungen
2. zum Schutz der folgenden Rechtsgüter
- a) Leib, Leben oder Freiheit einer Person,
 - b) Bestand oder Sicherheit des Bundes oder eines Landes,
 - c) Bestand oder Sicherheit von Einrichtungen der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages oder Bestand oder Sicherheit eines Mitgliedsstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages oder
 - d) außenpolitische Handlungsfähigkeit der Bundesrepublik Deutschland
3. zum Schutz von gewichtigen Rechtsgütern der Allgemeinheit, deren Grundlagen die Existenz
der Menschen berührt.

(5) Der Bundesnachrichtendienst darf die Erhebung von personenbezogenen Inhaltsdaten im Rahmen der strategischen Ausland-Fernmeldeaufklärung nur anhand von Suchbegriffen durchführen. Diese müssen für die strategischen Aufklärungsmaßnahmen nach Absatz 1 bestimmt, geeignet und erforderlich sein und ihre Verwendung muss im Einklang mit den außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland stehen.

(6) Soweit dies zur Durchführung strategischer Aufklärungsmaßnahmen nach Absatz 1 erforderlich ist, darf sich der Bundesnachrichtendienst mit technischen Mitteln Zugang zu informationstechnischen Systemen eines ausländischen Telekommunikations- oder Telemediendiensteanbieters im Ausland auch ohne dessen Wissen verschaffen und personenbezogene Daten, die dieser anlässlich der Erbringung seines Dienstes verarbeitet, aus der laufenden Kommunikation erheben. Dabei darf der Bundesnachrichtendienst auch personenbezogene Daten erheben, die der ausländischen Telekommunikations- oder Telemediendiensteanbieter während seiner Verarbeitung der laufenden Kommunikation in seinen informationstechnischen Systemen speichert, sofern diese innerhalb des Anordnungszeitraums der strategischen Aufklärungsmaßnahme nach Absatz 1 erhoben werden und vor ihrer Erhebung durch den Bundesnachrichtendienst nicht älter als 48 Stunden sind. Verschafft sich der Bundesnachrichtendienst nach Satz 1 Zugang zu einem informationstechnischen System eines ausländischen Telekommunikations- oder Telemediendiensteanbieters im Ausland, darf er auch Bestandsdaten des ausländischen Telekommunikations- oder Telemediendiensteanbieters verarbeiten, die dieser anlässlich der Erbringung seines Dienstes verarbeitet, soweit diese anhand von Suchbegriffen erhoben werden oder sich auf die Gegenstelle der anhand des Suchbegriffs erhobenen Erfassung beziehen.

(7) Eine Erhebung von personenbezogenen Daten der folgenden Personen aus Telekommunikationsverkehren ist unzulässig:

1. deutsche Staatsangehörige,
2. inländische juristische Personen sowie
3. sich im Bundesgebiet aufhaltende Personen.

Soweit technisch möglich, ist durch den Einsatz automatisierter Filter dafür zu sorgen, dass solche Daten herausgefiltert werden. Die herausgefilterten Daten sind unverzüglich automatisiert zu löschen. Die Filtermethoden werden kontinuierlich fortentwickelt und sind auf dem jeweiligen Stand der Technik zu halten. Werden trotz dieser Filterung Daten entgegen Satz 1 erhoben, sind diese Daten unverzüglich zu löschen. Dies gilt nicht, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass durch die Weiterverarbeitung der Daten eine erhebliche Gefahr für Leib, Leben oder Freiheit einer Person, die Sicherheit des Bundes oder eines Landes oder die Sicherheit anderer Mitgliedstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages abgewendet werden kann. Werden die Daten nicht unverzüglich gelöscht, ist die G10-Kommission in ihrer nächsten Sitzung zu unterrichten.

(8) Eine unbeschränkte strategische Ausland-Fernmeldeaufklärung ist unzulässig. Das Volumen der strategischen Ausland-Fernmeldeaufklärung ist auf nicht mehr als 30 Prozent der bestehenden Telekommunikationsnetze zu begrenzen.

(9) Eine strategische Ausland-Fernmeldeaufklärung zum Zweck der Erzielung von Wettbewerbsvorteilen (Wirtschaftsspionage) ist unzulässig.

(10) Personenbezogene Daten sind unmittelbar nach der Datenerhebung wie folgt zu kennzeichnen:

1. Angabe des Zwecks der Datenerhebung nach Absatz 1 und
2. Angabe des Mittels der Datenerhebung.

Die Kennzeichnung entfällt bei Übermittlungen.

§ 20

Besondere Formen der strategischen Ausland-Fernmeldeaufklärung

(1) Die gezielte Erhebung von personenbezogenen Daten nach § 19 Absatz 5 von Einrichtungen der Europäischen Union, von öffentlichen Stellen der Mitgliedstaaten der Europäischen Union oder von Unionsbürgerinnen oder darf nur erfolgen, wenn dies erforderlich ist

1. zur Früherkennung von Gefahren im Sinne des § 19 Absatz 4, oder
2. zur Sammlung und Auswertung von Informationen im Sinne des § 19 Absatz 3, soweit ausschließlich Daten über Vorgänge in Drittstaaten gewonnen werden sollen, die von besonderer außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind.

Wird nachträglich erkannt, dass eine gezielte Datenerhebung von Einrichtungen der Europäischen Union, von öffentlichen Stellen der Mitgliedstaaten der Europäischen Union oder von Unionsbürgerinnen oder Unionsbürgern erfolgt ist, dürfen die erhobenen personenbezogenen Daten nur bei Vorliegen der Voraussetzungen des Satzes 1 weiterverarbeitet werden. Anderenfalls sind sie unverzüglich zu löschen.

(2) Die gezielte Erhebung von personenbezogenen Daten von Personen hinsichtlich derer

1. tatsächliche Anhaltspunkte dafür vorliegen, dass sie Verursacher von Gefahren im Sinne des § 19 Absatz 4 sind und
2. eine Übermittlung der erhobenen personenbezogenen Daten zum Zweck der Weiterverarbeitung für Folgemaßnahmen mit unmittelbarer Außenwirkung für den Betroffenen nach Nummer 1 im Bereich der Gefahrenabwehr oder Strafverfolgung beabsichtigt ist,

darf zur Gefahrenfrüherkennung (§ 19 Absatz 1 Nummer 2) nach § 23 Absatz 5 Nummer 2 nur angeordnet werden, wenn bei der Prüfung der Verhältnismäßigkeit die gegenüber diesen Personen gesteigerte Wahrscheinlichkeit belastender Folgen besonders berücksichtigt wurde.

(3) Die individualisierte Überwachung des gesamten Telekommunikationsverkehrs einer Person ist unzulässig.

§ 21

Schutz von Vertraulichkeitsbeziehungen

(1) Die gezielte Erhebung von personenbezogenen Daten nach § 19 Absatz 5 zum Zweck der Erlangung von Daten aus einer Vertraulichkeitsbeziehung ist unzulässig. Vertraulichkeitsbeziehungen im Sinne des Satzes 1 sind solche von Geistlichen, Verteidigern, Rechtsanwälten und Journalisten, die dem Schutz des § 53 Absatz 1 Satz 1 Nummer 1, 2, 3 und 5 sowie Satz 2 der Strafprozessordnung unterfallen würden.

(2) Abweichend von Absatz 1 ist die gezielte Datenerhebung zulässig, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass

1. die in Absatz 1 aufgeführte Person Täter oder Teilnehmer einer der in § 29 Absatz 3 genannten Straftaten ist oder
2. dies notwendig ist zur Verhinderung einer 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.

(3) Sofern erst die Weiterverarbeitung der erhobenen personenbezogenen Daten ergibt, dass diese schutzwürdig nach Absatz 1 sind, dürfen sie nur verwendet werden, wenn die Voraussetzungen des Absatzes 2 vorliegen. Andernfalls sind die Daten unverzüglich zu löschen. Die Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung von Kontrollen der Datenverarbeitung, einschließlich der Datenschutzkontrolle verwendet werden. Die Protokolldaten sind bis zum Ablauf des zweiten auf die Protokollierung folgenden Kalenderjahres aufzubewahren und danach unverzüglich zu löschen.

§ 22

Kernbereichsschutz

(1) Die Datenerhebung zum Zweck der Erlangung von Erkenntnissen über den Kernbereich privater Lebensgestaltung ist unzulässig.

(2) Sofern erst die Weiterverarbeitung der erhobenen personenbezogenen Daten ergibt, dass diese dem Kernbereich privater Lebensgestaltung unterfallen, sind diese unverzüglich zu löschen. Die Löschung ist zu protokollieren. Die Protokolldaten dürfen

ausschließlich zur Durchführung der Datenschutzkontrolle verwendet werden. Die Protokolldaten sind bis zum Ablauf des zweiten auf die Protokollierung folgenden Kalenderjahres aufzubewahren und danach unverzüglich zu löschen.

(3) Bestehen im Rahmen der Weiterverarbeitung nach Absatz 2 Zweifel und sollen die Daten nicht unverzüglich gelöscht werden, dürfen die Daten nicht ohne vorherige Prüfung durch den Unabhängigen Kontrollrat verwendet werden. Stellt der Unabhängige Kontrollrat fest, dass die Daten nicht weiterverarbeitet werden dürfen, sind die Daten unverzüglich zu löschen. Die Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung der Datenschutzkontrolle verwendet werden. Die Protokolldaten sind bis zum Ablauf des zweiten auf die Protokollierung folgenden Kalenderjahres aufzubewahren und danach unverzüglich zu löschen.

§ 23 Anordnung

(1) Strategische Aufklärungsmaßnahmen nach § 19 Absatz 1 bedürfen der Anordnung durch die Präsidentin oder den Präsidenten des Bundesnachrichtendienstes oder durch eine Vertretung, die die Präsidentin oder der Präsident des Bundesnachrichtendienstes bestimmt hat.

(2) Die Anordnung nach Absatz 1 ergeht schriftlich. In der Anordnung sind anzugeben

1. der Aufklärungszweck,
2. das Aufklärungsthema im Sinne des § 19 Absatz 3 oder Absatz 4,
3. der geografische Fokus,
4. die Dauer,
5. eine Begründung.

(3) Bei strategischen Aufklärungsmaßnahmen nach § 19 Absatz 1 Nummer 2 ist bei der Darstellung des Aufklärungsthemas die Art der Gefahr nach § 19 Absatz 4 zu benennen, die aufgeklärt werden soll.

(4) Der Unabhängige Kontrollrat prüft die Rechtmäßigkeit der Anordnung von strategischen Aufklärungsmaßnahmen vor deren Vollzug. Bestätigt der Unabhängige Kontrollrat die Rechtmäßigkeit der Anordnung nicht, tritt die Anordnung außer Kraft. Bei Gefahr im Verzug erfolgt eine vorläufige Prüfung der Rechtmäßigkeit durch ein Mitglied des Unabhängigen Kontrollrats, wenn andernfalls der Aufklärungszweck der strategischen Aufklärungsmaßnahme vereitelt oder wesentlich erschwert würde. Wird im Rahmen der vorläufigen Prüfung festgestellt, dass die Anordnung 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 3 auf, tritt die Anordnung außer Kraft und die bereits erhobenen Daten sind unverzüglich zu löschen.

(5) Die gezielte Datenerhebung nach

1. § 20 Absatz 1, soweit sich diese auf Einrichtungen der Europäischen Union oder auf öffentliche Stellen ihrer Mitgliedstaaten bezieht,
 2. § 20 Absatz 2 und
 3. § 21 Absatz 2
- bedarf der Anordnung durch die Präsidentin oder den Präsidenten des Bundesnachrichtendienstes oder durch eine Vertretung, die die Präsidentin oder der

Präsident des Bundesnachrichtendienstes bestimmt hat. Soweit zu den in Nummer 1 bis 3 genannten Zielen bereits eine Beschränkungsanordnung nach den §§ 3, 5 oder § 8 des Artikel-10-Gesetzes vorliegt, ist die Anordnung nach Satz 1 entbehrlich. Der Unabhängige Kontrollrat ist über entsprechende Beschränkungsanordnungen zu unterrichten.

(6) Die Anordnung nach Absatz 5 Satz 1 ergeht schriftlich. In der Anordnung sind anzugeben

1. die strategische Aufklärungsmaßnahme, in deren Rahmen die gezielte Datenerhebung erfolgt,
2. das Ziel der gezielten Datenerhebung,
3. die Dauer der gezielten Datenerhebung,
4. eine Begründung.

Die Nennung einzelner Suchbegriffe, die zur gezielten Datenerhebung verwendet werden, ist nicht erforderlich.

(7) Der Unabhängige Kontrollrat prüft die Rechtmäßigkeit der Anordnungen der gezielten Datenerhebung vor deren Vollzug. Bestätigt der Unabhängige Kontrollrat die Rechtmäßigkeit der Anordnung nicht, tritt die Anordnung außer Kraft. Bei Gefahr im Verzug erfolgt eine vorläufige Prüfung der Rechtmäßigkeit durch ein Mitglied des Unabhängigen Kontrollrats, wenn andernfalls der Aufklärungszweck der gezielten Datenerhebung vereitelt oder wesentlich erschwert würde. Die Prüfung durch den Unabhängigen Kontrollrat ist unverzüglich nachzuholen. Wird im Rahmen der vorläufigen Prüfung festgestellt, dass die Anordnung 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 3 auf, tritt die Anordnung außer Kraft und die bereits erhobenen Daten sind unverzüglich zu löschen.

(8) Der Bundesnachrichtendienst unterrichtet das Bundeskanzleramt in regelmäßigen Abständen über Anordnungen nach den Absätzen 1 und 5.

§ 24 Eignungsprüfung

(1) Der Bundesnachrichtendienst darf personenbezogene Daten aus Telekommunikationsnetzen erheben und auswerten, soweit dies zur Bestimmung

1. geeigneter Telekommunikationsnetze oder
2. geeigneter Suchbegriffe

im Rahmen strategischer Aufklärungsmaßnahmen nach § 19 Absatz 1 erforderlich ist (Eignungsprüfung).

(2) Eine Eignungsprüfung nach Absatz 1 Nummer 1 darf nur durchgeführt werden, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass in dem zu prüfenden Telekommunikationsnetz geeignete Daten für strategische Aufklärungsmaßnahmen übertragen werden. Die Eignungsprüfung nach Absatz 1 Nummer 1 ist auf sechs Monate zu befristen. Eine mehrmalige Verlängerung um jeweils sechs Monate ist zulässig.

(3) Die Eignungsprüfung nach Absatz 1 Nummer 1 ist durch die Präsidentin oder den Präsidenten des Bundesnachrichtendienstes oder durch eine Vertretung, die die

Präsidentin oder der Präsident des Bundesnachrichtendienstes bestimmt hat, schriftlich anzuordnen.

(4) Ist für die Durchführung der Eignungsprüfung die Mitwirkung eines Unternehmens erforderlich, das geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt und in Deutschland eine Niederlassung hat oder die vorgenannten Dienste oder Mitwirkungshandlungen in Deutschland erbringt, gilt § 25 entsprechend.

(5) Die im Rahmen einer Eignungsprüfung erhobenen personenbezogenen Daten dürfen nur zum Zweck der Eignungsprüfung verwendet werden. § 5 Absatz 7 Satz 2 bis 8 des BSI-Gesetzes gilt entsprechend. Der Bundesnachrichtendienst darf die erhobenen personenbezogenen Daten speichern, soweit dies zur Durchführung der Eignungsprüfung erforderlich ist. Die Auswertung ist unverzüglich nach der Erhebung durchzuführen.

(6) Personenbezogene Daten für eine Eignungsprüfung nach Absatz 1 Nummer 2 sind spätestens zwei Wochen, personenbezogene Daten für eine Eignungsprüfung nach Absatz 1 Nummer 1 spätestens vier Wochen nach ihrer Erhebung zu löschen. Satz 1 findet keine Anwendung auf personenbezogene Daten, sofern und solange deren Inhalte zum Zeitpunkt der Erhebung aus technischen Gründen nicht lesbar gemacht werden können und zu Forschungszwecken benötigt werden. Auch diese Daten, die im Rahmen der Eignungsprüfung erhoben wurden, sind spätestens nach zehn Jahren zu löschen. Die Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung von Kontrollen der Datenverarbeitung, einschließlich der Datenschutzkontrolle, verwendet werden. Die Protokolldaten sind bis zum Ablauf des zweiten auf die Protokollierung folgenden Kalenderjahres aufzubewahren und danach unverzüglich zu löschen.

(7) Abweichend von Absatz 5 Satz 1 ist zulässig,

1. die Weiterverarbeitung der im Rahmen einer Eignungsprüfung erhobenen personenbezogenen Daten, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass eine erhebliche Gefahr besteht für
 - a) Leib, Leben oder Freiheit einer Person oder
 - b) die Sicherheit des Bundes oder eines Landes oder die Sicherheit von Einrichtungen der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages oder der Mitgliedstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages
2. die Übermittlung der im Rahmen einer Eignungsprüfung erhobenen personenbezogenen Daten an die Bundeswehr, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies erforderlich ist
 - a) zum Schutz von Leib, Leben oder Freiheit einer Person,
 - b) zum Schutz der Funktionsfähigkeit der Bundeswehr für die Landes- oder Bündnisverteidigung,
 - c) zum Schutz der Funktionsfähigkeit der Bundeswehr bei Auslandseinsätzen, oder
 - d) zum Schutz der Funktionsfähigkeit der Streitkräfte von Mitgliedstaaten der Europäischen Union, des Nordatlantikvertrages oder der Europäischen Freihandelsassoziation

Eine Übermittlung darf in Fällen des Satzes 1 Nummer 2 auch automatisiert erfolgen. Die Kennzeichnung der Daten gemäß § 19 Absatz 10 erfolgt erst bei der Weiterverarbeitung der Daten nach Satz 1.

§ 25

Pflichten der Anbieter von Telekommunikationsdiensten, Entschädigung

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt und in Deutschland eine Niederlassung hat oder die vorgenannten Dienste oder Mitwirkungshandlungen in Deutschland erbringt, hat dem Bundesnachrichtendienst auf Anordnung des Bundeskanzleramtes Auskunft über die näheren Umstände der nach Wirksamwerden der Anordnung durchgeführten Telekommunikation zu erteilen, Sendungen, die ihm zur Übermittlung auf dem Telekommunikationsweg anvertraut sind, auszuhändigen sowie die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen. Die §§ 3 und 4 bleiben unberührt. Ob und in welchem Umfang das verpflichtete Telekommunikationsunternehmen Vorkehrungen für die technische und organisatorische Umsetzung zu treffen hat, bestimmt sich nach § 110 des Telekommunikationsgesetzes und der dazu erlassenen Rechtsverordnung.

(2) Die Anordnung nach Absatz 1 Satz 1 ergeht schriftlich und ist dem nach Absatz 1 verpflichteten Unternehmen insoweit mitzuteilen, als dies erforderlich ist, um die Erfüllung seiner Verpflichtungen zu ermöglichen. Die Anordnung muss bezeichnen

1. das verpflichtete Unternehmen,
2. die Dauer der Verpflichtung sowie
3. die betroffene Telekommunikation.

(3) Das nach Absatz 1 verpflichtete Unternehmen hat vor Durchführung einer beabsichtigten Maßnahme unverzüglich die Personen, die mit der Durchführung der Maßnahme betraut werden sollen,

1. auszuwählen,
2. einer einfachen Sicherheitsüberprüfung unterziehen zu lassen und
3. über Mitteilungsverbote nach § 60 sowie die Strafbarkeit eines Verstoßes nach § 66 zu belehren; die Belehrung ist aktenkundig zu machen.

Mit der Durchführung einer Maßnahme dürfen nur Personen betraut werden, die nach Maßgabe des Satzes 1 überprüft und belehrt worden sind. Nach Zustimmung des Bundeskanzleramtes kann die Präsidentin oder der Präsident des Bundesnachrichtendienstes oder eine Vertretung, die die Präsidentin oder der Präsident des Bundesnachrichtendienstes bestimmt hat, die nach Absatz 1 verpflichteten Unternehmen schriftlich auffordern, die Maßnahme bereits vor Abschluss der Sicherheitsüberprüfung durchzuführen. Die nach Absatz 1 verpflichteten Unternehmen haben sicherzustellen, dass die Geheimschutzmaßnahmen nach der vom Bundesministerium des Innern, für Bau und Heimat erlassenen Verschlusssachenanweisung vom 10. August 2018 (GMBl. 2018 Nr. 44 – 47, S. 826) in der jeweils geltenden Fassung getroffen werden.

(4) Die Sicherheitsüberprüfung nach Absatz 3 Satz 1 Nummer 2 ist entsprechend dem Sicherheitsüberprüfungsgesetz durchzuführen. Zuständig ist das Bundesministerium des Innern, für Bau und Heimat. Soll mit der Durchführung einer Maßnahme eine Person betraut werden, für die innerhalb der letzten fünf Jahre bereits eine gleich- oder

höherwertige Sicherheitsüberprüfung nach Bundes- oder Landesrecht durchgeführt worden ist, soll von einer erneuten Sicherheitsüberprüfung abgesehen werden.

(5) Der Bundesnachrichtendienst vereinbart mit den nach Absatz 1 verpflichteten Unternehmen für die dort genannten Leistungen eine Entschädigung, deren Höhe sich an den nachgewiesenen tatsächlichen Kosten orientiert.

§ 26

Verarbeitung von personenbezogenen Verkehrsdaten

(1) Der Bundesnachrichtendienst darf im Rahmen von strategischen Aufklärungsmaßnahmen nach § 19 Absatz 1 auch Verkehrsdaten verarbeiten. § 19 Absatz 6 Satz 1 und 2 gelten entsprechend.

(2) Die Kennzeichnung erfolgt abweichend von § 19 Absatz 10 erst bei der Weiterverarbeitung der Daten im Rahmen der manuellen Auswertung.

(3) Eine Verarbeitung von personenbezogenen Verkehrsdaten der folgenden Personen ist unzulässig:

1. deutsche Staatsangehörige,
2. inländische juristische Personen und
3. sich im Bundesgebiet aufhaltende Personen.

Satz 1 gilt nicht, sofern

1. ausschließlich Daten, die im Rahmen des automatisierten Informationsaustausches zwischen informationstechnischen Systemen ohne unmittelbaren Bezug zu einem konkreten menschlichen Kommunikationsvorgang anfallen, verarbeitet werden oder
2. diejenigen Verkehrsdaten, eine Identifizierung der in Satz 1 genannten Personen ermöglichen, unverzüglich nach ihrer Erhebung automatisiert unkenntlich gemacht werden.

Die automatisierte Unkenntlichmachung nach Satz 2 Nummer 2 ist so durchzuführen, dass die Eindeutigkeit der Daten erhalten bleibt und eine rückwirkende Identifizierung der in Satz 1 genannten Personen unmöglich oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Der Bundesnachrichtendienst darf Verkehrsdaten, die nach Satz 2 Nummer 2 unkenntlich gemacht wurden, zur Erfüllung seiner Aufgaben weiterverarbeiten, um

1. Personen außerhalb des in Satz 1 genannten Personenkreises zu erkennen, die einen Deutschlandbezug aufweisen und über die Informationen erlangt werden können, die für die Aufgabenerfüllung des Bundesnachrichtendienstes relevant sind, sowie
2. geeignete Übertragungswege im Sinne des § 10 Absatz 4 Satz 2 des Artikel 10-Gesetzes zu bestimmen.

(4) Ergibt erst die Datenauswertung, dass Daten entgegen Absatz 3 Satz 2 Nummer 2 nicht unkenntlich gemacht wurden, sind diese Daten unverzüglich entsprechend Absatz 3 Satz 3 unkenntlich zu machen. Werden die Daten nicht unverzüglich unkenntlich gemacht, so sind sie unverzüglich zu löschen. Dies gilt nicht, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass durch die Weiterverarbeitung der Daten eine erhebliche Gefahr für Leib, Leben oder Freiheit einer Person, die Sicherheit des Bundes oder eines Landes oder die Sicherheit anderer Mitgliedstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages abgewendet werden kann. Werden die Daten nicht unverzüglich unkenntlich gemacht oder gelöscht, ist die G10-Kommission in ihrer nächsten Sitzung zu unterrichten.

(5) Die Verkehrsdaten werden höchstens sechs Monate gespeichert. Eine darüber hinaus gehende Speicherung ist im Einzelfall möglich, soweit die Speicherung für die Aufgabenerfüllung des Bundesnachrichtendienstes weiterhin erforderlich ist. Für die weitere Speicherung gilt § 27 entsprechend.

§ 27

Auswertung der Daten und Prüfpflichten

(1) Der Bundesnachrichtendienst prüft die anhand von Suchbegriffen erhobenen personenbezogenen Inhaltsdaten unverzüglich und sodann regelmäßig in Abständen von höchstens sieben Jahren daraufhin, ob sie allein oder zusammen mit bereits vorliegenden Daten für die in § 19 Absatz 1 bestimmten Zwecke erforderlich sind. Hierbei ist auf den jeweiligen Zweck der Erhebung gemäß § 19 Absatz 1 abzustellen. Soweit die personenbezogenen Daten für diese Zwecke nicht erforderlich sind, sind sie unverzüglich zu löschen. Die Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung von Kontrollen der Datenverarbeitung, einschließlich der Datenschutzkontrolle, verwendet werden. Die Protokolldaten sind bis zum Ablauf des zweiten auf die Protokollierung folgenden Kalenderjahres aufzubewahren und danach unverzüglich zu löschen.

(2) Die Löschung der Daten unterbleibt, solange und soweit die Daten für eine Mitteilung nach § 59 oder zu Kontrollzwecken des Unabhängigen Kontrollrats erforderlich sind.

§ 28

Datenerhebung durch eine ausländische öffentliche Stelle

(1) Der Bundesnachrichtendienst darf ausländische öffentliche Stellen zur Durchführung strategischer Aufklärungsmaßnahmen ersuchen.

(2) Der Bundesnachrichtendienst darf die von der ausländischen öffentlichen Stelle erhobenen Daten verarbeiten. Die in diesem Unterabschnitt geregelten Vorschriften zur Datenverarbeitung finden entsprechende Anwendung.

(3) Soweit die ausländische öffentliche Stelle zur Datenerhebung Suchbegriffe des Bundesnachrichtendienstes verwendet, müssen diese Suchbegriffe die Voraussetzungen des § 19 Absatz 5 und der §§ 20 bis 22 und 23 Absatz 5 erfüllen. Die ausländische öffentliche Stelle darf diese Suchbegriffe für eigene Zwecke nur nach vorheriger Zustimmung des Bundesnachrichtendienstes nutzen. Eine solche Zustimmung kann erteilt werden, wenn eine Übermittlung der Suchbegriffe nach § 30 zulässig wäre.

Unterabschnitt 2

Übermittlung von personenbezogenen Daten aus der strategischen Ausland-Fernmeldeaufklärung

§ 29

Übermittlung von personenbezogenen Daten aus der strategischen Ausland-Fernmeldeaufklärung an inländische öffentliche Stellen und andere inländische Stellen

(1) Der Bundesnachrichtendienst darf an das Bundesamt für Verfassungsschutz, die Verfassungsschutzbehörden der Länder und an den Militärischen Abschirmdienst übermitteln:

1. die mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten, wenn tatsächliche Anhaltspunkte dafür bestehen, dass dies erforderlich ist zum Schutz besonders gewichtige Rechtsgüter und
2. die mit dem Zweck der politischen Unterrichtung oder mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten zum Zweck der Unterrichtung der Bundesregierung oder einer Landesregierung, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung zur Erfüllung seiner Aufgaben oder der Aufgaben der Empfänger erforderlich ist.

(2) Der Bundesnachrichtendienst darf die mit dem Zweck der politischen Unterrichtung oder mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten an andere inländische öffentliche Stellen zum Zweck der Unterrichtung der Bundesregierung oder einer Landesregierung übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung zur Erfüllung seiner Aufgaben oder der Aufgaben der Empfänger erforderlich ist.

(3) Der Bundesnachrichtendienst darf die mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten an Strafverfolgungsbehörden übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass dies erforderlich ist zur Verfolgung von

1. Straftaten nach § 100b Absatz 2 der Strafprozessordnung oder
2. vorsätzlichen Straftaten nach den §§ 17 und 18 des Außenwirtschaftsgesetzes.

(4) Der Bundesnachrichtendienst darf die mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten an die in Absatz 2 genannten Stellen auch zum Zweck der Weiterverarbeitung für Folgemaßnahmen mit unmittelbarer Außenwirkung für den Betroffenen, insbesondere zur Gefahrenabwehr, übermitteln,

1. soweit dies in anderen Rechtsvorschriften vorgesehen ist oder
2. wenn tatsächliche Anhaltspunkte dafür bestehen, dass dies erforderlich ist zur Abwehr einer Gefahr für besonders gewichtige Rechtsgüter oder zur Abwehr einer besonders schwerwiegenden Beeinträchtigung der Rechte Einzelner.

(5) Der Bundesnachrichtendienst darf die mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten an die Bundeswehr übermitteln, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies erforderlich ist

1. zum Schutz der Funktionsfähigkeit der Bundeswehr für die Landes- oder Bündnisverteidigung und bei Auslandseinsätzen,
2. zum Schutz der Funktionsfähigkeit der Streitkräfte von Mitgliedstaaten der Europäischen Union, des Nordatlantikvertrages oder der Europäischen Freihandelsassoziation
3. zum Schutz von Leib, Leben oder Freiheit einer Person, oder
4. zum Schutz von anderen besonders gewichtigen Rechtsgütern.

Die in Satz 1 genannten personenbezogenen Daten darf der Bundesnachrichtendienst auch automatisiert an die Bundeswehr übermitteln, sofern diese auf Grundlage von Suchbegriffen erhoben wurden, die strategischen Aufklärungsmaßnahmen nach § 19 Absatz 4 Nummer 1 Buchstabe a) oder Nummer 2 Buchstabe a zugeordnet sind.

(6) Der Bundesnachrichtendienst darf die mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten an andere inländische Stellen

übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung erforderlich ist,

1. zum Schutz der freiheitlich demokratischen Grundordnung,
2. des Bestandes oder der Sicherheit des Bundes oder eines Landes oder
3. zur Gewährleistung der Sicherheit von lebenswichtigen Gütern der Allgemeinheit, insbesondere zum Schutz von Einrichtungen kritischer Infrastruktur.

Übermittlungen nach Satz 1 bedürfen der vorherigen Zustimmung durch das Bundeskanzleramt. Der Bundesnachrichtendienst darf personenbezogene Daten an andere inländische Stellen auch ohne Vorliegen der Voraussetzungen der Sätze 1 und 2 übermitteln, wenn sie lediglich zur Konkretisierung einer Anfrage an eine andere Stelle übermittelt werden und dieser die Daten bereits bekannt sind.

(7) Der Bundesnachrichtendienst darf die mit dem Zweck der politischen Unterrichtung der Bundesregierung gekennzeichneten personenbezogenen Daten an inländische öffentliche Stellen über die Absätze 1 und 2 hinaus auch übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass eine Übermittlung erforderlich ist zur Verhinderung einer unmittelbar bevorstehenden Gefahr für

1. Leib, Leben oder Freiheit einer Person,
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.

In Fällen von Satz 1 Nummer 1 ist über Absatz 6 hinaus auch eine Übermittlung an andere inländische Stellen zulässig.

(8) Eine Übermittlung von personenbezogenen Daten aus einer Vertraulichkeitsbeziehung (§ 21 Absatz 1 Satz 2) ist unzulässig. Abweichend von Satz 1 ist eine Übermittlung zulässig, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass

1. die in § 21 Absatz 1 Satz 2 aufgeführte Person Täter oder Teilnehmer einer der in Absatz 3 genannten Straftaten ist oder
2. dies erforderlich ist zur Verhinderung einer 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.

(9) Eine Übermittlung personenbezogener Daten von Minderjährigen vor Vollendung des 14. Lebensjahres darf nur erfolgen, wenn tatsächliche Anhaltspunkte dafür bestehen, dass der Minderjährige einer der in § 3 Absatz 1 des Artikel 10-Gesetzes genannten Straftaten plant, begeht oder begangen hat oder wenn nach den Umständen des Einzelfalls nicht ausgeschlossen werden kann, dass von dem Minderjährigen eine Gefahr für Leib oder Leben deutscher Staatsangehöriger im Ausland oder für deutsche Einrichtungen im Ausland ausgeht. Eine Übermittlung personenbezogener Daten von Minderjährigen nach Vollendung des 14. Lebensjahres darf nur erfolgen, wenn dies zur Abwehr einer erheblichen Gefahr oder zur Verfolgung einer Straftat von erheblicher Bedeutung erforderlich ist.

(10) Eine Übermittlung unterbleibt, wenn

1. für den Bundesnachrichtendienst 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. überwiegende Sicherheitsinteressen entgegenstehen oder
3. besondere gesetzliche Weiterverarbeitungsregelungen entgegenstehen; die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- und Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(11) Die Verantwortung für die Zulässigkeit der Übermittlung trägt der Bundesnachrichtendienst. Erfolgt die Übermittlung auf Ersuchen einer inländischen öffentlichen Stelle, trägt diese die Verantwortung. In den Fällen des Satzes 2 prüft der Bundesnachrichtendienst nur, ob das Übermittlungersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht.

(12) Der Bundesnachrichtendienst hat den Empfänger darauf hinzuweisen, zu welchen Zwecken die Daten verarbeitet werden dürfen. Der Empfänger darf die personenbezogenen Daten nur zu den Zwecken verarbeiten, zu denen sie ihm übermittelt worden sind. Der Empfänger ist verpflichtet, dem Bundesnachrichtendienst auf Verlangen Auskunft zu erteilen. Hierauf ist der Empfänger bei der Übermittlung hinzuweisen. Eine Weiterverarbeitung zu anderen Zwecken ist unzulässig, es sei denn, es liegen die Voraussetzungen des Absatz 7 vor und der Bundesnachrichtendienst stimmt der Zweckänderung zu. Der Bundesnachrichtendienst darf einer über Satz 5 hinausgehenden Zweckänderung der mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten Daten auf Ersuchen des Empfängers zustimmen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass diese zum Schutz vergleichbar bedeutsamer Rechtsgüter erforderlich ist.

(13) Der Empfänger prüft, ob die übermittelten personenbezogenen Daten für die Erfüllung seiner Aufgaben erforderlich sind. Ergibt die Prüfung, dass sie nicht erforderlich sind, hat er die Daten zu löschen. Die Löschung kann unterbleiben, wenn die Trennung von anderen Informationen, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit übermäßigem Aufwand möglich ist. In diesem Fall ist die Verarbeitung der Daten einzuschränken.

(14) Sind mit personenbezogenen Daten weitere personenbezogene Daten der betroffenen Person oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit übermäßigem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechnete Interessen der betroffenen Person oder eines Dritten an der Geheimhaltung offensichtlich überwiegen. Eine Weiterverarbeitung dieser Daten ist unzulässig.

(15) Erweisen sich personenbezogene Daten nach ihrer Übermittlung als unvollständig oder unrichtig, so sind diese unverzüglich gegenüber dem Empfänger zu berichtigen, es sei denn, dass dies für die Beurteilung des Sachverhaltes ohne Bedeutung ist.

(16) Die Empfänger, die Rechtsgrundlage für die Übermittlung sowie der Zeitpunkt der Übermittlung sind zu protokollieren. Die Protokolldaten sind bis zum Ablauf des zweiten auf die Protokollierung folgenden Kalenderjahres aufzubewahren und danach unverzüglich zu löschen.

§ 30

Übermittlung personenbezogener Daten aus der strategischen Ausland-Fernmeldeaufklärung an ausländische öffentliche Stellen, über- und zwischenstaatliche Stellen sowie an andere ausländische Stellen

(1) Der Bundesnachrichtendienst darf die mit dem Zweck der politischen Unterrichtung oder mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten zum Zweck der Unterrichtung im Rahmen der internationalen politischen Zusammenarbeit an ausländische öffentliche Stellen sowie über- und zwischenstaatliche Stellen übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung zur Erfüllung seiner Aufgaben erforderlich ist.

(2) Der Bundesnachrichtendienst darf die mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten an die in Absatz 1 genannten Stellen übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass dies erforderlich ist zur Verfolgung von Straftaten, die den in § 29 Absatz 3 genannten Straftaten entsprechen. Die Regelungen des Gesetzes über die internationale Rechtshilfe in Strafsachen bleiben unberührt.

(3) Der Bundesnachrichtendienst darf die mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten an die in Absatz 1 genannten Stellen auch zum Zweck der Weiterverarbeitung für Folgemaßnahmen mit unmittelbarer Außenwirkung für den Betroffenen, insbesondere zur Gefahrenabwehr, übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass

1. dies erforderlich ist zur Abwehr einer Gefahr für besonders gewichtige Rechtsgüter oder zur Abwehr einer besonders schwerwiegenden Beeinträchtigung der Rechte Einzelner, oder
2. die Übermittlung für den Bestand oder die Sicherheit des Bundes oder eines Landes, zur Wahrung erheblicher außenpolitischer Belange des Bundes oder eines Landes oder für die Sicherheit des Empfängerstaates erforderlich ist.

(4) Eine Übermittlung personenbezogener Daten an andere ausländische Stellen ist unzulässig. Abweichend von Satz 1 darf der Bundesnachrichtendienst die im Rahmen der strategischen Ausland-Fernmeldeaufklärung erhobenen und mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten an die in Satz 1 genannten Stellen übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung erforderlich ist zur Verhinderung einer unmittelbar bevorstehenden Gefahr für

1. Leib, Leben oder Freiheit einer Person,
2. lebenswichtige Güter der Allgemeinheit oder
3. den Bestand oder die Sicherheit des Bundes oder eines Landes oder die Sicherheit eines Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages.

Übermittlungen nach Satz 2 bedürfen der vorherigen Zustimmung durch das Bundeskanzleramt. Der Bundesnachrichtendienst darf personenbezogene Daten an andere ausländische Stellen auch ohne Vorliegen der Voraussetzungen des Satzes 2 und 3 übermitteln, wenn sie lediglich zur Konkretisierung einer Anfrage an eine andere ausländische Stelle übermittelt werden und dieser die Daten bereits bekannt sind.

(5) Der Bundesnachrichtendienst darf die mit dem Zweck der politischen Unterrichtung der Bundesregierung gekennzeichneten personenbezogenen Daten an die in Absatz 1 genannten Stellen über Absatz 1 Satz 1 hinaus auch übermitteln, wenn tatsächliche

Anhaltspunkte dafür bestehen, dass eine Übermittlung erforderlich ist zur Verhinderung einer unmittelbar bevorstehenden Gefahr für

1. Leib, Leben oder Freiheit einer Person,
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.

In Fällen von Satz 1 Nummer 1 ist über Absatz 4 hinaus auch eine Übermittlung an andere ausländische Stellen zulässig.

(6) Eine Übermittlung unterbleibt, wenn für den Bundesnachrichtendienst erkennbar ist, dass unter Berücksichtigung der Art der personenbezogenen Daten und ihrer Erhebung die schutzwürdigen Interessen des Betroffenen das Allgemeininteresse an der Übermittlung überwiegen. Schutzwürdige Interessen des Betroffenen überwiegen insbesondere dann, wenn tatsächliche Anhaltspunkte dafür bestehen, dass durch die Nutzung der übermittelten Daten im Empfängerstaat erhebliche Menschenrechtsverletzungen oder die Verletzung von elementaren rechtsstaatlichen Grundsätzen, wie im Falle der Verwendung der Daten zur politischen Verfolgung oder zu unmenschlicher oder erniedrigender Bestrafung oder Behandlung, drohen. In Zweifelsfällen hat der Bundesnachrichtendienst maßgeblich zu berücksichtigen, ob der Empfänger einen angemessenen Schutz der übermittelten Daten verbindlich zusichert und ob Anhaltspunkte dafür vorliegen, dass die Zusicherung nicht eingehalten wird. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- und Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt. Eine Übermittlung unterbleibt ferner, wenn hierdurch wesentliche Sicherheitsinteressen des Bundes oder der Länder würden, oder wesentliche auswärtige Belange der Bundesrepublik Deutschland beeinträchtigt würden. Bei der Prüfung, ob eine Übermittlung zu unterbleiben hat, berücksichtigt der Bundesnachrichtendienst insbesondere die Art der Information und ihre Erhebung sowie den bisherigen Umgang des Empfängers mit übermittelten Daten. Die Regelungen des Gesetzes über die internationale Rechtshilfe in Strafsachen bleiben unberührt.

(7) Eine Übermittlung personenbezogener Daten Minderjähriger vor Vollendung des 16. Lebensjahres darf weder an ausländische noch an über- und zwischenstaatliche Stellen erfolgen. Abweichend von Satz 1 dürfen personenbezogene Daten über das Verhalten Minderjähriger, die das 14. Lebensjahr vollendet haben, übermittelt werden, wenn nach den Umständen des Einzelfalls nicht ausgeschlossen werden kann, dass die Übermittlung zur Abwehr einer erheblichen Gefahr für Leib oder Leben einer Person erforderlich ist oder tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung zur Verfolgung einer der in § 3 Absatz 1 des Artikel 10-Gesetzes genannten Straftaten erforderlich ist. Eine Übermittlung personenbezogener Daten von Minderjährigen nach Vollendung des 16. Lebensjahres darf nur erfolgen, wenn dies zur Abwehr einer erheblichen Gefahr oder zur Verfolgung einer Straftat von erheblicher Bedeutung erforderlich ist.

(8) Die Verantwortung für die Zulässigkeit der Übermittlung trägt der Bundesnachrichtendienst. Der Empfänger darf die übermittelten Daten nur zu dem Zweck weiterverarbeiten, zu dem sie ihm übermittelt worden sind. Er ist auf die Weiterverarbeitungsbeschränkung und darauf hinzuweisen, dass der Bundesnachrichtendienst sich vorbehält, Auskunft über die Weiterverarbeitung der Daten zu verlangen. Entsprechende Auskunftsrechte sind mit dem Empfänger zu

vereinbaren. Dieser muss auch eine verbindliche Zusicherung abgeben, einer Löschungsaufforderung des Bundesnachrichtendienstes Folge zu leisten. Sofern tatsächliche Anhaltspunkte dafür bestehen, dass eine solche Zusicherung vom Empfänger nicht eingehalten wird, hat eine Übermittlung zu unterbleiben.

(9) § 29 Absatz 8 und 13 bis 16 gilt entsprechend.

Unterabschnitt 3 Kooperation im Rahmen der strategischen Ausland-Fernmeldeaufklärung.

§ 31 Kooperationen mit ausländischen öffentlichen Stellen

(1) Soweit der Bundesnachrichtendienst im Rahmen der strategischen Ausland-Fernmeldeaufklärung mit ausländischen öffentlichen Stellen kooperiert, die nachrichtendienstliche Aufgaben wahrnehmen, dürfen dabei auch personenbezogene Daten nach den §§ 32 und 33 verarbeitet werden. Eine Erstreckung der Kooperation auf Daten der folgenden Personen ist unzulässig:

1. deutsche Staatsangehörige,
 2. inländische juristische Personen und
 3. sich im Bundesgebiet aufhaltenden Personen
- § 19 Absatz 7 Satz 1 bis 4 findet Anwendung.

(2) Die strategische Ausland-Fernmeldeaufklärung auf dem Gebiet der Bundesrepublik Deutschland darf im Rahmen einer solchen Kooperation nur durch den Bundesnachrichtendienst erfolgen.

(3) Eine Kooperation mit den in Absatz 1 Satz 1 genannten ausländischen öffentlichen Stellen ist zulässig, um

1. frühzeitig erhebliche Gefahren für die innere oder äußere Sicherheit der Bundesrepublik Deutschland, die Verteidigung oder das Gemeinwohl erkennen und diesen Gefahren begegnen zu können,
2. die außen- und sicherheitspolitische Handlungsfähigkeit der Bundesrepublik Deutschland zu wahren oder
3. die Aufgabenerfüllung durch den Bundesnachrichtendienst sicherzustellen, die ohne eine solche Kooperation wesentlich erschwert oder unmöglich ist.

(4) Einzelheiten der Kooperation sind vor ihrem Beginn zwischen dem Bundesnachrichtendienst und der ausländischen öffentlichen Stelle in einer Absichtserklärung schriftlich niederzulegen. In die Absichtserklärung sind insbesondere aufzunehmen:

1. Zweck der Kooperation,
2. Dauer der Kooperation,
3. eine verbindliche Zusicherung der ausländischen öffentlichen Stelle, dass
 - a) die im Rahmen der Kooperation erhobenen Daten nur zu dem Zweck verwendet werden, zu dem sie erhoben wurden, und eine Weitergabe an Dritte nur mit Zustimmung des Bundesnachrichtendienstes erfolgt,
 - b) Daten aus Telekommunikationsverkehren von deutschen Staatsangehörigen, von inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen, die unbeabsichtigt entgegen Absatz 1 Satz 2 in Verbindung mit § 19 Absatz 7 verarbeitet wurden und von der ausländischen

- öffentlichen Stelle bei der Datenauswertung als solche erkannt werden, unverzüglich gelöscht werden,
- c) Daten von schutzwürdigen Personen nach § 21 Absatz 1 Satz 2, die unbeabsichtigt verarbeitet wurden und von der ausländischen öffentlichen Stelle bei der Datenauswertung als solche erkannt werden, unverzüglich gelöscht werden,
 - d) Daten betreffend den Kernbereich privater Lebensgestaltung, die unbeabsichtigt verarbeitet wurden und von der ausländischen öffentlichen Stelle bei der Datenauswertung als solche erkannt werden, unverzüglich gelöscht werden,
 - e) die Verwendung der Daten mit grundlegenden rechtstaatlichen Prinzipien vereinbar ist und die Daten insbesondere weder zu politischer Verfolgung noch zu unmenschlicher oder erniedrigender Bestrafung oder Behandlung oder zur Unterdrückung Oppositioneller oder bestimmter Bevölkerungsgruppen eingesetzt werden,
 - f) sich die ausländische öffentliche Stelle bereit erklärt, auf Ersuchen des Bundesnachrichtendienstes Auskunft über die vorgenommene Verwendung der Daten zu erteilt wird,
 - g) einer Löschungsaufforderung des Bundesnachrichtendienstes Folge geleistet wird,
 - h) im Falle einer Datenübermittlung nach § 33 die Verkehrsdaten nicht über einen längeren Zeitraum als sechs Monate bevorratend gespeichert werden.

(5) Der Zweck der Kooperation muss gerichtet sein auf die Gewinnung von Informationen

1. zur Früherkennung von Gefahren durch den internationalen Terrorismus oder Extremismus, der gewaltbereit oder auf die planvoll verborgen betriebene Durchsetzung politischer, religiöser oder ideologischer Ansichten ausgerichtet ist, oder dessen Unterstützung,
2. zur Früherkennung von Gefahren durch die illegale Verbreitung von Massenvernichtungs- und Kriegswaffen sowie durch den unerlaubten Außenwirtschaftsverkehr mit Waren und technischen Unterstützungsleistungen in Fällen von erheblicher Bedeutung,
3. zum Schutz der Bundeswehr und der Streitkräfte der an der Kooperation beteiligten Staaten oder der Streitkräfte des Kooperationspartners,
4. zu krisenhaften Entwicklungen im Ausland und zu deren Auswirkungen,
5. zur Gefährdungs- und Sicherheitslage von deutschen und ausländischen Staatsangehörigen,
6. zu politischen, wirtschaftlichen oder militärischen Vorgängen im Ausland, die von erheblicher außen- und sicherheitspolitischer Bedeutung sind,
7. zu nachrichten- oder geheimdienstlichen Aktivitäten mit Bezug zur Bundesrepublik Deutschland oder zum Kooperationspartner,
8. zur internationalen organisierten Kriminalität,
9. zur Herstellung oder zum Erhalt wesentlicher Fähigkeiten des Bundesnachrichtendienstes oder des Kooperationspartners,
10. zu internationalen kriminellen, terroristischen oder staatlichen Angriffen mittels Schadprogrammen auf die Vertraulichkeit, Integrität oder Verfügbarkeit von informationstechnischen Systemen oder
11. zu vergleichbaren Fällen.

(6) Für einzelne Kooperationszwecke nach Absatz 5 innerhalb solcher Kooperationen sind Erkenntnisziel und Dauer schriftlich festzulegen. Die Erkenntnisziele dürfen den

außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland nicht entgegenstehen.

(7) Die Absichtserklärung bedarf der Zustimmung des Bundeskanzleramtes, wenn die Kooperation mit ausländischen öffentlichen Stellen von Mitgliedstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages erfolgt. Im Übrigen bedarf die Absichtserklärung der Zustimmung der Chefin oder des Chefs des Bundeskanzleramtes. Das Parlamentarische Kontrollgremium ist über die Absichtserklärung zu unterrichten.

§ 32

Verarbeitung von selektierten personenbezogenen Daten im Rahmen von Kooperationen

(1) Die Verarbeitung selektierter personenbezogener Daten durch den Bundesnachrichtendienst im Rahmen einer Kooperation nach § 31 ist zulässig, 1. um die vereinbarten Kooperationszwecke zu erreichen und 2. wenn bei der Erhebung von Inhaltsdaten nur solche Suchbegriffe verwendet werden, die zur Erreichung der vereinbarten Kooperationszwecke geeignet sind.

Die Erhebung der personenbezogenen Daten und die Verwendung der Suchbegriffe müssen zudem in Einklang mit den außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland stehen. Im Übrigen findet § 19 Absatz 5, 7 und 9, § 20 Absatz 1, § 21 Absatz 1 und 2 und § 22 Absatz 1 entsprechende Anwendung.

(2) Die Verantwortung für die Zulässigkeit der Kooperation trägt der Bundesnachrichtendienst. Sofern Anhaltspunkte dafür bestehen, dass der Kooperationspartner die abgegebenen Zusicherungen oder Absprachen nicht einhält, hat der Bundesnachrichtendienst auf deren Einhaltung hinzuwirken und erforderlichenfalls die Kooperation zu beenden.

(3) Im Rahmen der Kooperation dürfen selektierte personenbezogene Daten erhoben werden, wenn eine automatisierte Prüfung die Zulässigkeit der hierfür verwendeten Suchbegriffe ergibt. Diese Zulässigkeit liegt vor, wenn

1. die Ausrichtung der von dem Kooperationspartner übermittelten Suchbegriffe an den Kooperationszielen und -inhalten von dem Kooperationspartner hinreichend plausibel gemacht wird und
2. keine tatsächlichen Anhaltspunkte dafür bestehen, dass
 - a) durch die Verwendung der Suchbegriffe Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, oder
 - b) Suchbegriffe einer besonders schutzbedürftigen Person nach § 21 Absatz 1 Satz 2 verwendet werden.

(4) Im Rahmen der Kooperation dürfen die anhand der Suchbegriffe nach Absatz 3 erhobenen Daten an den Kooperationspartner automatisiert übermittelt werden, wenn zuvor die folgenden im Rahmen einer automatisierten Prüfung erkannten Daten gelöscht wurden:

1. Daten nach § 19 Absatz 7 Satz 1 oder Daten, deren Übermittlung nationalen Interessen der Bundesrepublik Deutschland entgegenstehen würden,
2. Daten, die zum Kernbereich privater Lebensgestaltung gehören und
3. Daten, die einer besonders schutzbedürftigen Person nach § 21 Absatz 1 zugeordnet werden können.

(5) Der Bundesnachrichtendienst hat unter Nutzung der Ergebnisse und Erfahrungen seiner Arbeit etwaige Hinweise auf besonders schutzbedürftigen Personen nach § 21 Absatz 1 zu sammeln und Suchbegriffe, die diesen Personen zuzuordnen sind, zusammenzuführen, um dem besonderen Schutzbedürfnis dieser Personen Rechnung tragen zu können. Die diesbezüglichen Datenbanken und Filterverfahren sind kontinuierlich zu aktualisieren und fortzuentwickeln.

(6) Die Übermittlung der Daten ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung von Kontrollen der Datenverarbeitung, einschließlich der Datenschutzkontrolle, sowie zur Löschaufforderung an den Kooperationspartner nach Absatz 7 Satz 3 verwendet werden. Die Protokolldaten sind bis zum Ablauf des zweiten auf die Protokollierung folgenden Kalenderjahres aufzubewahren und danach unverzüglich zu löschen.

(7) Das ordnungsgemäße Funktionieren der automatisierten Prüfung nach den Absätzen 3 und 4 ist durch den Bundesnachrichtendienst stichprobenartig zu überprüfen. Die Prüfung erfolgt unter Aufsicht einer Bediensteten oder eines Bediensteten des Bundesnachrichtendienstes, die oder der die Befähigung zum Richteramt hat. Sofern nachträglich erkannt wird, dass Daten entgegen dieser Vorgaben erhoben und an den Kooperationspartner übermittelt wurden, wird der Kooperationspartner zur Löschung der Daten aufgefordert. Der Bundesnachrichtendienst unterrichtet das Bundeskanzleramt in Abständen von höchstens sechs Monaten über die Durchführung der Prüfung nach Satz 1.

(8) Die im Rahmen der Kooperation auf Grundlage der vom Kooperationspartner benannten Suchbegriffe erhobenen Daten werden durch den Bundesnachrichtendienst zum Zweck der Durchführung der Stichproben nach Absatz 7 Satz 1 sowie zur Bestimmung neuer Suchbegriffe nach § 24 Absatz 1 Nummer 2 für die Dauer von zwei Wochen gespeichert.

§ 33

Verarbeitung von unselektierten Verkehrsdaten im Rahmen von Kooperationen

(1) Die automatisierte Übermittlung von unselektierten personenbezogenen Verkehrsdaten im Rahmen einer Kooperation durch den Bundesnachrichtendienst ist nur zulässig, wenn zusätzlich zum Vorliegen der Voraussetzungen nach § 31 ein qualifizierter Aufklärungsbedarf vorhanden ist.

(2) Ein qualifizierter Aufklärungsbedarf liegt vor, wenn die Übermittlung von Verkehrsdaten aufgrund bestimmter Ereignisse erforderlich ist, um konkreten Bedrohungen entgegenzuwirken oder die Handlungsfähigkeit der Bundesrepublik Deutschland oder des Kooperationspartners sicherzustellen. Diese Voraussetzungen sind insbesondere dann gegeben, wenn tatsächliche Anhaltspunkte bestehen für

1. die Vorbereitung eines bewaffneten Angriffs auf die Bundesrepublik Deutschland oder auf Mitgliedstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages oder auf den Kooperationspartner,
2. die Vorbereitung terroristischer Anschläge,
3. Verschiebungen von Kriegswaffen auf einer bestimmten Route oder mit einem bestimmten Ziel,

4. Internationale kriminelle, terroristische oder staatliche Angriffe mittels Schadprogrammen auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen,
5. die Aufklärung der Arbeitsweise anderer Nachrichtendienste mit dem Ziel der Aufdeckung staatlich gesteuerter, auf Destabilisierung angelegter Desinformationskampagnen mit unmittelbarem Bezug zur Bundesrepublik Deutschland oder mit dem Ziel der Vorbereitung oder Durchführung von staatsterroristischen Aktivitäten, oder
6. die Vorbereitungen eines Angriffs auf solche Rechtsgüter der Allgemeinheit, deren Bedrohung die Sicherheit oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt.

Der qualifizierte Aufklärungsbedarf ist schriftlich niederzulegen und einer strategischen Aufklärungsmaßnahme nach § 19 Absatz 1 zuzuordnen. Der Unabhängige Kontrollrat prüft die Rechtmäßigkeit der Feststellung des qualifizierten Aufklärungsbedarfs der Kooperation vor Vollzug der Datenübermittlung. Bestätigt der Unabhängige Kontrollrat die Rechtmäßigkeit der Feststellung nicht, hat die Datenübermittlung zu unterbleiben.

(3) Kooperationen nach § 31, die die Verarbeitung unselektierter Verkehrsdaten nach Absatz 1 umfassen, bedürfen der Genehmigung durch die Präsidentin oder den Präsidenten des Bundesnachrichtendienstes oder durch eine Vertretung, die die Präsidentin oder der Präsident des Bundesnachrichtendienstes bestimmt hat.

Unterabschnitt 4 Besondere Formen der technischen Aufklärung.

§ 34 Eingriff in informationstechnische Systeme von Ausländern im Ausland

(1) Der Bundesnachrichtendienst darf zur Erfüllung seiner Aufgaben ohne Wissen der betroffenen Person auf der Grundlage einer zuvor angeordneten individuellen Aufklärungsmaßnahme mit technischen Mitteln in von Ausländern im Ausland genutzte informationstechnische Systeme eingreifen und auf ihnen gespeicherte personenbezogene Daten einschließlich Inhalte und Umstände der laufenden Kommunikation erheben, soweit dies erforderlich ist für den Zweck

1. der politischen Unterrichtung der Bundesregierung oder einer Landesregierung oder
2. der Früherkennung von aus dem Ausland drohenden Gefahren von internationaler Bedeutung im Sinne des § 19 Absatz 4.

Die individuelle Aufklärungsmaßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 1 Absatz 2 erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.

(2) Eine individuelle Aufklärungsmaßnahme nach Absatz 1 Satz 1 Nummer 1 ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass sie der Gewinnung von Informationen dient, mit deren Aufklärung das Bundeskanzleramt den Bundesnachrichtendienst beauftragt hat, sie der Gewinnung von Informationen dient, mit deren Aufklärung das Bundeskanzleramt den Bundesnachrichtendienst beauftragt hat und die von herausgehobener außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind.

(3) Eine individuelle Aufklärungsmaßnahme nach Absatz 1 Satz 1 Nummer 2 ist nur zulässig, wenn Tatsachen die Annahme rechtfertigen, dass durch sie Erkenntnisse

gewonnen werden über Gefahren nach § 19 Absatz 4 in Fällen von herausgehobener außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland.

(4) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.

(5) Die individuelle Aufklärungsmaßnahme zum Zweck der Gefahrenfrüherkennung nach Absatz 1 Nummer 2 darf sich nur richten gegen Personen, hinsichtlich derer tatsächliche Anhaltspunkte dafür vorliegen, dass sie

1. Verursacher von Gefahren im Sinne des § 19 Absatz 4 sind oder
2. für den Verursacher gemäß Nummer 1 bestimmte oder von ihm herrührende Informationen entgegennehmen oder weitergeben oder der Verursacher gemäß Nummer 1 ihr informationstechnisches System benutzt.

(6) Eine individuelle Aufklärungsmaßnahme darf auch durchgeführt werden, wenn andere Personen oder Informationssysteme unvermeidbar betroffen werden. Sie darf unter Abwägung aller vorliegenden Erkenntnisse keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht. § 19 Absatz 7 findet Anwendung mit der Maßgabe, dass anstelle der Unterrichtung der G10-Kommission die Unterrichtung des Unabhängigen Kontrollrates und anstelle der Entscheidung der G10-Kommission in den Fällen des § 59 Absatz 2 die Entscheidung des Unabhängigen Kontrollrates tritt.

(7) Der Bundesnachrichtendienst prüft unverzüglich, ob die im Rahmen einer individuellen Aufklärungsmaßnahme nach Absatz 1 erhobenen personenbezogenen Daten alleine oder zusammen mit bereits vorliegenden Daten für die Zwecke nach Absatz 1 erforderlich sind. Mit Zustimmung des Unabhängigen Kontrollrates kann abweichend von Satz 1 im Einzelfall ein Prüfzeitraum von bis zu drei Jahren festgelegt werden, wenn eine unverzügliche Prüfung nicht möglich ist. Soweit die Daten für die Zwecke nach Absatz 1 nicht erforderlich sind, sind sie unverzüglich unter Aufsicht einer Bediensteten oder eines Bediensteten, die oder der die Befähigung zum Richteramt hat, zu löschen. Die Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich für die Durchführung von Kontrollen der Datenverarbeitung, einschließlich der Datenschutzkontrolle, verwendet werden. Die Protokolldaten sind am Ende des zweiten auf die Protokollierung folgenden Kalenderjahres zu löschen.

(8) Personenbezogene Daten sind unmittelbar nach der Datenerhebung wie folgt zu kennzeichnen:

1. Angabe des Zwecks der Datenerhebung nach Absatz 1 und
2. Angabe des Mittels der Datenerhebung.

Die Kennzeichnung entfällt bei Übermittlungen.

(9) Für die Auswertung von informationstechnischen Systemen von Ausländern im Ausland, die sich im Besitz des Bundesnachrichtendienstes befinden oder deren Abbildern, findet Absatz 7 entsprechende Anwendung mit der Maßgabe, dass die Auswertung innerhalb von drei Jahren nach Lesbarmachung der Daten durchgeführt

sein muss, wenn nicht der Unabhängige Kontrollrat aufgrund der Umstände des Einzelfalls einer längeren Frist zustimmt.

§ 35

Schutz von Vertraulichkeitsbeziehungen

(1) Individuelle Aufklärungsmaßnahmen nach § 34 Absatz 1 zum Zweck der Erhebung von personenbezogenen Daten aus einer Vertraulichkeitsbeziehung (§ 21 Absatz 1 Satz 2) sind unzulässig.

(2) Abweichend von Absatz 1 sind individuelle Aufklärungsmaßnahmen zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass

1. die in § 21 Absatz 1 Satz 2 aufgeführte Person Täter oder Teilnehmer einer der in § 29 Absatz 3 genannten Straftaten ist oder
2. dies erforderlich ist zur Verhinderung einer 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.

(3) Sofern erst die Verarbeitung der Daten ergibt, dass diese schutzwürdig nach Absatz 1 sind, dürfen die Daten nur verwendet werden, wenn die Voraussetzungen des Absatzes 2 vorliegen. Andernfalls sind die Daten unverzüglich zu löschen. Die Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung der Datenschutzkontrolle verwendet werden. Die Protokolldaten sind bis zum Ablauf des zweiten auf die Protokollierung folgenden Kalenderjahres aufzubewahren und danach unverzüglich zu löschen.

§ 36

Kernbereichsschutz

(1) Die Datenerhebung zum Zweck der Erlangung von Erkenntnissen zum Kernbereich privater Lebensgestaltung ist unzulässig.

(2) Sofern erst die Weiterverarbeitung der erhobenen personenbezogenen Daten ergibt, dass Daten erhoben wurden, die dem Kernbereich privater Lebensgestaltung unterfallen, sind diese unverzüglich zu löschen. Die Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung der Datenschutzkontrolle verwendet werden. Die Protokolldaten sind bis zum Ablauf des zweiten auf die Protokollierung folgenden Kalenderjahres aufzubewahren und danach unverzüglich zu löschen.

(3) Bestehen im Rahmen der Weiterverarbeitung nach Absatz 2 Zweifel und sollen die Daten nicht unverzüglich gelöscht werden, dürfen die Daten nicht ohne vorherige Prüfung durch den Unabhängigen Kontrollrat weiterverarbeitet werden. Stellt der Unabhängige Kontrollrat fest, dass die Daten nicht weiterverarbeitet werden dürfen, sind die Daten unverzüglich zu löschen. Die Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung der Datenschutzkontrolle verwendet werden. Die Protokolldaten sind bis zum Ablauf des zweiten auf die Protokollierung folgenden Kalenderjahres aufzubewahren und danach unverzüglich zu löschen.

§ 37 Anordnung

(1) Individuelle Aufklärungsmaßnahmen nach § 34 Absatz 1 bedürfen der Anordnung durch die Präsidentin oder den Präsidenten des Bundesnachrichtendienstes oder durch eine Vertretung, die die Präsidentin oder der Präsident des Bundesnachrichtendienstes bestimmt hat. Der Unabhängige Kontrollrat prüft die Rechtmäßigkeit der Anordnung vor ihrem Vollzug. Bestätigt der Unabhängige Kontrollrat die Rechtmäßigkeit der Anordnung nicht, tritt die Anordnung außer Kraft. Bei Gefahr im Verzug erfolgt eine vorläufige Prüfung der Rechtmäßigkeit durch ein Mitglied des Unabhängigen Kontrollrats, wenn andernfalls der Aufklärungszweck der strategischen Aufklärungsmaßnahme vereitelt oder wesentlich erschwert würde. Wird im Rahmen der vorläufigen Prüfung festgestellt, dass die Anordnung 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 4 auf, tritt die Anordnung außer Kraft und die bereits erhobenen Daten sind unverzüglich zu löschen.

(2) Die Anordnung nach Absatz 1 ergeht schriftlich. In ihr sind anzugeben

1. der Aufklärungszweck,
2. das verfolgte Aufklärungsthema,
3. das Ziel der individuellen Aufklärungsmaßnahmen,
4. Art, Umfang und Dauer der individuellen Aufklärungsmaßnahme,
5. eine Begründung sowie
6. erforderlichenfalls die Festlegung eines längeren Prüfzeitraumes nach § 34 Absatz 7 Satz 2 oder Absatz 9.

(3) Die Anordnung ist auf höchstens zwölf Monate zu befristen. Verlängerungen um jeweils bis zu zwölf Monate sind zulässig, soweit die Anordnungsvoraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, ist die individuelle Aufklärungsmaßnahme unverzüglich zu beenden.

(4) Der Bundesnachrichtendienst unterrichtet das Bundeskanzleramt in regelmäßigen Abständen über Anordnungen nach Absatz 1. Das Bundeskanzleramt unterrichtet darüber hinaus das Parlamentarische Kontrollgremium jährlich über die Anzahl der angeordneten individuellen Aufklärungsmaßnahmen.

§ 38 Übermittlung von personenbezogenen Daten aus individuellen Aufklärungsmaßnahmen an inländische öffentliche Stellen und andere inländische Stellen

(1) Der Bundesnachrichtendienst darf an das Bundesamt für Verfassungsschutz, die Verfassungsschutzbehörden der Länder und an den Militärischen Abschirmdienst übermitteln:

1. die mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten, wenn tatsächliche Anhaltspunkte dafür bestehen, dass dies erforderlich ist zum Schutz besonders gewichtiger Rechtsgüter und
2. die mit dem Zweck der politischen Unterrichtung oder mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten zum

Zweck der Unterrichtung der Bundesregierung oder einer Landesregierung, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung zur Erfüllung seiner Aufgaben oder der Aufgaben der Empfänger erforderlich ist.

(2) Der Bundesnachrichtendienst darf die mit dem Zweck der politischen Unterrichtung der Bundesregierung oder einer Landesregierung oder mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten an andere inländische öffentliche Stellen zum Zweck der Unterrichtung der Bundesregierung oder einer Landesregierung übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung zur Erfüllung seiner Aufgaben oder der Aufgaben der Empfänger erforderlich ist.

(3) Der Bundesnachrichtendienst darf die mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten an inländische Strafverfolgungsbehörden übermitteln, wenn Tatsachen die Annahme rechtfertigen, dass dies erforderlich ist zur Verfolgung einer Straftat nach § 29 Absatz 3.

(4) Der Bundesnachrichtendienst darf die mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten an die in Absatz 2 genannten Stellen auch zum Zweck der Weiterverarbeitung für Folgemaßnahmen mit unmittelbarer Außenwirkung für den Betroffenen, insbesondere zur Gefahrenabwehr, übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass dies erforderlich ist zur Abwehr einer Gefahr für besonders gewichtige Rechtsgüter oder zur Abwehr einer besonders schwerwiegenden Beeinträchtigung der Rechte Einzelner.

(5) Der Bundesnachrichtendienst darf die mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten an die Bundeswehr übermitteln, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies erforderlich ist

1. zum Schutz der Funktionsfähigkeit der Bundeswehr für die Landes- oder Bündnisverteidigung und bei Auslandseinsätzen,
2. zum Schutz der Funktionsfähigkeit der Streitkräfte von Mitgliedstaaten der Europäischen Union, des Nordatlantikvertrages oder der Europäischen Freihandelsassoziation,
3. zum Schutz von Leib, Leben oder Freiheit einer Person, oder
4. zum Schutz von anderen besonders gewichtigen Rechtsgütern

Die in Satz 1 genannten personenbezogenen Daten darf der Bundesnachrichtendienst auch automatisiert an die Bundeswehr übermitteln, sofern diese im Rahmen von individuellen Aufklärungsmaßnahmen nach § 34 Absatz 1 mit Bezug zu den in § 19 Absatz 4 Nummer 1 a) oder Nummer 2 a) genannten Gefahren erhoben wurden.

(6) Für Übermittlungen an andere inländische Stellen gilt § 29 Absatz 6 entsprechend.

(7) Der Bundesnachrichtendienst darf die mit dem Zweck der politischen Unterrichtung der Bundesregierung gekennzeichneten personenbezogenen Daten an inländische öffentliche Stellen über die Absätze 1 und 2 hinaus auch übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass eine Übermittlung erforderlich ist zur Verhinderung einer unmittelbar bevorstehenden Gefahr für

1. Leib, Leben oder Freiheit einer Person,
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.

In Fällen von Satz 1 Nummer 1 ist über Absatz 6 hinaus auch eine Übermittlung an andere inländische Stellen zulässig.

(8) Für Übermittlungen nach den Absätzen 1 bis 7 gilt im Übrigen § 29 Absatz 8 bis 16 entsprechend.

§ 39

Übermittlung von personenbezogenen Daten aus individuellen Aufklärungsmaßnahmen an ausländische öffentliche Stellen, über- und zwischenstaatliche Stellen sowie an andere ausländische Stellen

(1) Der Bundesnachrichtendienst darf die mit dem Zweck der politischen Unterrichtung der Bundesregierung oder einer Landesregierung oder mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten zum Zweck der Unterrichtung im Rahmen der internationalen politischen Zusammenarbeit an ausländische öffentliche Stellen sowie über- und zwischenstaatliche Stellen übermitteln, soweit tatsächliche Anhaltspunkte vorliegen, dass die Übermittlung zur Erfüllung seiner Aufgaben erforderlich ist.

(2) Der Bundesnachrichtendienst darf die mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten an die in Absatz 1 genannten Stellen übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass dies erforderlich ist zur Verfolgung von Straftaten, die den in § 29 Absatz 3 genannten Straftaten entsprechen. Die Regelungen des Gesetzes über die internationale Rechtshilfe in Strafsachen bleiben unberührt.

(3) Der Bundesnachrichtendienst darf die mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogene Daten an die in Absatz 1 genannten Stellen auch zum Zweck der Weiterverarbeitung für Folgemaßnahmen mit unmittelbarer Außenwirkung für den Betroffenen, insbesondere zur Gefahrenabwehr, übermitteln, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass

1. die Daten für den Empfänger zur Früherkennung von Gefahren im Sinne des § 19 Absatz 4 von erheblicher Bedeutung oder zur Wahrung anderer erheblicher Sicherheitsinteressen erforderlich sind, oder
2. die Übermittlung zur Wahrung erheblicher außen- und sicherheitspolitischer Belange des Bundes oder eines Landes erforderlich ist.

Die Entscheidung über die Erforderlichkeit der Übermittlung erfolgt unter Aufsicht einer oder eines Bediensteten des Bundesnachrichtendienstes, die oder der die Befähigung zum Richteramt hat.

(4) Der Bundesnachrichtendienst darf die mit dem Zweck der politischen Unterrichtung gekennzeichneten personenbezogene Daten an die in Absatz 1 genannten Stellen über Absatz 2 hinaus auch übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass eine Übermittlung erforderlich ist zur Verhinderung einer unmittelbar bevorstehenden Gefahr für

1. Leib, Leben oder Freiheit einer Person,
2. für 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.

(5) Für Übermittlungen an andere ausländische Stellen gilt § 30 Absatz 4 und Absatz 5 Satz 2 entsprechend.

(6) Für Übermittlungen nach den Absätzen 1 bis 5 gilt im Übrigen § 30 Absatz 6 bis 9 entsprechend.

Unterabschnitt 5 Unabhängige Rechtskontrolle

§ 40 Ausübung der unabhängigen Rechtskontrolle

(1) Die Rechtmäßigkeit der technischen Aufklärung und damit einhergehender Übermittlungen und Kooperationen des Bundesnachrichtendienstes auf der Grundlage der durch dieses Gesetz eingeräumten Befugnisse unterliegt der Rechtskontrolle durch den Unabhängigen Kontrollrat.

(2) Die Rechtskontrolle wird ausgeübt als

1. gerichtsähnliche Rechtskontrolle durch das gerichtsähnliche Kontrollorgan und
2. administrative Rechtskontrolle durch das administrative Kontrollorgan.

§ 41 Unabhängiger Kontrollrat

(1) Der Unabhängige Kontrollrat ist eine oberste Bundesbehörde und als unabhängiges Organ der Kontrolle der technischen Aufklärung des Bundesnachrichtendienstes nur dem Gesetz unterworfen.

(2) Der Unabhängige Kontrollrat wird von einer Präsidentin oder einem Präsidenten geleitet. Die Präsidentin oder der Präsident vertritt die Behörde nach außen. Sie oder er leitet die Verwaltung des Unabhängigen Kontrollrates und übt die Dienstaufsicht aus.

(3) Der Unabhängige Kontrollrat ist bei der Erfüllung seiner Aufgaben und bei der Ausübung seiner Befugnisse unabhängig und nicht weisungsgebunden.

(4) Der Unabhängige Kontrollrat unterliegt der Prüfung der Haushalts- und Wirtschaftsführung durch den Bundesrechnungshof, soweit hierdurch seine Unabhängigkeit nicht beeinträchtigt wird.

(5) Der Unabhängige Kontrollrat gibt sich nach Anhörung des Bundeskanzleramtes

1. eine Geschäftsordnung und
2. eine Verfahrensordnung.

Geheimhaltungsbelangen des Bundesnachrichtendienstes ist Rechnung zu tragen. Über die Geschäfts- und Verfahrensordnung entscheiden die Mitglieder des gerichtsähnlichen Kontrollorgans mit der Mehrheit der Stimmen. Im Falle der Stimmengleichheit entscheidet die Stimme der Präsidentin oder des Präsidenten. Der Unabhängige Kontrollrat unterrichtet das Parlamentarische Kontrollgremium über die Geschäftsordnung.

(6) Dienstsitze des Unabhängigen Kontrollrates sind Berlin und Pullach.

§ 42

Zuständigkeit des gerichtsähnlichen Kontrollorgans

(1) Das gerichtsähnliche Kontrollorgan ist im Rahmen der strategischen Ausland-Fernmeldeaufklärung zuständig für die Vorabkontrolle der Rechtmäßigkeit:

1. der Anordnung von strategischen Aufklärungsmaßnahmen nach § 23 Absatz 1 (§ 23 Absatz 4),
2. der Anordnung von Zielen nach § 23 Absatz 5 (§ 23 Absatz 7),
3. der Feststellung eines qualifizierten Aufklärungsbedarfs bei der Verarbeitung von unselektierten Verkehrsdaten im Rahmen von Kooperationen des Bundesnachrichtendienstes mit ausländischen Nachrichtendiensten nach § 33 Absatz 2 und
4. der Verwertbarkeit oder Löschung von Daten nach § 22 Absatz 3 im Falle von Zweifeln und
5. der Übermittlung von Daten nach § 29 Absatz 8 und § 30 Absatz 9.

(2) Das gerichtsähnliche Kontrollorgan ist im Rahmen der strategischen Ausland-Fernmeldeaufklärung ferner zuständig für die Kontrolle der Rechtmäßigkeit:

1. der Verwendung der Daten nach § 21 Absatz 3,
2. der Übermittlung nach § 29 Absatz 8 und § 30 Absatz 9,
3. einer Zweckänderung nach § 29 Absatz 7 und § 30 Absatz 5,
4. der Dienstvorschriften des Bundesnachrichtendienstes nach § 62 soweit sie Regelungen zur Auswertung von Daten beinhalten und
5. die abschließende Entscheidung über Beanstandungen der administrativen Rechtskontrolle (§ 52 Absatz 3).

(3) Das gerichtsähnliche Kontrollorgan ist im Rahmen von Eingriffen in informationstechnische Systeme von Ausländern im Ausland nach § 34 zuständig für die Vorabkontrolle der Rechtmäßigkeit der Anordnung von individuellen Aufklärungsmaßnahmen nach § 37 Absatz 1 und der Übermittlung von Daten nach § 38 Absatz 8 in Verbindung mit § 29 Absatz 8 sowie § 39 Absatz 6 in Verbindung mit § 30 Absatz 9.

(4) Das gerichtsähnliche Kontrollorgan ist im Rahmen von Eingriffen in informationstechnische Systeme von Ausländern im Ausland nach § 34 ferner zuständig für die Kontrolle der Rechtmäßigkeit

1. der Verwendung der Daten nach § 35 Absatz 3,
2. der Übermittlung nach § 38 Absatz 8 und § 39 Absatz 6,
3. einer Zweckänderung nach § 38 Absatz 7 und § 39 Absatz 4 und
4. die abschließende Entscheidung über Beanstandungen der administrativen Rechtskontrolle (§ 52 Absatz 3).

§ 43

Besetzung des gerichtsähnlichen Kontrollorgans; Wahl der Mitglieder

(1) Das gerichtsähnliche Kontrollorgan des Unabhängigen Kontrollrates besteht aus sechs Mitgliedern, die vor ihrer Ernennung als Mitglied beim gerichtsähnlichen Kontrollorgan tätig waren als

1. Richterinnen oder Richter am Bundesgerichtshof (richterliche Mitglieder) und in dieser Tätigkeit über langjährige Erfahrung verfügen, oder
2. Bundesanwältin oder Bundesanwalt beim Generalbundesanwalt beim Bundesgerichtshof (staatsanwaltschaftliche Mitglieder).

Mindestens vier Mitglieder des gerichtsähnlichen Kontrollorgans müssen richterliche Mitglieder sein. Nicht mehr als zwei Mitglieder dürfen staatsanwaltliche Mitglieder sein. Die Präsidentin oder der Präsident des Unabhängigen Kontrollrates ist Vorsitzende oder Vorsitzender des gerichtsähnlichen Kontrollorgans.

(2) Die Mitglieder des gerichtsähnlichen Kontrollorgans haben sich einer erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlungen nach dem Sicherheitsüberprüfungsgesetz zu unterziehen.

(3) Das Parlamentarische Kontrollgremium wählt die Mitglieder des gerichtsähnlichen Kontrollorgans auf Vorschlag der Präsidentin oder des Präsidenten des Bundesgerichtshofes für die richterlichen Mitglieder und der Generalbundesanwältin oder des Generalbundesanwaltes beim Bundesgerichtshof für die staatsanwaltlichen Mitglieder mit einfacher Mehrheit. Die Präsidentin oder der Präsident oder die Generalbundesanwältin oder der Generalbundesanwalt teilt den Vorschlag vor der Wahl der Bundesregierung zur Kenntnisnahme mit.

§ 44

Rechtsstellung und Ernennung der Mitglieder des gerichtsähnlichen Kontrollorgans

(1) Die Mitglieder des gerichtsähnlichen Kontrollorgans werden zu Beamtinnen und Beamten auf Zeit ernannt. Vorbehaltlich der Regelungen in diesem Gesetz finden die Vorschriften des Bundesbeamtengesetzes mit Ausnahme der Vorschriften über die Laufbahnen und die Probezeit entsprechende Anwendung. Die Mitglieder des gerichtsähnlichen Kontrollorgans sind unabhängig und nur dem Gesetz unterworfen.

(2) Der Bundespräsident oder die Bundespräsidentin ernennt die nach § 43 Absatz 3 Gewählten.

(3) Die Mitglieder des gerichtsähnlichen Kontrollorgans leisten vor der Präsidentin oder dem Präsidenten des Deutschen Bundestages folgenden Eid: „Ich schwöre, dass ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann üben werde. So wahr mir Gott helfe.“ Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(4) Die Mitglieder des gerichtsähnlichen Kontrollorgans führen die Amtsbezeichnung Kontrollbeauftragte beim Unabhängigen Kontrollrat oder Kontrollbeauftragter beim Unabhängigen Kontrollrat.

§ 45

Amtszeit der Mitglieder des gerichtsähnlichen Kontrollorgans

(1) Die Amtszeit beträgt zwölf Jahre. Eine Wiederwahl ist unzulässig.

(2) Das Beamtenverhältnis auf Zeit der Mitglieder des gerichtsähnlichen Kontrollorgans beginnt mit der Aushändigung der Ernennungsurkunde, wenn nicht in der Urkunde ein späterer Tag bestimmt ist.

(3) Mit Ernennung in das Beamtenverhältnis auf Zeit ruhen für die Dauer der Amtszeit die Rechte und Pflichten aus dem zuletzt im Beamten- oder Richter Verhältnis auf

Lebenszeit übertragenen Amt. Dies gilt nicht für die Verschwiegenheitspflicht und das Verbot der Annahme von Belohnungen, Geschenken und sonstigen Vorteilen.

(4) Die Mitglieder des gerichtsähnlichen Kontrollorgans treten mit Ablauf der Amtszeit, spätestens aber mit Vollendung des 70. Lebensjahres, in den Ruhestand. Soweit die Amtszeit eines richterlichen Mitglieds beim Unabhängigen Kontrollrat vor Erreichen der gesetzlichen Regelaltersgrenze gemäß § 48 Absatz 1 des Deutschen Richtergesetzes endet, ist sie oder er auf Antrag auch als Richterin oder Richter am Bundesgerichtshof zu dem Zeitpunkt in den Ruhestand zu versetzen, zu dem ihr oder sein Amt als Mitglied im gerichtsähnlichen Kontrollorgan nach Maßgabe des § 45 Absatz 1 endet.

(5) Die Amtszeit nach Absatz 1 verlängert sich um den Zeitraum bis zur Wahl einer Nachfolgerin oder eines Nachfolgers. Bis dahin führen die Mitglieder des gerichtsähnlichen Kontrollorgans ihre Amtsgeschäfte fort.

§ 46

Besoldung der Mitglieder des gerichtsähnlichen Kontrollorgans

F

(1) Den Mitgliedern des gerichtsähnlichen Kontrollorgans wird vom Beginn des Kalendermonats an, in dem das Beamtenverhältnis auf Zeit beginnt, bis zum Ende des Kalendermonats, in dem dieses endet, im Falle des § 45 Absatz 5 bis zum Ende des Monats, in dem die Geschäftsführung endet, ein Amt der Besoldungsgruppe B 7 übertragen.

(2) Abweichend von Absatz 1 wird der Präsidentin oder dem Präsidenten des Unabhängigen Kontrollrates ein Amt der Besoldungsgruppe B 9 übertragen.

§ 47

Weitere Rechte und Pflichten der Mitglieder des gerichtsähnlichen Kontrollorgans

(1) Die für die Richterinnen und Richter an den obersten Gerichtshöfen des Bundes geltenden Vorschriften über Unabhängigkeit und Disziplinarmaßnahmen sind entsprechend anzuwenden. § 48 Absatz 4 und 5 des Deutschen Richtergesetzes findet Anwendung.

(2) Die Mitglieder des gerichtsähnlichen Kontrollorgans sehen von allen mit den Aufgaben ihres Amtes nicht zu vereinbarenden Handlungen ab. § 4 des Deutschen Richtergesetzes gilt entsprechend.

§ 48

Leitung des Unabhängigen Kontrollrates

Das Parlamentarische Kontrollgremium wählt mit einfacher Mehrheit auf Vorschlag der Vorsitzenden oder des Vorsitzenden des Parlamentarische Kontrollgremiums aus den gewählten richterlichen Mitgliedern des gerichtsähnlichen Kontrollorgans die Präsidentin oder den Präsidenten sowie aus allen übrigen Mitgliedern die Vizepräsidentin oder den Vizepräsidenten des Unabhängigen Kontrollrates. Abweichend von § 44 Absatz 4 führen die nach Satz 1 Gewählten die Amtsbezeichnung Präsidentin oder Präsident des Unabhängigen Kontrollrates und Direktorin oder Direktor in der Funktion der Vizepräsidentin oder des Vizepräsidenten des Unabhängigen Kontrollrates.

§ 49

Spruchkörper des gerichtsähnlichen Kontrollorgans; Beschlussfassung

- (1) Die Mitglieder des gerichtsähnlichen Kontrollorgans bilden den Senat des gerichtsähnlichen Kontrollorgans. Den Vorsitz im Senat hat die Präsidentin oder der Präsident. Ist die Präsidentin oder der Präsident verhindert, hat die Vizepräsidentin oder der Vizepräsident den Vorsitz.
- (2) Der Senat des gerichtsähnlichen Kontrollorgans beruft zwei Kammern, die jeweils mit drei Mitgliedern besetzt sind. Die Besetzung einer Kammer soll nicht länger als zwei Jahre unverändert bleiben. Jede Kammer bestimmte aus den richterlichen Mitgliedern eine Vorsitzende oder einen Vorsitzenden.
- (3) Die Spruchkörper des gerichtsähnlichen Kontrollorgans sind jeweils in der Mehrzahl mit richterlichen Mitgliedern besetzt.
- (4) Der Senat ist beschlussfähig, wenn die Mehrheit seiner Mitglieder anwesend ist und die Mehrheit richterliche Mitglieder sind. Die Kammern sind beschlussfähig, wenn die Mehrheit ihrer Mitglieder anwesend ist. Die Beschlussfassung der Spruchkörper erfolgt mit einfacher Stimmenmehrheit. Im Falle der Stimmengleichheit entscheidet die Stimme der oder des Vorsitzenden. Ist die oder der Vorsitzende verhindert, entscheidet die Stimme des richterlichen Mitglieds.

§ 50

Aufbau und Organisation des administrativen Kontrollorgans

Das administrative Kontrollorgan untersteht einer Leiterin oder einem Leiter. Die Leiterin oder der Leiter verfügt über die Befähigung zum Richteramt. Sie oder er steht in einem Beamtenverhältnis zum Bund und ihr oder ihm wird ein Amt der Besoldungsgruppe B 4 übertragen. Sie oder er führt die Amtsbezeichnung Direktorin oder Direktor **als Leiterin oder Leiter des administrativen Kontrollorgans**. Die Leiterin oder der Leiter unterliegt den Weisungen der Präsidentin oder des Präsidenten.

§ 51

Zuständigkeit des administrativen Kontrollorgans

- (1) Das administrative Kontrollorgan unterstützt das gerichtsähnliche Kontrollorgan in der Durchführung seiner Kontrollbefugnisse. Darüber hinaus ist es zuständig für die Rechtskontrolle der Bereiche der technischen Aufklärung, die nicht der Rechtskontrolle durch das gerichtsähnliche Kontrollorgan unterliegen; insbesondere kann es, soweit nicht die originäre Zuständigkeit des gerichtsähnlichen Kontrollorgans eröffnet ist, die Rechtmäßigkeit von Suchbegriffen überprüfen.
- (2) Die konkrete Ausgestaltung der Prüftätigkeit des administrativen Kontrollorgans wird von dem gerichtsähnlichen Kontrollorgan in regelmäßigen Abständen bestimmt. Hiervon unbenommen bleibt das Recht des gerichtsähnlichen Kontrollorgans zur Erteilung konkreter und einzelfallbezogener Prüfaufträge an das administrative Kontrollorgan.
- (3) Dem administrativen Kontrollorgan steht im Rahmen seiner Kontrollbefugnis ein Beanstandungsrecht nach § 52 zu.

§ 52 Beanstandungen

(1) Stellt das administrative Kontrollorgan im Rahmen seiner Kontrollzuständigkeit einen rechtswidrigen Zustand fest, kann es gegenüber dem Bundesnachrichtendienst eine Beanstandung aussprechen. Vor dem Ausspruch der Beanstandung hört das administrative Kontrollorgan den Bundesnachrichtendienst an.

(2) Spricht das administrative Kontrollorgan eine Beanstandung aus und wird dieser Beanstandung nicht innerhalb einer vom administrativen Kontrollorgan festgesetzten und angemessenen Frist abgeholfen, so kann das administrative Kontrollorgan die Beanstandung an das Bundeskanzleramt richten. Das Bundeskanzleramt nimmt zur Beanstandung Stellung.

(3) Hält das administrative Kontrollorgan auch nach Stellungnahme des Bundeskanzleramtes an der Beanstandung fest, oder nimmt das Bundeskanzleramt nicht innerhalb von drei Monaten nach Eingang der Beanstandung im Bundeskanzleramt Stellung, kann das administrative Kontrollorgan die Beanstandung dem gerichtsähnlichen Kontrollorgan zur abschließenden Entscheidung vorlegen.

(4) Das gerichtsähnliche Kontrollorgan entscheidet über die Beanstandung nach Anhörung des Bundeskanzleramtes. Kommt das gerichtsähnliche Kontrollorgan zu dem Ergebnis, dass die Beanstandung rechtmäßig erfolgt ist, ordnet es an, dass der Beanstandung unverzüglich oder innerhalb einer von ihm bestimmten Frist der Beanstandung abzuhelpen ist.

§ 53 Mitarbeiterinnen und Mitarbeiter des Unabhängigen Kontrollrates

Die Mitarbeiterinnen und Mitarbeiter des Unabhängigen Kontrollrats müssen deutsche Staatsangehörige sein und haben sich einer erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlungen nach dem Sicherheitsüberprüfungsgesetz zu unterziehen.

§ 54 Geheimhaltung; Aussagegenehmigung

(1) Die Beratungen des Unabhängigen Kontrollrates sind geheim.

(2) Die Mitglieder des gerichtsähnlichen Kontrollorgans sowie alle Mitarbeiterinnen und Mitarbeiter des Unabhängigen Kontrollrates sind zur Geheimhaltung der Angelegenheiten verpflichtet, die ihnen bei oder bei Gelegenheit ihrer Tätigkeit in dem Unabhängigen Kontrollrat bekannt geworden sind. Dies gilt auch für die Zeit nach ihrem Ausscheiden aus dem Unabhängigen Kontrollrat.

(3) Über die Erteilung einer Aussagegenehmigung entscheidet die Präsidentin oder der Präsident des Unabhängigen Kontrollrates. Die Genehmigung ist zu versagen, wenn die Aussage dem Wohl des Bundes oder eines Landes Nachteile bereiten oder die Erfüllung öffentlicher Aufgaben ernstlich gefährden oder erheblich erschweren würde. Über die Erteilung einer Aussagegenehmigung für die Präsidentin oder den Präsidenten entscheidet die Vizepräsidentin oder der Vizepräsident

§ 55

Unterrichtungen durch den Unabhängigen Kontrollrat

(1) Der Unabhängige Kontrollrat unterrichtet in Abständen von höchstens sechs Monaten das Parlamentarische Kontrollgremium über seine Tätigkeit.

(2) Die Unterrichtung nach Absatz 1 erfolgt nach Anhörung des Bundeskanzleramtes unter Beachtung des Geheimschutzes und erstreckt sich nur auf Informationen und Gegenstände, die der Verfügungsberechtigung des Bundesnachrichtendienstes unterliegen. Soweit diese nicht besteht, informiert das Bundeskanzleramt den Unabhängigen Kontrollrat. Auf Verlangen des Unabhängigen Kontrollrates ergreift das Bundeskanzleramt geeignete Maßnahmen, um das Parlamentarische Kontrollgremium über diese Informationen und Gegenstände unterrichten zu dürfen. Soweit dies aus Gründen des Wohls des Bundes oder eines Landes, insbesondere aus zwingenden Gründen des Nachrichtenzugangs oder aus Gründen des Schutzes von Persönlichkeitsrechten Dritter notwendig oder wenn der Kernbereich der exekutiven Eigenverantwortung betroffen ist, kann das Bundeskanzleramt die Unterrichtung nach Absatz 1 verweigern. Macht das Bundeskanzleramt von diesem Recht Gebrauch, so ist dies gegenüber dem Unabhängigen Kontrollrat zu begründen.

(3) Der Unabhängige Kontrollrat kann unter Beachtung des Geheimschutzes in abstrakter Weise und nach Anhörung des Bundeskanzleramtes den Deutschen Bundestag über Beanstandungen unterrichten. Das Bundeskanzleramt kann eine Stellungnahme beifügen.

§ 56

Pflicht des Bundesnachrichtendienstes zur Unterstützung

(1) Der Bundesnachrichtendienst unterstützt den Unabhängigen Kontrollrat bei seinen Aufgaben.

(2) Soweit seine Kontrollbefugnis reicht, kann der Unabhängige Kontrollrat vom Bundesnachrichtendienst verlangen, Akten oder andere in amtlicher Verwahrung befindliche Schriftstücke, soweit im Einzelfall ein berechtigtes Interesse besteht auch im Original, und in Dateien gespeicherte Daten zur Verfügung zu stellen.

(3) Dem Unabhängigen Kontrollrat ist jederzeit

1. Zutritt zu sämtlichen Dienststellen und
2. Zugang zu sämtlichen informationstechnischen Systemen, zu gewähren, soweit diese in alleiniger Verfügungsberechtigung des Bundesnachrichtendienstes stehen und dies für die Durchführung der Kontrolle erforderlich ist.

(4) Der Unabhängige Kontrollrat kann Mitarbeiterinnen und Mitarbeiter des Bundesnachrichtendienstes befragen oder von ihnen schriftliche Auskünfte einholen. Die Mitarbeiterinnen und Mitarbeiter des Bundesnachrichtendienstes sind verpflichtet, vollständige und wahrheitsgemäße Angaben zu machen.

(5) Den Verlangen des Unabhängigen Kontrollrates nach Absatz 4 hat der Bundesnachrichtendienst unverzüglich zu entsprechen.

§ 57

Personal- und Sachausstattung; Personalverwaltung

(1) Dem Unabhängigen Kontrollrat ist die für die Erfüllung seiner Aufgaben angemessene Personal- und Sachausstattung zur Verfügung zu stellen.

(2) Der Unabhängige Kontrollrat kann Aufgaben der Personalverwaltung und Personalwirtschaft auf das Bundeskanzleramt übertragen, soweit hierdurch die Unabhängigkeit des Unabhängigen Kontrollrates nicht beeinträchtigt wird. Diesen Stellen dürfen personenbezogene Daten der Beschäftigten übermittelt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist.

§ 58

Zusammenarbeit mit dem Parlamentarischen Kontrollgremium, der G 10-Kommission und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Der Unabhängige Kontrollrat, das Parlamentarische Kontrollgremium, die G10-Kommission und der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit können sich regelmäßig unter Wahrung der jeweils geltenden Geheimhaltungsvorschriften im Rahmen ihrer jeweiligen Kontrollzuständigkeit über allgemeine Angelegenheiten ihrer Kontrolltätigkeit austauschen.

(2) Die Rechte des Parlamentarischen Kontrollgremiums zur Kontrolle der Bundesregierung im Hinblick auf die Tätigkeit des Bundesnachrichtendienstes bleiben durch die Tätigkeit des Unabhängigen Kontrollrates unberührt. Die Rechte der G 10-Kommission und des oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur Kontrolle der Tätigkeit des Bundesnachrichtendienstes bleiben durch die Tätigkeit des Unabhängigen Kontrollrates unberührt.

Unterabschnitt 6 Mitteilungen und Evaluierung

§ 59

Mitteilung an Betroffene und Benachrichtigungspflichten

(1) Soweit personenbezogene Daten von Ausländern im Ausland erhoben werden, erfolgt keine Mitteilung an die betroffene Person.

(2) Werden Daten entgegen § 19 Absatz 7 Satz 1 erhoben und werden diese nach § 19 Absatz 7 Satz 5 nicht unverzüglich gelöscht, so ist die G 10-Kommission ihrer nächsten Sitzung darüber zu unterrichten und ist der betroffenen Person ist die Erhebung der Daten mitzuteilen, sobald

1. ausgeschlossen werden kann, dass hierdurch der Zweck der Maßnahme gefährdet ist, und
2. kein überwiegender Nachteil für das Wohl des Bundes oder eines Landes absehbar ist.

Erfolgt die Mitteilung nicht innerhalb von zwölf Monaten nach der Erhebung der Daten, bedarf die weitere Zurückstellung der Mitteilung der Zustimmung der G 10-Kommission. Die G 10-Kommission bestimmt die weitere Dauer der Zurückstellung. Fünf Jahre nach der Erhebung der Daten kann mit Zustimmung der G 10-Kommission endgültig von einer Mitteilung abgesehen werden, wenn die Voraussetzungen für die Mitteilung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden. Solange die personenbezogenen Daten für eine Mitteilung oder für eine gerichtliche Nachprüfung der Datenerhebung von Bedeutung sein können, wird die Löschung

zurückgestellt und die personenbezogenen Daten werden in ihrer Verarbeitung eingeschränkt; sie dürfen dann nur zu diesem Zweck verwendet werden.

§ 60 Mitteilungsverbote

(1) Personen, die Telekommunikations- oder Telemediendienste erbringen oder die an der Erbringung solcher Dienste mitwirken, sind in Bezug auf die ihnen gegenüber erfolgten Anordnungen und deren Umsetzung nach § 25 zur Verschwiegenheit verpflichtet.

(2) Erfolgt ein Auskunftersuchen oder eine Auskunftserteilung nach § 25 Absatz 1 Satz 1 auch in Verbindung mit § 24 Absatz 4, so darf diese Tatsache oder der Inhalt des Ersuchens oder der erteilten Auskunft von Personen, die zur Beantwortung verpflichtet oder mit der Beantwortung betraut sind oder die hieran mitwirken, anderen nicht mitgeteilt werden.

§ 61 Evaluierung

Der Unabhängige Kontrollrat erstellt alle fünf Jahre einen Bericht zur Evaluierung der Effektivität seiner Kontrolltätigkeit und übermittelt diesen dem Parlamentarischen Kontrollgremium. Das Bundeskanzleramt erhält vorab die Gelegenheit zur Stellungnahme zu diesem Bericht.

§ 62 Dienstvorschriften

Die technische und organisatorische Umsetzung der Regelungen zur technischen Aufklärung ist in Dienstvorschriften festzulegen. Die Dienstvorschriften bedürfen der Zustimmung des Bundeskanzleramtes. Das Bundeskanzleramt unterrichtet das Parlamentarische Kontrollgremium.“

22. Der bisherige § 32 wird § 63.
23. Der bisherige § 32a wird § 64 und in Nummer 2 wird nach der Angabe „46“ die Angabe „49, 50“ eingefügt.
24. Der bisherige § 33 wird § 65 und wie folgt neu gefasst:

„§ 65 Berichtspflicht und Information der Öffentlichkeit

(1) Der Bundesnachrichtendienst unterrichtet unmittelbar das Bundeskanzleramt die Bundesministerien im Rahmen ihrer Zuständigkeiten; hierbei ist auch die Übermittlung personenbezogener Daten zulässig. Die §§ 11, 29 und 38 finden Anwendung.

(2) Der Bundesnachrichtendienst kann die Öffentlichkeit über Erkenntnisse informieren, die er im Rahmen seiner Aufgaben nach § 1 Absatz 2 oder bei der Aufarbeitung seiner Historie gewinnt. Bei der Information darf er auch personenbezogene Daten bekanntgeben, wenn

1. dies für das Verständnis des Zusammenhanges oder für das Verständnis der Darstellung von Organisationen oder unorganisierten Gruppierungen erforderlich ist und
 2. die Interessen der Allgemeinheit das schutzwürdige Interesse des Betroffenen überwiegen.“
25. Der bisherige § 34 wird § 66 und die Angabe „§ 17“ wird durch die Angabe „§ 59 Absatz 2“ ersetzt.
26. Der bisherige § 35 wird § 67 und Absatz 1 wird wie folgt geändert:
- a) In Nummer 1 werden die Wörter „§ 8 Absatz 1 Satz 1 oder Absatz 2 Satz 3“ durch die Wörter „§ 25 Absatz 1 Satz 1 oder Absatz 3 Satz 3“ ersetzt.
 - b) In Nummer 2 werden die Wörter „§ 8 Absatz 2 Satz 2“ durch die Wörter „§ 25 Absatz 3 Satz 2“ ersetzt.
27. Der bisherige § 36 wird durch die folgenden §§ 68 und 69 ersetzt:

„§ 68

Einschränkung von Grundrechten

Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) sowie das Grundrecht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) werden durch dieses Gesetz eingeschränkt.

§ 69

Übergangsvorschriften

(1) Maßnahmen der technischen Aufklärung im Sinne des Abschnitts 4, die bereits vor dem 1. Januar 2022 begonnen wurden, dürfen bis zum 31. Dezember 2022 fortgeführt werden. Diese Maßnahmen unterliegen der Rechtskontrolle durch das administrative Kontrollorgan. § 51 findet entsprechende Anwendung. Wird die Maßnahme erstmals nach § 23 Absatz 1 oder Absatz 5 oder § 37 Absatz 1 angeordnet und bestätigt das gerichtsähnliche Kontrollorgan die Rechtmäßigkeit der Anordnung nicht, ist die Maßnahme unverzüglich einzustellen.

(2) Die Speicherung von Daten, die vor dem 1. Januar 2022 erhoben wurden, sowie die Speicherung von Daten, die auf der Grundlage einer Maßnahme nach Absatz 1 erhoben wurden, bestimmt sich nach den §§ 18 und 19 in der am 19. Juni 2020 geltenden Fassung.

(3) Die Übermittlung von Daten, die vor dem 1. Januar 2022 erhoben wurden, sowie die Übermittlung von Daten, die auf der Grundlage einer Maßnahme nach Absatz 1 erhoben wurden, bestimmt sich nach § 23 in der am 19. Juni 2020 geltenden Fassung.

(4) Bis zur Schaffung der technischen Voraussetzungen für die in § 19 Absatz 10 Satz 1 und § 34 Absatz 8 Satz 1 vorgesehene Kennzeichnung ist die Weiterverarbeitung der nach Abschnitt 4 erhobenen personenbezogener Daten in den bestehenden Systemen des Bundesnachrichtendienstes auch ohne die Kennzeichnung zulässig, sofern hinsichtlich der ab dem 1. Januar 2022 erhobenen Daten jeweils der Zweck und das Mittel der Datenerhebung anderweitig nachvollziehbar sind. Die Weiterverarbeitung in den strukturierten Grundlagenbanken des Bundesnachrichtendienstes ist darüber

hinaus bis zur Schaffung der technischen Voraussetzungen für die Kennzeichnung von Zweck und Mittel auch dann zulässig, wenn der Zweck und das Mittel der Datenerhebung nicht für jedes Datenfeld anderweitig nachvollziehbar sind; die Übermittlung dieser Daten richtet sich insoweit nach Absatz 3. Das Bundeskanzleramt berichtet dem Parlamentarischen Kontrollgremium jährlich über den Fortschritt bei der Schaffung der technischen Voraussetzungen für die Kennzeichnung nach Satz 2.

(5) Die am 1. Januar 2022 bestehenden Kooperationsvereinbarungen mit ausländischen öffentlichen Stellen nach § 13 in der am 19. Juni 2020 geltenden Fassung gelten bis längstens zum 31. Dezember 2024 fort.“

Artikel 2 **Änderung des Artikel 10-Gesetzes**

Das Artikel 10-Gesetz vom 26. Juni 2001 (BGBl. I S. 1254, 2298; 2007 I S. 154), das zuletzt durch Artikel 38 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:

1. Nach § 4 wird folgender § 4a eingefügt:

„§ 4a

Weiterverarbeitung von Verkehrsdaten durch den Bundesnachrichtendienst

(1) Der Bundesnachrichtendienst darf erhobene Verkehrsdaten, bei denen für einen Teilnehmer der Kommunikation eine Beschränkung nach § 3 angeordnet ist, zur Erfüllung seiner Aufgaben auch weiterverarbeiten, um

1. Personen zu erkennen, die einen Deutschlandbezug aufweisen und über die Informationen erlangt werden können, die für die Aufgabenerfüllung des Bundesnachrichtendienstes relevant sind, oder
2. geeignete Übertragungswege im Sinne des § 10 Absatz 4 Satz 2 zu bestimmen.

(2) Spätestens drei Monate nach ihrer Erhebung sind die nach Absatz 1 gespeicherten Verkehrsdaten daraufhin zu prüfen, ob die weitere Speicherung zur Erfüllung der Aufgaben des Bundesnachrichtendienstes erforderlich ist. Spätestens sechs Monate nach ihrer Erhebung sind diese Daten zu löschen, es sei denn, es wurde im Einzelfall festgestellt, dass eine weitere Speicherung für die Zwecke des Absatzes 1 erforderlich ist. Ist im Einzelfall festgestellt worden, dass eine weitere Speicherung für die Zwecke nach Absatz 1 erforderlich ist, prüft der Bundesnachrichtendienst sodann regelmäßig in Abständen von höchstens sechs Monaten, ob die weitere Speicherung der Verkehrsdaten für diese Zwecke erforderlich ist.

(3) Die Erfüllung der in den Absätzen 1 und 2 genannten Voraussetzungen wird regelmäßig stichprobenartig durch eine hierzu beauftragte Bedienstete des Bundesnachrichtendienstes oder einen hierzu beauftragten Bediensteten des Bundesnachrichtendienstes, der die Befähigung zum Richteramt hat, überprüft. Soweit die Überprüfung eine unzulässige Verarbeitung ergibt, sind die Daten unverzüglich unter Aufsicht einer Bediensteten oder eines Bediensteten des Bundesnachrichtendienstes, die oder der die Befähigung zum Richteramt hat, zu löschen. § 4 Absatz 1 Satz 3 bis 5 gilt entsprechend.“

2. § 6 wird wie folgt geändert:

- a) In Absatz 1 Satz 4 werden die Wörter „zu Zwecken der Datenschutzkontrolle“ durch die Worte „zur Durchführung von Kontrollen der Datenverarbeitung, einschließlich der Datenschutzkontrolle,“ ersetzt.
- b) In Absatz 3 Satz 5 werden die Wörter „zu Zwecken der Datenschutzkontrolle“ durch die Worte „zur Durchführung von Kontrollen der Datenverarbeitung, einschließlich der Datenschutzkontrolle,“ ersetzt.
- c) Die folgenden Absätze 4 bis 6 werden angefügt:
„(4) Unabhängig von Absatz 1 Satz 1 und 2 darf der Bundesnachrichtendienst auf den nach § 5 Absatz 1 in Verbindung mit § 10 Absatz 4 Satz 2 angeordneten Übertragungswegen zur Erfüllung seiner Aufgaben Verkehrsdaten erheben und unter den Voraussetzungen des Satzes 3 weiterverarbeiten, sofern diejenigen

Verkehrsdaten, die eine Identifizierung von deutschen Staatsangehörigen, von inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen ermöglichen, im Falle ihrer Erhebung unverzüglich automatisiert unkenntlich gemacht werden. Die automatisierte Unkenntlichmachung ist so durchzuführen, dass

1. die Eindeutigkeit der Daten erhalten bleibt und
2. eine rückwirkende Identifizierung der in Satz 1 genannten Personen unmöglich oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

Der Bundesnachrichtendienst darf Verkehrsdaten, die nach den Sätzen 1 und 2 unkenntlich gemacht wurden, zur Erfüllung seiner Aufgaben weiterverarbeiten, um

1. Personen außerhalb des in Satz 1 genannten Personenkreises zu erkennen, die einen Deutschlandbezug aufweisen und über die Informationen erlangt werden können, die für die Aufgabenerfüllung des Bundesnachrichtendienstes relevant sind, sowie
2. geeignete Übertragungswege im Sinne des § 10 Absatz 4 Satz 2 zu bestimmen.

Die in Satz 1 genannten Verkehrsdaten sind spätestens sechs Monate nach ihrer Erhebung zu löschen, es sei denn, es wurde im Einzelfall festgestellt, dass eine weitere Speicherung für die Zwecke nach Satz 3 erforderlich ist. Ist im Einzelfall festgestellt worden, dass eine weitere Speicherung für die Zwecke nach Satz 3 erforderlich ist, prüft der Bundesnachrichtendienst bei der Einzelfallbearbeitung und nach festgesetzten Fristen, spätestens nach zehn Jahren, ob die unkenntlich gemachten Verkehrsdaten weiterhin für diese Zwecke erforderlich sind.

(5) Unabhängig von Absatz 1 Satz 1 und 2 darf der Bundesnachrichtendienst erhobene Verkehrsdaten, die auf der Grundlage eines Suchbegriffs nach § 5 Absatz 2 erfasst worden sind, zur Erfüllung seiner Aufgaben weiterverarbeiten, um

1. Personen zu erkennen, die einen Deutschlandbezug aufweisen und über die Informationen erlangt werden können, die für die Aufgabenerfüllung des Bundesnachrichtendienstes relevant sind, sowie
2. geeignete Übertragungswege im Sinne des § 10 Absatz 4 Satz 2 zu identifizieren.

Wird bei der Weiterverarbeitung nach Satz 1 erkannt, dass eine darüber hinausgehende Weiterverarbeitung der Verkehrsdaten durch den Bundesnachrichtendienst erforderlich ist, um Straftaten im Sinne des § 3 Absatz 1 oder Gefahren im Sinne des § 5 Absatz 1 Satz 3 oder des § 8 Absatz 1 zu erkennen und einer solchen Gefahr zu begegnen, darf der Bundesnachrichtendienst diese Daten auch zu diesen Zwecken weiterverarbeiten.

Spätestens drei Monate nach ihrer Erhebung sind die in den Sätzen 1 und 2 genannten Verkehrsdaten daraufhin zu prüfen, ob die weitere Speicherung zur Erfüllung der Aufgaben des Bundesnachrichtendienstes erforderlich ist. Spätestens sechs Monate nach ihrer Erhebung sind die in den Sätzen 1 und 2 genannten Daten zu löschen, es sei denn, es wurde im Einzelfall festgestellt, dass eine weitere Speicherung für die Zwecke nach den Sätzen 1 und 2 erforderlich ist. Ist im Einzelfall festgestellt worden, dass eine weitere Speicherung für die Zwecke nach den Sätzen 1 und 2 erforderlich ist, prüft der Bundesnachrichtendienst sodann regelmäßig in Abständen von höchstens

sechs Monaten, ob die weitere Speicherung der Verkehrsdaten für diese Zwecke nach den Sätzen 1 und 2 erforderlich ist.

(6) Die Erfüllung der in Absatz 5 genannten Voraussetzungen wird regelmäßig stichprobenartig durch eine hierzu beauftragte Bedienstete oder einen hierzu beauftragten Bediensteten des Bundesnachrichtendienstes, die oder der die Befähigung zum Richteramt hat, überprüft. Soweit die Überprüfung eine unzulässige Verarbeitung ergibt, sind die Daten unverzüglich unter Aufsicht eines Bediensteten des Bundesnachrichtendienstes, der die Befähigung zum Richteramt hat, zu löschen. Absatz 1 Satz 3 bis 5 gilt entsprechend.“

3. In § 7 Absatz 1 werden die Worte „§ 33 des BND-Gesetzes“ geändert in „§ 65 Absatz 1“.
4. § 8 wird wie folgt geändert:
 - a) Absatz 4 Satz 4 wird wie folgt gefasst:
„§ 6 Absatz 1 Satz 4 und 5, Absatz 2 Satz 1 und 2 und Absatz 5 und 6 mit der Maßgabe, dass die Weiterverarbeitung nach Absatz 5 Satz 2 nur zur Erkennung und Begegnung von Gefahren im Sinne des § 8 Absatz 1 zulässig ist, gilt entsprechend.“
 - b) In Absatz 5 wird die Angabe „§ 33“ durch die Angabe „§ 65 Absatz 1“ ersetzt.

Artikel 3 **Änderung des Bundesbesoldungsgesetzes** [noch zu ergänzen]

Artikel 4 **Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung - TKÜV)**

Telekommunikations-Überwachungsverordnung in der Fassung der Bekanntmachung vom 11. Juli 2017 (BGBl. S. 2316), die zuletzt durch Artikel 27 des Gesetzes vom 20. November 2019 (BGBl. I S. 1724) geändert worden ist.

1. In § 1 Nummer 1 Buchstabe e) werden die Worte „§§ 6, 12 und 14 des BND-Gesetzes“ geändert in „§§ 19, 24 und 26 des BND-Gesetzes“.
2. In § 1 Nummer 4 werden die Worte „§§ 6, 12 oder 14 des BND-Gesetzes“ geändert in „§§ 19, 24 und 26 des BND-Gesetzes“.
3. In § 2 Nummer 1 Buchstabe a) werden die Worte „§ 9 des BND-Gesetzes“ geändert in „§ 25 Absatz 1 Satz 1 des BND-Gesetzes“.
4. In § 2 Nummer 3 Buchstabe a) werden die Worte „§§ 6, 12 oder 14 des BND-Gesetzes“ geändert in „§§ 19, 24 und 26 des BND-Gesetzes“.
5. In § 2 Nummer 15 werden die Worte „§§ 6, 12 oder 14 des BND-Gesetzes“ geändert in „§§ 19, 24 und 26 des BND-Gesetzes“.

6. In § 2 Nummer 17 Buchstabe c) werden die Worte „§§ 6, 12 oder 14 des BND-Gesetzes“ geändert in „§§ 19, 24 und 26 des BND-Gesetzes“.
7. In der Überschrift des Teils 3 werden die Worte „§§ 6, 12 und 14 des BND-Gesetzes“ geändert in „19, 24 und 26 des BND-Gesetzes“.
8. In § 27 Absatz 1 Satz 1 werden die Worte „§§ 6, 12 oder 14 des BND-Gesetzes die Telekommunikation, die in dem in der Anordnung bezeichneten Telekommunikationsnetz übermittelt wird, einschließlich der in diesem Telekommunikationsnetz“ geändert in „§§ 19, 24 und 26 des BND-Gesetzes die Telekommunikation, die in der Anordnung nach § 25 Absatz 1 Satz 1 des BND-Gesetzes bezeichnet wird, einschließlich der in dieser Telekommunikation“.
9. In § 27 Absatz 8 Satz 2 werden die Worte „§§ 6, 12 oder 14 des BND-Gesetzes eine Anordnung nach § 6 Absatz 1 Satz 2 des BND-Gesetzes“ geändert in „§§ 19, 24 und 26 des BND-Gesetzes eine Anordnung nach § 25 Absatz 1 Satz 1 des BND-Gesetzes“.
10. In § 28 Absatz 1 werden die Worte „§§ 6, 12 oder 14 des BND-Gesetzes“ geändert in „§§ 19, 24 und 26 des BND-Gesetzes“.

Artikel 5

Zollverwaltungsgesetz (ZollVG)

Zollverwaltungsgesetz vom 21. Dezember 1992 (BGBl. I S. 2125; 1993 I S. 2493), das zuletzt durch Artikel 210 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist.

In § 12a Absatz 8 werden die Worte „§ 8 des BND-Gesetzes“ geändert in „§ 10 des BND-Gesetzes“.

Artikel 6

Gesetz zum Schutz vor Gefährdung der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten (Satellitendatensicherheitsgesetz - SatDSiG)

Satellitendatensicherheitsgesetz vom 23. November 2007 (BGBl. I S. 2590), das zuletzt durch Artikel 2 des Gesetzes vom 10. Juli 2020 (BGBl. I S. 1637) geändert worden ist.

In § 27 Absatz 1 Satz 2 werden die Worte „§ 23 Abs. 3 des BND-Gesetzes“ geändert in „§ 10 Absatz 3 des BND-Gesetzes“.

Artikel 7

Telekommunikationsgesetz (TKG)

Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 319 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist.

1. In § 110 Absatz 1 Nummer 5 werden die Worte „§ 6, 12 und 14 des BND-Gesetzes“ geändert in „§§ 19, 24 und 26 des BND-Gesetzes“.
2. In § 110 Absatz 2 werden die Worte „§ 8 Absatz 1 Satz 1 des BND-Gesetzes“ geändert in „§ 25 Absatz 1 Satz 1 des BND-Gesetzes“.
3. In § 114 Absatz 1 Nummer 5 werden die Worte „§ 6, 12 und 14 des BND-Gesetzes“ geändert in „§§ 19, 24 und 26 des BND-Gesetzes“.

Artikel 8

Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlussachen (Sicherheitsüberprüfungsgesetz - SÜG)

Sicherheitsüberprüfungsgesetz vom 20. April 1994 (BGBl. I S. 867), das zuletzt durch Artikel 20 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist.

In § 36 Absatz 2 werden die Worte „§ 31 des BND-Gesetzes“ geändert in „§ 12 des BND-Gesetzes“ und die Worte „§ 21 des BND-Gesetzes“ geändert in „§ 18 des BND-Gesetzes“

Artikel 9

Gesetz über das Ausländerzentralregister (AZR-Gesetz)

AZR-Gesetz vom 2. September 1994 (BGBl. I S. 2265), das zuletzt durch Artikel 167 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist.

1. In § 11 Absatz 2 werden die Worte „§ 33 des BND-Gesetzes“ geändert in „§ 65 Absatz 1 des BND-Gesetzes“.
2. In § 34 Absatz 3 werden die Worte „§ 22 des BND-Gesetzes“ geändert in „§ 9 des BND-Gesetzes“.

Artikel 10

Strafprozeßordnung (StPO)

Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 des Gesetzes vom 9. Oktober 2020 (BGBl. I S. 2075) geändert worden ist.

1. In § 474 Absatz 2 werden die Worte „§ 23 des BND-Gesetzes“ geändert in „§ 10 des BND-Gesetzes“.
2. In § 492 Absatz 4 werden die Worte „§ 23 Absatz 3 des BND-Gesetzes“ geändert in „§ 10 Absatz 3 des BND-Gesetzes“.

Artikel 11

Bekanntmachungserlaubnis

Das Bundeskanzleramt kann den Wortlaut des BND-Gesetzes in der vom Inkrafttreten dieses Gesetzes an geltenden Fassung im Bundesgesetzblatt bekannt machen.

Artikel 12 Eingriff in Grundrechte

Durch Abschnitt 4 des Artikel 1 (BNDG) sowie durch Artikel 2 (G10) wird das Grundrecht des Post-, Brief- und Fernmeldegeheimnis (Artikel 10 GG) eingeschränkt.

Artikel 13 Inkrafttreten

In Artikel 1 Nummer 21 treten die §§ 41, 43 bis 50 und 53 des BND-Gesetzes am Tag nach der Verkündung in Kraft. Im Übrigen tritt dieses Gesetz am 1. Januar 2022 in Kraft. Im Übrigen tritt dieses Gesetz tritt am 1. Januar 2022 in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Das Bundesverfassungsgericht hat mit seiner Entscheidung vom 19. Mai 2020 - 1 BvR 2835/17 (BND - Ausland-Ausland-Fernmeldeaufklärung) die §§ 6, 7, 13 bis 15 des Gesetzes über den Bundesnachrichtendienst (BNDG) für mit Artikel 10 Absatz 1 Grundgesetz (GG) sowie mit Artikel 5 Absatz 1 GG nicht vereinbar erklärt und dem Gesetzgeber eine Frist für eine verfassungskonforme Neuregelung bis zum 31. Dezember 2021 gesetzt. Das Gleiche gilt für § 19 Absatz 1 und § 24 Absatz 1 Satz 1, Absatz 2 Satz 1 und Absatz 3 BNDG, soweit sie zur Verarbeitung personenbezogener Daten berechtigen.

Der gesetzliche Auftrag des Bundesnachrichtendienstes ist die Gewinnung von Erkenntnissen über das Ausland, die von außen- oder sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind. Hierdurch leistet der Bundesnachrichtendienst einen unverzichtbaren Beitrag für die Sicherheitsarchitektur der Bundesrepublik Deutschland.

Die strategische Fernmeldeaufklärung stellt in diesem Zusammenhang ein wesentliches Element dar. Durch sie ist der Bundesnachrichtendienst in der Lage, ohne Zeitverzug aktuelle Geschehnisse zu erfassen und politische Bedarfsträger und auch internationale Partner hierüber zu informieren.

In einer globalisierten und technisch vernetzten Welt gewinnt die technische Aufklärung durch Nachrichtendienste eine zunehmend große Bedeutung. Um Gefahrenbereiche umfassend aufklären zu können, ist es für die Arbeit des Bundesnachrichtendienstes unerlässlich, mit den technischen Entwicklungen einer mehr und mehr vernetzten Welt Stand halten zu können. Die dabei genutzten Kommunikationsformen sind volatil und fortlaufenden Veränderungen unterworfen.

Schon im Zuge der letzten Novellierung des BNDG im Jahr 2016 wurde versucht, dieser Entwicklung durch die Schaffung angemessener und hinreichend bestimmter Rechtsgrundlagen zu begegnen.

Stützte der Bundesnachrichtendienst zuvor seine Durchführung der strategischen Ausland-Fernmeldeaufklärung allein auf die gesetzliche Aufgabenzuweisungsnorm des § 1 Absatz 2 BNDG, wurde im Rahmen der letzten Novelle die damalige Rechtslage präzisiert und spezielle rechtliche Grundlagen für die strategische Fernmeldeaufklärung von Ausländern im Ausland vom Inland aus sowie diesbezügliche Kooperationen mit ausländischen öffentlichen Stellen geschaffen. Auch für die gemeinsame Datenhaltung mit ausländischen öffentlichen Stellen wurde eine eigene Rechtsgrundlage geschaffen.

Mit seinem Urteil vom 19. Mai 2020 (1 BvR 2835/17) hat das Bundesverfassungsgericht dem Gesetzgeber in diesem Bereich jedoch darüberhinausgehende Vorgaben gemacht,

indem das Gericht vor allem den bis dahin nicht höchstrichterlich geklärten Geltungsbereich der Grundrechte des deutschen Grundgesetzes definiert hat. Das vor allem durch die technische Aufklärung von Nachrichtendiensten betroffene Grundrecht des Brief-, Post- und Fernmeldegeheimnis des Artikels 10 Absatz 1 GG findet demnach auch auf Ausländer im Ausland Anwendung. Diese Ausweitung des Anwendungsbereichs hat zur Folge, dass der Gesetzgeber die Normen des BNDG einer grundsätzlichen Überprüfung unterziehen musste.

Um den verfassungsgerichtlichen Vorgaben gerecht zu werden und den geforderten Grundrechtsschutz zu gewährleisten, müssen die einschlägigen Normen des BNDG grundlegend überarbeitet werden, um den geforderten Grundrechtsschutz zu gewährleisten; dabei muss der Gesetzgeber dabei der hervorgehobenen Rolle des Bundesnachrichtendienstes im Rahmen der Sicherheitsarchitektur der Bundesrepublik Deutschland Rechnung tragen. Das Bundesverfassungsgericht hat insoweit betont, dass das öffentliche Interesse an einer wirksamen Auslandsaufklärung - und in diesem Zusammenhang auch an einer effektiven technischen Aufklärung - überragend ist.

Das Ziel dieser grundlegenden Novelle der bestehenden Rechtslage des Bundesnachrichtendienstes ist somit, die Arbeit des Bundesnachrichtendienstes im Rahmen der technischen Aufklärung auf eine rechtssichere und bestimmte Rechtsgrundlage zu stellen, welche dem vom Bundesverfassungsgericht gezogenen verfassungsrechtlichen Rahmen ausreichend Rechnung trägt.

II. Wesentlicher Inhalt des Entwurfs

Der Entwurf setzt die zuvor genannten Vorgaben aus dem Urteil und die darin zum Ausdruck kommenden Regelungsaufträge an den Gesetzgeber um.

Diesem ist der Gesetzgeber insbesondere im neuen Abschnitt 4 des Gesetzes (§§ 19 bis 39) nachgekommen, indem beispielsweise die Erhebung personenbezogener Daten im Rahmen der strategischen Ausland-Fernmeldeaufklärung den in § 19 genannten qualifizierten Aufklärungszwecken auf der Grundlage eigens zuvor festgelegter Maßnahmen unterliegen muss. § 20 regelt bestimmte zusätzliche Hürden bei besonderen Formen der gezielten Datenerhebung. Besondere Vorkehrungen zum Individualschutz treffen § 21 und § 22, welche Maßgaben zum Schutz bestimmter Vertraulichkeitsbeziehungen und der Gewährleistung des Schutzes des Kernbereichs privater Lebensgestaltung beinhalten.

Den weiteren richterlichen Forderungen nach konkreten Maßgaben zur Aussonderung der Telekommunikationsdaten von Deutschen und Inländern, einer Begrenzung des Volumens der zu erhebenden Daten, einer Erhebungsgrundlage für Verkehrsdaten ohne den vorherigen Einsatz von Suchbegriffen, sowie der besonderen Eingriffstiefe von Maßnahmen der Ausland-Fernmeldeaufklärung Rechnung tragenden Bestimmungen zur Datenauswertung und Löschpflichten, wird ebenfalls in diesem Abschnitt Rechnung getragen.

Darüber hinaus wurde die Übermittlung personenbezogener Daten aus der strategischen Ausland-Fernmeldeaufklärung neu ausgestaltet. Den Vorgaben des Bundesverfassungsgerichts folgend, beinhalten die §§ 29 und 30 klare Vorgaben, die die Übermittlung solcher personenbezogener Daten nur zum Schutz besonders gewichtiger Rechtsgüter erlauben. Dazu bedarf es tatsächlicher Anhaltspunkte, dass dies erforderlich

ist zur Abwehr einer Gefahr für besonders gewichtige Rechtsgüter oder zur Abwehr einer besonders schwerwiegenden Beeinträchtigung der Rechte Einzelner sowie der Einhaltung formaler Vorgaben. Von diesen strengen Vorgaben jedoch abweichend gilt ein solcher Maßstab nicht für die Unterrichtung der Bundesregierung oder Landesregierungen, welche ausschließlich der politischen Information und Vorbereitung von Regierungsentscheidungen dient.

Umgesetzt wurden des Weiteren die vom Bundesverfassungsgericht gesetzten Maßstäbe im Rahmen der Kooperation mit ausländischen Nachrichtendiensten. Um den verfassungsrechtlich gebotenen Leitlinien zu entsprechen, setzen die §§ 31 bis 33 die richterliche Forderung um, dass die Verantwortung des Bundesnachrichtendienstes für die von ihm erhobenen und ausgewerteten Daten im Rahmen des gegenseitigen Austausches gewahrt bleibt. Dabei trifft den Bundesnachrichtendienst eine strenge Kontroll- und Vergewisserungspflicht. Er hat darüber hinaus gehaltvolle Zusagen von seinem Kooperationspartner einzuholen.

Ein erhebliches Mehr an Rechtssicherheit schaffen auch die spezialgesetzlichen Regelungen besonderer Formen der technischen Aufklärung in den §§ 34 bis 39. Der nunmehr gesetzlich speziell geregelte Eingriff in informationstechnische Systeme von Ausländern im Ausland hegt eine solche Maßnahme ein in ein rechtsstaatlich strukturiertes System mit dem ebenfalls berücksichtigten Schutz von Vertraulichkeitsbeziehungen und des Kernbereichs privater Lebensgestaltung. Besondere Maßgaben für die Übermittlung von Daten, die aus einer solchen Maßnahme gewonnen wurden, knüpfen dabei an die aktuelle Entscheidung des Bundesverfassungsgerichts an.

Zuletzt wird die strategische Ausland-Fernmeldeaufklärung zukünftig durch eine starke und unabhängige objektivrechtliche Kontrolle flankiert werden. In Umsetzung der verfassungsgerichtlichen Vorgaben regeln die §§ 40 bis 58 die Einführung des Unabhängigen Kontrollrates, welcher zukünftig als oberste Bundesbehörde seine Arbeit aufnehmen wird, sowie dessen Befugnisse. Er beinhaltet zwei Kontrollorgane: Ein gerichtsähnliches Kontrollorgan für die gerichtsähnliche Rechtskontrolle mit abschließender Entscheidungsbefugnis, das die wesentlichen Verfahrensschritte ex-ante prüft, und ein administratives Kontrollorgan der administrativen Rechtskontrolle, das den gesamten Prozess der strategischen Ausland-Fernmeldeaufklärung eigeninitiativ und stichprobenartig einsehen und prüfen kann. Darüber hinaus unterliegen alle Eingriffe in informationstechnische Systeme von Ausländern im Ausland vor deren Durchführung der umfassenden Rechtmäßigkeitsprüfung durch den Unabhängigen Kontrollrat. Dieses von der sogenannten Third-Party-Rule unabhängige agierende Kontrollorgan, verfügt über institutionelle Eigenständigkeit, was in seiner eigenen Personalhoheit und Verfahrensautonomie Ausdruck findet.

Für den Bundesnachrichtendienst werden ferner Rechtsgrundlagen zur Verarbeitung von Verkehrsdaten von deutschen Staatsangehörigen, inländischen juristischen Personen oder sich im Bundesgebiet aufhaltenden Personen geschaffen, deren Verarbeitung nach der Rechtsprechung des Bundesverwaltungsgericht auch in anonymisierter Form einer speziellen Rechtsgrundlage bedarf. Die Verarbeitung dieser Verkehrsdaten ist einer konkreten Zweckbindung unterworfen und steht unter der Voraussetzung, dass die weiterverarbeiteten Verkehrsdaten grundsätzlich keine Identifizierung der geschützten Telekommunikationsteilnehmer oder Anschluss Teilnehmer erlauben.

III. Alternativen

Keine.

IV. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes für die Änderung des BND-Gesetzes ergibt sich aus Artikel 73 Absatz 1 Nummer 1 GG. Die Gesetzgebungskompetenz für die Änderung des Artikel 10-Gesetzes folgt aus Artikel 73 Absatz 1 Nummer 10 Buchstabe b) und c) 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 Datenverarbeitung in ihren Persönlichkeitsrechten betroffen sind, her.

1. Rechts- und Verwaltungsvereinfachung

[noch zu ergänzen]

2. Nachhaltigkeitsaspekte

[noch zu ergänzen]

3. Haushaltsausgaben ohne Erfüllungsaufwand

Es entstehen keine Haushaltsausgaben ohne Erfüllungsaufwand.

4. Erfüllungsaufwand

a) Erfüllungsaufwand für Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

b) Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entsteht Erfüllungsaufwand in nicht bezifferbarer Höhe.

c) Erfüllungsaufwand für die Verwaltung

[noch zu ergänzen]

5. Weitere Kosten

Weitere Kosten sind nicht zu erwarten.

6. Weitere Gesetzesfolgen

Keine.

7. Befristung; Evaluierung

Eine fortlaufende Evaluierung des Abschnittes 4 (Technische Aufklärung) erfolgt auf Grundlage des § 61 des Gesetzesentwurfes.

B. Besonderer Teil

Zu Artikel 1 (Änderung des BNDG)

Zu Nummer 1

Die Überschrift wurde redaktionell angepasst.

Zu Nummer 2 (§ 1 Organisation und Aufgaben)

Die Änderung in Absatz 2 Satz 2 ergibt sich aus dem geänderten Aufbau des Gesetzes, eine materielle Änderung der Befugnisse erfolgt nicht.

Zu Nummer 3 (§ 3 Besondere Auskunftsverlangen)

Der in Absatz 3 enthaltene Hinweis auf die insoweit erfolgende Einschränkung des Grundrechts des Fernmeldegeheimnisses (Artikel 10 des GG) wurde gestrichen, da nunmehr ein solcher Verweis im eigens zur Erfüllung des Zitiergebotes neu geschaffenen § 64 enthalten ist.

Zu Nummer 4 (§ 4 Weitere Auskunftsverlangen)

Die Einschränkung des Grundrechts aus Artikel 10 Absatz 1 des GG ergibt sich nunmehr aus § 68.

Zu Nummer 5 (§ 5 Besondere Formen der Datenerhebung)

Der Verweis auf § 8 Absatz 2 des Bundesverfassungsschutzgesetzes (BVerfSchG) wird von Satz 1 in Satz 2 verschoben. Außerdem wird ein Verweis auf § 1 Absatz 2 Satz 1 aufgenommen. Eine inhaltliche Änderung des rechtlichen Handlungsrahmens des Bundesnachrichtendienstes im Vergleich zur Vorversion erfolgt nicht.

Zu Nummer 6 (Abschnitt 2 Weiterverarbeitung von Daten)

Im Abschnitt 2 werden allgemeine Aussagen zur Weiterverarbeitung von Daten, die bisher im Abschnitt 3 geregelt waren, nach vorne verschoben. Der vormalige Abschnitt 2 „Ausland-Ausland-Fernmeldeaufklärung“ wird damit zum Abschnitt 4. Die Überschrift des Abschnitts wird geringfügig sprachlich verändert („Weiterverarbeitung von Daten“ statt „Datenweiterverarbeitung“).

Zu Nummer 7 (Aufhebung der §§ 6 bis 18)

Die §§ 6 bis 18 werden aus dem Gesetz gestrichen.

Zu Nummer 8 (Streichung der Überschrift des Abschnitts 3)

Die Überschrift des Abschnitts 3 wird gestrichen.

Zu Nummer 9

Die §§ 6 bis 8 wurden redaktionell angepasst.

Zu Nummer 10

§ 9 wird redaktionell angepasst.

Zu Nummer 11 (Abschnitt 3 Übermittlung von Daten und gemeinsame Dateien)

Die Überschrift wurde redaktionell angepasst.

Zu Nummer 12 (§ 10 Übermittlung von Informationen an den Bundesnachrichtendienst)

Die Norm wurde redaktionell angepasst.

Zu Nummer 13 (§ 11 Übermittlung von Informationen durch den Bundesnachrichtendienst)

Die Norm wurde redaktionell angepasst.

Zu Nummer 14 (§ 12 Projektbezogene gemeinsame Dateien mit inländischen öffentlichen Stellen)

§ 12 entspricht im Wesentlichen der Regelung in der bisherigen Fassung des § 25, die nur an wenigen Stellen angepasst wurde. So wurde in Absatz 1 Satz 1 die Möglichkeit geschaffen, projektbezogene gemeinsame Dateien auch mit Dienststellen im Geschäftsbereich des Bundesministeriums der Verteidigung zu führen. Konsequenterweise wurde in Absatz 1 Satz 2 der Zweck der Dateien daher um die Landes- und Bündnisverteidigung sowie die Unterstützung von Auslandseinsätzen der Bundeswehr erweitert. Ein Bedürfnis für diese Änderung ergibt sich aus dem Umstand, dass der Bundesnachrichtendienst der alleinige Auslandsnachrichtendienst der Bundesrepublik Deutschland ist und die Bundeswehr daher auf eine Führung gemeinsamer projektbezogener Dateien im angewiesen ist. In Absatz 3 sind die Verweise an die geänderte Reihenfolge der Bezugsnormen angepasst worden. In Absatz 6 wurde klarstellend ergänzt, dass der Bundesnachrichtendienst nur in den Fällen des Absatzes 3, also wenn er selbst die gemeinsame Datei führt, eine Dateianordnung nach § 8 erstellt. In den Fällen, in denen die Dateiführung bei einer anderen inländischen öffentlichen Stelle liegt, verfügt der Bundesnachrichtendienst nicht über die für ein Dateianordnungsverfahren erforderlichen Informationen, so dass die Erstellung einer Dateianordnung nicht möglich ist.

Zu Nummer 15 (§ 13 Gemeinsame Dateien mit ausländischen öffentlichen Stellen)

Die Regelung entspricht dem bisherigen § 26 und wird nur in Absatz 1 hinsichtlich der Verweise aktualisiert sowie redaktionell angepasst.

Zu Nummer 16 (§ 14 Führung gemeinsamer Dateien durch den Bundesnachrichtendienst mit ausländischen öffentlichen Stellen)

Die Regelung entspricht dem bisherigen § 27 und wird in Absatz 1 hinsichtlich der Verweise aktualisiert sowie redaktionell angepasst. Die Ergänzung des Regelungstitels um ausländische öffentliche Stellen erfolgt aus Gründen der Klarstellung.

Zu Nummer 17 (§ 15 Dateianordnung bei gemeinsamen Dateien mit ausländischen öffentlichen Stellen)

Die Regelung entspricht dem bisherigen § 28. Im Regelungstitel wird die Ergänzung um ausländische öffentliche Stellen aufgenommen.

Zu Nummer 18 (§ 16 Eingabe in und Zugriff auf die vom Bundesnachrichtendienst geführten gemeinsamen Dateien mit ausländischen öffentlichen Stellen)

Die Regelung entspricht dem bisherigen § 29 und wird in Absatz 2 hinsichtlich der Verweise aktualisiert sowie redaktionell angepasst. Wie schon bei §§ 14, 15 erfolgt auch hier aus Gründen der Klarstellung die Ergänzung des Regelungstitels um ausländische öffentliche Stellen.

Zu Nummer 19 (§ 17 Beteiligung an gemeinsamen Dateien mit ausländischen öffentlichen Stellen)

Die Regelung entspricht dem bisherigen § 30 und wird lediglich hinsichtlich der Verweise aktualisiert.

Zu Nummer 20 (§ 18) Verfahrensregeln für die Übermittlung von Informationen

Die Regelung entspricht dem bisherigen § 31 und wird nur hinsichtlich der Verweise aktualisiert.

Zu Nummer 21 (Abschnitt 4 technische Aufklärung)

Der Abschnitt 4 wird neu eingefügt.

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

§ 19 (Strategische Ausland-Fernmeldeaufklärung)

Die strategische Ausland-Fernmeldeaufklärung ist ein unverzichtbares Instrument zur Erfüllung des gesetzlichen Auftrags des Bundesnachrichtendienstes. Ihre erhebliche Bedeutung für den Bundesnachrichtendienst ergibt sich insbesondere aus der Tatsache, dass diese Aufkommensart aktuelle und unverfälschte Erkenntnisse in Echtzeit zu liefern vermag. Weil ihre Sensorik rein technisch aktiviert werden kann, können mit der strategischen Ausland-Fernmeldeaufklärung zudem vielfach aus dem Stand heraus Informationen zu neu in den Aufgabenfokus rückenden Themen oder Regionen geliefert werden. Die Werbung und Entwicklung menschlicher Quellen benötigt demgegenüber aus methodischen Gründen in der Regel längere Vorlaufzeiten, bis erste lagerelevante Informationen gewonnen werden. Zudem liefert die strategische Ausland-Fernmeldeaufklärung insofern authentische Erkenntnisse, als feststeht, dass die agierenden Personen die aus ihren Telekommunikationsverkehren erfassten Informationen auch tatsächlich so untereinander übermittelt haben. Bei Informationen menschlicher Quellen, aber gegebenenfalls auch bei Informationen ausländischer Nachrichtendienste, ist nicht auszuschließen, dass der Informationsgehalt durch den Informationsgeber – bewusst oder unbewusst – verändert bzw. verfälscht wurde. Im Übrigen zeichnet sich die strategische Ausland-Fernmeldeaufklärung dadurch aus, dass beim Einsatz dieser Art der Informationsgewinnung eigene Mitarbeiter oder Quellen des Bundesnachrichtendienstes weitaus weniger dem – nicht selten lebensgefährlichen – Zugriff ausländischer Abwehrbehörden ausgesetzt werden müssen als dies beispielsweise beim Einsatz menschlicher Quellen gegen besonders streng abgeschottete Aufklärungsobjekte in fremden Staaten oder gegen terroristische bzw. extremistische Gruppierungen der Fall ist. Die strategische Ausland-Fernmeldeaufklärung gehört deshalb zum unverzichtbaren Methodenspektrum für eine erfolgreiche Aufgabenerfüllung des Bundesnachrichtendienstes.

Eine Befugnis zur Ausland-Fernmeldeaufklärung ist mit dem Grundrecht aus Artikel 10 Absatz 1 GG grundsätzlich vereinbar. So hat das Bundesverfassungsgericht in seinem Urteil vom 19. Mai 2020 (BVerfG, a.a.O., Randnummer 143 ff.) ausdrücklich hervorgehoben, dass die Einräumung einer Befugnis zur Auslandsaufklärung im Wege der strategischen Fernmeldeaufklärung durch Artikel 10 Absatz 1 GG nicht ausgeschlossen ist, sondern vielmehr durch das Ziel der Auslandsaufklärung und deren besondere Handlungsbedingungen bei hinreichend begrenzter Ausgestaltung vor Artikel 10 Absatz 1 GG und dem Verhältnismäßigkeitsgrundsatz gerechtfertigt werden kann. Insofern stellt die frühzeitige Erkennung von Gefahren, die Wahrung der Handlungsfähigkeit der Bundesrepublik und die Versorgung der Bundesregierung mit Informationen zu außen- und sicherheitspolitischen Fragen nach Auffassung des Bundesverfassungsgerichts ein legitimes Ziel der strategischen Telekommunikationsüberwachung dar (BVerfG, a.a.O.,

Randnummer 144). Die strategische Telekommunikationsüberwachung sei hierfür auch ein geeignetes Mittel, da sie es ermögliche, an solche Informationen zu gelangen. Dass hierbei in großem Umfang zunächst Daten miterfasst werden, die keinen relevanten Informationsgehalt haben, ändere nichts daran, dass die Erfassung und Auswertung von Datenströmen im Ergebnis zu bedeutsamen Erkenntnissen führen könne. Gleichfalls genüge die strategische Überwachung den Anforderungen der Erforderlichkeit. Ohne die breit angelegte anlasslose Erfassung von Datenströmen und deren Auswertung könnten entsprechende Informationen nicht gewonnen werden. Ein weniger eingriffsintensives Mittel, das generell vergleichbare Informationen sicherstellte, sei nicht ersichtlich. Auch im Hinblick auf die Verhältnismäßigkeit im engeren Sinne könne eine strategische Ausland-Fernmeldeaufklärung der Kommunikation von Ausländern im Ausland vor Artikel 10 Absatz 1 GG gerechtfertigt werden (BVerfG, a.a.O., Randnummer 145). Zwar handelt es sich bei ihr nach der Auffassung des Gerichts um ein Instrument von besonders schwerem Eingriffsgewicht. Gegenüber Ausländern im Ausland ist das Eingriffsgewicht jedoch dahingehend gemindert, dass eine Überwachung nicht stets in gleicher Weise auf unmittelbar operative Konsequenzen gerichtet ist wie in der Regel Überwachungsmaßnahmen gegenüber Deutschen oder im Inland befindlichen Personen, da der deutsche Staat dort nicht über Hoheitsbefugnisse verfügt und der Bundesnachrichtendienst auch grundsätzlich keine eigenen operativen Befugnisse hat (BVerfG, a.a.O., Randnummer 149). Überdies bestätigt das Gericht das überragende öffentliche Interesse an einer wirksamen Auslandsaufklärung (BVerfG, a.a.O., Randnummer 161).

Zu Absatz 1

Absatz 1 bildet die zentrale Norm der strategischen Ausland-Fernmeldeaufklärung. Hiernach darf der Bundesnachrichtendienst zur Erfüllung seiner Aufgaben mit technischen Mitteln personenbezogene Daten von Ausländern im Ausland auf der Grundlage zuvor angeordneter strategischer Aufklärungsmaßnahmen verarbeiten. Diese Legaldefinition der strategischen Ausland-Fernmeldeaufklärung konkretisiert einerseits den gesetzlichen Aufklärungsauftrag des § 1 Absatz 2. Andererseits grenzt sie durch den Bezug zu technischen Mitteln die strategische Ausland-Fernmeldeaufklärung von anderen nachrichtendienstlichen Informationsquellen ab, insbesondere von der Aufklärung mittels menschlicher Quellen. Die Norm regelt die Erhebung von personenbezogenen Daten in Abgrenzung zu reinen Sachdaten, die mangels Grundrechtsrelevanz keiner Regelung bedürfen und stellt klar, dass es sich um personenbezogene Daten von Ausländern im Ausland handeln muss. Deutsche und Inländer sind folglich nicht erfasst vom Regelungsgehalt der Norm. Damit wird eine klare Trennung von der Fernmeldeaufklärung nach dem Artikel 10-Gesetz sichergestellt.

Von § 19 erfasst ist nur die Erhebung personenbezogener Inhaltsdaten. Unter Inhaltsdaten sind Inhalte einer Individual-Kommunikation zu verstehen. Von der Norm nicht erfasst ist die Erfassung personenbezogener Metadaten im Rahmen einer strategischen Aufklärungsmaßnahme. Metadaten sind alle über die Inhaltsdaten hinausgehenden Daten. Dies sind zum Beispiel technische und fernmeldebetriebliche Informationen, die die Umstände einer Telekommunikation, den technischen Übertragungsweg oder auch die Bereitstellung der technischen Mittel einer Übertragung ohne willentliches Zutun des Nutzers beschreiben. Als Metadaten werden beispielsweise Daten bezeichnet, die den Aufbau und die Benutzung anderer Daten beschreiben, oder Daten über Daten, wie Datentyp, Bedeutung, Beziehungen zwischen Entitätstypen, Integritätsbedingungen, Verdichtungsregeln. Verkehrsdaten sind solche Metadaten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (vgl. § 3 Nr. 30 TKG). Die Verarbeitung von personenbezogenen Verkehrs- und

sonstigen Metadaten richtet sich nach den speziellen Vorgaben des § 26. Auf die dortigen Ausführungen wird verwiesen.

Die Datenerhebung gemäß § 19 darf nur auf Grundlage zuvor von der Leitung des Bundesnachrichtendienstes angeordneter strategischer Aufklärungsmaßnahmen erfolgen. Die Rechtmäßigkeit der Anordnung wird vor deren Vollzug durch den Unabhängigen Kontrollrat geprüft (vgl. § 23 Absatz 1).

Im Weiteren differenziert Absatz 1 zwischen zwei zentralen Erhebungszwecken. Die Erhebung ist möglich zum Zweck der politischen Unterrichtung der Bundesregierung (Nummer 1) oder zum Zweck der Früherkennung von aus dem Ausland drohenden Gefahren von internationaler Bedeutung (Nummer 2). Dass eine an diesen Zwecken ausgerichtete strategische Fernmeldeaufklärung mit dem Grundgesetz vereinbar ist, hat das Bundesverfassungsgericht ausdrücklich festgestellt (BVerfG, a.a.O., Randnummer 157).

Zu Absatz 2

Absatz 2 definiert den Begriff der strategischen Aufklärungsmaßnahme und deren Inhalt.

Zu Absatz 3

Nach Absatz 3 sind strategische Aufklärungsmaßnahmen nach Absatz 1 Nummer 1 nur zulässig, wenn sie der Gewinnung von Informationen dienen, mit deren Aufklärung das Bundeskanzleramt den Bundesnachrichtendienst beauftragt hat. Mit dieser Norm wird sichergestellt, dass Aufklärungsmaßnahmen nach Absatz 1 Nummer 1 in Einklang mit dem sogenannten Auftragsprofil der Bundesregierung (APB), welches das Bundeskanzleramt im Einvernehmen mit den zuständigen Bundesministerien festlegt, und anderen Weisungen des Bundeskanzleramtes, die den gesetzlichen Auftrag des Bundesnachrichtendienstes konkretisieren, stehen. Durch das APB legt die Bundesregierung die Prioritäten fest, anhand derer der Bundesnachrichtendienst gemäß seinem gesetzlichen Auftrag Erkenntnisse von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland zu beschaffen hat.

Zu Absatz 4

Absatz 4 konkretisiert die Früherkennung von aus dem Ausland drohenden Gefahren von internationaler Bedeutung nach Absatz 1 Nummer 2. Strategische Aufklärungsmaßnahmen nach Absatz 1 Nummer 2 sind nur zulässig, wenn zusätzlich zu den Voraussetzungen des Absatzes 3 tatsächliche Anhaltspunkte dafür vorliegen, dass durch sie Erkenntnisse über aus dem Ausland drohenden Gefahren von internationaler Bedeutung gewonnen werden können. Satz 2 definiert den Gefahrenbegriff im nachrichtendienstlichen Sinne. Über den polizeilichen Gefahrenbegriff hinaus umfasst dieser gerade auch die Früherkennung von Entwicklungen im Ausland, die sich negativ auf die Stellung der Bundesrepublik Deutschland in der Staatengemeinschaft auswirken können. Dies kann beispielsweise bei politischen krisenhaften Entwicklungen im Ausland der Fall sein, von denen die Bundesrepublik Deutschland betroffen ist. Eine krisenhafte Entwicklung in diesem Sinne wäre zum Beispiel die Zuspitzung einer politischen Krise in der Peripherie Europas oder das Aufflammen bewaffneter Konflikte zwischen den Anrainerstaaten einer wichtigen maritimen Handelsroute. Eine Gefahr von internationaler Bedeutung in diesem Sinne liegt vor, wenn sie einen Bezug zu den in Nummer 1 aufgezählten Phänomenbereichen aufweist oder die in Nummer 2 und 3 genannten

Rechtsgüter bedroht. Ein solcher Bezug kann sich auch mittelbar daraus ergeben, dass Informationen mittels der strategischen Fernmeldeaufklärung beschafft werden müssen, um hierdurch in die Lage versetzt zu werden, die Früherkennung der jeweiligen Gefahr durchzuführen. Beispielhaft kann hier die Aufklärung einer im terroristischen Umfeld befindlichen Person genannt werden, um auf diese Weise Erkenntnisse zu erlangen, die eine Anbahnung als nachrichtendienstliche Quelle ermöglichen.

Nummer 1

Gefahren müssen im Einklang mit den von der Bundesregierung vorgegebenen Aufklärungsaufträgen des Bundesnachrichtendienstes einen Bezug zu den nachfolgend genannten Phänomenbereichen aufweisen, um eine strategische Aufklärungsmaßnahme begründen zu können.

Buchstabe a)

Unter die Landes- und Bündnisverteidigung fallen einerseits nationale Verteidigungsinteressen der Bundesrepublik Deutschland und andererseits Bündnisverpflichtungen in internationalen Bündnissen, an denen die Bundesrepublik Deutschland beteiligt ist, darunter insbesondere die der NATO.

Strategische Aufklärungsmaßnahmen im Rahmen der Landes- und Bündnisverteidigung kommen unter anderem bei sich entwickelnden Gefährdungen der territorialen Integrität Deutschlands sowie eines Bündnispartners, bei zwischenstaatlichen Konflikten, bei fragiler Staatlichkeit und schlechter Regierungsführung, bei weltweiter Aufrüstung, bei Gefährdung der Informations-, Kommunikations-, Transport und Handelslinien, der Sicherheit der Rohstoff- und Energieversorgung sowie bei der Abwehr von Gefahren aus dem Cyber- und Informationsraum zum Tragen. Auch Aufklärungsmaßnahmen fremder Staaten und insbesondere von deren Nachrichtendiensten, die ihrerseits die Maßnahmen der Bundesrepublik Deutschland und ihrer internationalen Bündnispartner aufzuklären versuchen, um anhand der gewonnenen Erkenntnisse Strategien zur Schwächung und bzw. oder Umgehung der vorgenannten Verteidigungsinteressen entwickeln zu können, sind Bestandteil entsprechender strategischer Aufklärungsmaßnahmen.

Eine vergleichbare Interessenlage liegt bei Auslandseinsätzen der Bundeswehr oder verbündeter Streitkräfte im Ausland vor, z. B. bei humanitären Einsätzen. Die Bundeswehr ist an einer Vielzahl von Auslandseinsätzen beteiligt und leistet damit einen wertvollen Beitrag zur weltweiten Sicherheit und Stabilität. Der Bundesnachrichtendienst ist als einziger Auslandsnachrichtendienst der Bundesrepublik Deutschland auch zuständig für die militärische Auslandsaufklärung. Durch strategische Aufklärungsmaßnahmen kann er beispielsweise Erkenntnisse unmittelbar zur Sicherheitslage und zu besonderen, situativ verschärften Gefährdung der gesundheitlichen Versorgung vor Ort und der Peripherie des Einsatzlandes gewinnen und trägt damit zur Sicherheit der eingesetzten deutschen Soldatinnen und Soldaten bei. So werden einflussreiche Personen in den Einsatzländern erfahrungsgemäß - auch über ihren Zuständigkeitsbereich hinaus - über sicherheitsrelevante Ereignisse informiert, wenn sich Betroffene davon Hilfe und Unterstützung erhoffen. Besonders nützlich ist die Erhebung von internen Kommunikationsverkehren von Militär und Sicherheitsbehörden. Lagerelevante Informationen werden regelmäßig sehr zeitnah an Vorgesetzte weitergegeben. Im Gegensatz zu offiziellen Mitteilungen, in denen Gefahren häufig verharmlost und die eigenen Erfolge in den Vordergrund gestellt werden, erlauben die durch strategische Aufklärungsmaßnahmen gewonnenen Informationen einen weitgehend unverfälschten Einblick in die tatsächliche Einsatzbereitschaft und die Leistungsfähigkeit der Sicherheitskräfte sowie deren Operationsführung bzw. Vorgehen. Strategische Aufklärungsmaßnahmen sind häufig die Hauptinformationsquelle zum Schutz deutscher

Soldatinnen und Soldaten im Auslandseinsatz. Zu deren Schutz ist vor allem auch die Gewinnung von Erkenntnissen zu Techniken, Taktiken und Vorgehensweisen militanter Gruppierungen, die auch gegen die Einsatzkräfte der Bundeswehr agieren, erforderlich. Die Sicherstellung des Schutzes der Soldatinnen und Soldaten im Rahmen der sogenannten Force Protection durch Gewinnung nachrichtendienstlicher Erkenntnisse über das jeweilige Einsatzland ist eine der wesentlichen Aufgaben des Bundesnachrichtendienstes. Ein weiterer Aspekt zum Schutz von Leib und Leben der im Auslandseinsatz befindlichen Soldaten und Soldatinnen ist auch die Aufklärung der Fähigkeiten, Leistungs- und Einsatzbereitschaft der Sanitätsdienste fremder Streitkräfte. Dieser Faktor ist für die Sicherheits- und Bedrohungslage im Einsatzgebiet maßgeblich. Hier steht zum einen die eigene medizinische Versorgung im Vordergrund. Zum anderen gehört aber auch die wehrmedizinische Forschung staatlicher und nichtstaatlicher Akteure in Russland und in China, zu den Zielen von Aufklärungsmaßnahmen der Strategischen Fernmeldeaufklärung.

Auch der Schutz von Auslandseinsätzen anderer deutscher Behörden, zum Beispiel zum Schutz polizeilicher Einsätze im Ausland, ist eine wesentliche Aufgaben des Bundesnachrichtendienstes und diesem auch mit Mitteln der strategischen Ausland-Fernmeldeaufklärung gestattet. Ferner übermittelt der Bundesnachrichtendienst sicherheitsrelevante Erkenntnisse zur Unterstützung der deutschen Entwicklungshilfe im Ausland, die in der Regel nur aufgrund einer Vereinbarung mit dem Einsatzland erfolgen kann. Entsprechende Einsätze finden häufig weitab der Hauptstädte in Gebieten mit besonderen Sicherheitsrisiken statt. Auch hier liefern oftmals allein die durch die strategischen Aufklärungsmaßnahmen gewonnenen Erkenntnisse ein wirklich zutreffendes und hinreichend aktuelles Bild der Sicherheitslage vor Ort, das erforderlich ist, um deutsche Entwicklungshelfer keinen unnötigen Gefahren auszusetzen bzw. notfalls sogar Evakuierungen zu ermöglichen.

Buchstabe b)

Krisenhafte Entwicklungen im Ausland können rasch zu einer Destabilisierung von Ländern oder sogar ganzen Regionen führen, weshalb sie von besonderer Relevanz für die Auftragserfüllung des Bundesnachrichtendienstes sind. Das internationale System verändert sich kontinuierlich. Multipolarität und geopolitische Machtverschiebungen sind u.a. das Resultat aus dem wachsenden politischen, wirtschaftlichen und militärischen Einfluss von Schlüsselstaaten. Die damit einhergehenden dynamischen Prozesse sind hinsichtlich der Sicherheitsinteressen Deutschlands und seiner Verbündeten insbesondere vor dem Hintergrund deren langfristigen Folgewirkungen mit krisenhaftem Entwicklungspotential, wechselseitigen Verstärkungen und Interdependenzen ein besonderes Aufklärungsziel.

Der Bundesnachrichtendienst gewinnt durch strategische Aufklärungsmaßnahmen Erkenntnisse über sich zum Teil schnell zuspitzende politische Spannungen, beispielsweise aufgrund strategischer Absichten einer dominierenden militanten Opposition, über soziale Unruhen und/oder bewaffnete Auseinandersetzungen, die zu einer Änderung der politischen, gesellschaftlichen, wirtschaftlichen oder militärischen (Kräfte-)Verhältnisse führen können und daher zur Gefahr für deutsche oder europäische Einrichtungen, Staatsbürger sowie Interessen werden.

Weiterhin kann der Bundesnachrichtendienst durch strategische Aufklärungsmaßnahmen Erkenntnisse über potentiell grenzüberschreitende Entwicklungen (Chemieunfälle, Krankheitsausbrüche, etc.) erlangen, deren Existenz oder Ausmaß nationale Regierungen unter Umständen nicht oder nur zögerlich einräumen. Dies kann auch zivile oder militärische Auseinandersetzungen zwischen zwei Staaten betreffen. Nur in Kenntnis solcher Lagen kann die Bundesregierung rechtzeitig Maßnahmen zum Schutz deutscher Staatsbürger im Ausland bzw. – je nach Reichweite

des Ereignisses – der Bevölkerung in Deutschland ergreifen (z.B. Warn- und Reisehinweise, Evakuierungen oder Ausgabe von Medikamenten).

Darüber hinaus gewinnt der Bundesnachrichtendienst durch strategische Aufklärungsmaßnahmen auch Erkenntnisse über Entwicklungen, deren Fortgang schwerste Verbrechen, die die internationale Gemeinschaft als Ganzes berühren (Völkermord, Verbrechen gegen die Menschlichkeit, Kriegsverbrechen), erwarten lassen. So entzündeten sich Konflikte im Rahmen von Wahlkämpfen, Kämpfen um Ressourcen (Weideland, Zugang zu Wasser, zu staatlichen Geldern etc.) oder Kämpfen um größere Autonomie oft entlang ethnischer oder religiöser Zugehörigkeiten, was zu ethnischen Vertreibungen, bewaffneten Angriffen auf die Zivilbevölkerung etc. führen kann. Die Verhinderung solcher Verbrechen durch das Ergreifen von Gegenmaßnahmen liegt im Interesse der Bundesrepublik Deutschland sowie der internationalen Staatengemeinschaft. Auf Basis der Übermittlung von Erkenntnissen zu derartigen Entwicklungen und den involvierten Akteuren kann die Bundesrepublik Deutschland auf diplomatischem, politischem und wirtschaftlichem Wege Einfluss auf die Konfliktparteien nehmen. Zudem kann sie ihre Mitgliedschaft in internationalen Organisationen nutzen, um über die nationale Ebene hinaus einzuwirken.

Durch strategische Aufklärungsmaßnahmen gewinnt der Bundesnachrichtendienst ferner Erkenntnisse über die Auswirkungen krisenhafter Entwicklungen im Ausland, insbesondere auch über krisenbedingte illegale Migrationsbewegungen in Richtung der Bundesrepublik Deutschland bzw. von Staaten der Europäischen Union, soweit diese nicht in organisierten kriminellen Strukturen (vgl. hierzu Buchstabe e)) erfolgt.

Krisenhafte Entwicklungen im Ausland können sich auf die Bundesrepublik Deutschland auch in dem Zusammenhang auswirken, dass die Bundesrepublik Deutschland als rohstoffarmes Land mehr als andere Länder auf den freien grenzüberschreitenden Handel mit Energie und Rohstoffen angewiesen ist. Beeinträchtigungen in diesem Bereich in Form von Lieferengpässen oder -ausfällen haben erhebliche Folgen für die Bevölkerung und die deutsche Volkswirtschaft. Teilweise setzen staatliche Akteure die Zurückhaltung von Rohstoffexporten gezielt als politisches Druckmittel gegen andere Länder ein. Die Aufklärung solcher Beeinträchtigungen ist für die Auftragserfüllung des Bundesnachrichtendienstes von herausragender Bedeutung, da die Bundesrepublik z.B. Rohöl für deutsche Raffinerien oder Erdgas in erheblichem Umfang aus dem Ausland bezieht, teilweise über Pipelines, die ihrerseits durch mehrere Länder verlegt sind. Einseitige Maßnahmen der Lieferstaaten oder Auseinandersetzungen zwischen Liefer- und Transitstaaten können die Energieversorgung der Bundesrepublik gefährden. Bei rechtzeitiger Warnung hätte die Bundesregierung beispielsweise die Möglichkeit, diplomatisch aktiv zu werden und vermittelnd einzugreifen bzw. Maßnahmen zur Aufrechterhaltung der Energieversorgung einzuleiten.

Buchstabe c)

Buchstabe c) erfasst den Phänomenbereich des internationalen Terrorismus und Extremismus, der entweder durch Gewaltbereitschaft charakterisiert wird, oder auf die planvoll verborgen betriebene Durchsetzung politischer, religiöser oder ideologischer Ansichten ausgerichtet ist. Die Bedrohungslage durch den internationalen gewaltbereiten Terrorismus durch Terrororganisationen ist unverändert hoch.

Gewalttätige und extremistisch ausgerichtete Organisationen haben Verbindungen nach Deutschland und Europa und betreiben von dort aus anschlagsvorbereitenden Maßnahmen der Finanzierung und Rekrutierung. Dabei erfolgt auch eine Nutzung europäischer Staaten als Flucht- und Ruheraum für Mitglieder der Organisationen.

Darüber hinaus hat der gewaltbereite, international vernetzte Extremismus an Gefährdungspotential gewonnen. Gerade auch im Bereich des gewaltbereiten Rechtsextremismus bieten insbesondere soziale Netzwerke Möglichkeiten zum

Austausch bzw. zur Kooperation mit entsprechenden Gruppierungen im Ausland. Hieraus erwächst die Gefahr, dass sich Radikalisierungen vollziehen. Transnationale Netzwerke verfolgen das Ziel einer weltweiten Durchsetzung ihres extremistischen Gedankengutes. Nicht in allen Fällen wird hierzu auf das Mittel der Gewalt gesetzt. Die Netzwerke sind bestrebt, auch in Deutschland Grundwerte der freiheitlichen Demokratie zu beseitigen. Angesichts der von Extremisten genutzten modernen Kommunikationsmittel bildet die strategische Ausland-Fernmeldeaufklärung einen ganz wesentlichen und unabdingbaren Bestandteil bei der Aufklärung und Identifizierung solcher Personennetzwerke und somit der Erkennung von Bedrohungen für die Sicherheit der Bundesrepublik Deutschland.

Buchstabe d)

Buchstabe d) betrifft Cyberangriffe von erheblicher Bedeutung. In diesem Phänomenbereich agiert eine Vielzahl von Akteuren aus dem kriminellen oder terroristischen Milieu. Auch gezielt gesteuerte Angriffe von staatlicher Seite sind nicht auszuschließen. Darüber hinaus werden organisierte Cyberangriffe auch zur gezielten Destabilisierung relevanter Infrastrukturen durchgeführt (sogenannter „Hacktivismus“). Ziele können dabei nicht nur die IT-Systeme staatlicher Stellen sein, sondern auch IT-Systeme von Unternehmen, die zum Zweck der Erzielung von Wettbewerbsvorteilen (Wirtschaftsspionage) angegriffen werden. Die Risiken von Cyberangriffen gewinnen in einer immer enger digital vernetzten Gesellschaft weiter an Bedeutung, weshalb der Früherkennung von Cyber-Gefahren ebenfalls wachsende Bedeutung zukommt. Cyber-Angriffe terroristischer Gruppen und staatlicher Akteure – einschließlich fremder Nachrichtendienste – können auch die Störung oder Zerstörung kritischer, ziviler Infrastruktur zum Ziel haben, um die sich gegebenenfalls daraus ergebende destabilisierende Wirkung für eigene Zwecke nutzen zu können.

Durch die Begrenzung auf internationale Fälle scheiden Sachverhalte mit rein regionalem Bezug und eingeschränkter Bedeutung als Aufklärungsziele für die strategische Ausland-Fernmeldeaufklärung aus.

Buchstabe e)

Organisierte Kriminalität ist die von Gewinn- oder Machtstreben bestimmte, planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, und bei der mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken.

Die Bedrohungslage durch die internationale organisierte Kriminalität ist insbesondere in ihrer Ausprägung durch den internationalen Rauschgifthandel unverändert hoch. Rauschgiftkriminalität ist seit Jahren das Hauptbetätigungsfeld von Organisierter Kriminalität in Deutschland. Konspirativ agierende kriminelle Organisationen bedienen sich dabei eng verzweigter, internationaler Transport- und Logistikwege. Typischerweise stellen Erpressungs- und Tötungsdelikte, Eigentumskriminalität sowie Waffenhandel/-schmuggel Nebenaktivitäten im Bereich der Rauschgiftkriminalität dar.

Darüber hinaus ist die Aufklärung von internationalen Geldwäscheaktivitäten für die Auftragserfüllung des Bundesnachrichtendienstes von herausragender Bedeutung, da legal einsetzbare Gewinne eine wichtige Voraussetzung für das Handeln organisierter krimineller Strukturen darstellen. Ohne Aussicht auf diese, beispielsweise zum Erwerb von Luxusgütern, müssten die kriminellen Strukturen komplett in ihrem eigenen Milieu verbleiben. Zudem erlauben legalisierte Gelder den Aufbau wirtschaftlichen und politischen Einflusses. Gefahren für die Bundesrepublik Deutschland gehen dabei sowohl von nationalen kriminellen Strukturen, die internationale Geldwäschestrukturen

zur Legalisierung ihrer inkriminierten Gelder nutzen, als auch von internationalen Akteuren aus. Durch die strategische Fernmeldeaufklärung erlangt der Bundesnachrichtendienst insbesondere Erkenntnisse über die klandestinen Methoden der entsprechenden Akteure betreffend die Einschleusung inkriminierter Gelder in den legalen Wirtschaftskreislauf.

Fest verankert in der internationalen organisierten Kriminalität ist ferner der Menschenhandel. Der Begriff des „Menschenhandels“ bezeichnet die Anwerbung, Beförderung, Verbringung, Beherbergung oder Aufnahme von Personen durch die Androhung oder Anwendung von Gewalt oder anderen Formen der Nötigung, durch Entführung, Betrug, Täuschung, Missbrauch von Macht oder Ausnutzung besonderer Hilflosigkeit oder durch Gewährung oder Entgegennahme von Zahlungen oder Vorteilen zur Erlangung des Einverständnisses einer Person, die Gewalt über eine andere Person hat, zum Zweck der Ausbeutung. Ausbeutung umfasst mindestens die Ausnutzung der Prostitution anderer oder andere Formen sexueller Ausbeutung, Zwangsarbeit oder Zwangsdienstbarkeit, Sklaverei oder sklavereiähnliche Praktiken, Leibeigenschaft oder die Entnahme von Organen. Insbesondere illegale Migranten geraten in die Fänge von Menschenhändler-Strukturen. Dies führt regelmäßig zu Zwangsprostitution und zu sonstiger Zwangs-/Schwarzarbeit, woraus auch Gefahren für Gesundheit, Leib und Leben dieser Personen erwachsen. Durch die strategische Ausland-Fernmeldeaufklärung erlangt der Bundesnachrichtendienst insbesondere Erkenntnisse zu relevanten Personen/Personenzusammenschlüsse und deren Modi Operandi. Die Aufklärung dieses Phänomenbereichs ist für die Auftragserfüllung des Bundesnachrichtendienstes daher ebenfalls von herausragender Bedeutung.

Darüber hinaus unterfällt die illegale Migration regelmäßig dem Phänomenbereich der organisierten Kriminalität. Illegale Migration bezeichnet die Einreise nach und den Aufenthalt in Staaten unter Verstoß gegen die dort geltenden gesetzlichen Bestimmungen. Sie ist regelmäßig nur unter Zuhilfenahme krimineller Strukturen (Schleuser, Dokumentenfälscher, Menschenhändler etc.) möglich. Für die kriminellen Akteure steht dabei die Profitmaximierung im Vordergrund. Für die illegalen Migranten ist der Weg nach Deutschland dagegen mit erheblichen Gefahren für Leib und Leben verbunden. Lukrativstes Geschäft für die internationale organisierte Kriminalität ist in diesem Zusammenhang die Ausbeutung illegal migrierter Arbeitskräfte in vielfältiger Form („Abarbeiten“ von Vermittlungsgebühren oder vorgestreckter Reisekosten, Vorenthalten von Arbeitslohn etc.). Illegale Migrationsbewegungen können zudem die Grenzsicherheit und damit die Ausübung staatlicher Souveränitätsrechte entlang der EU-Außengrenze gefährden. Durch die strategische Ausland-Fernmeldeaufklärung erlangt der Bundesnachrichtendienst insbesondere Erkenntnisse zu relevanten Personen und Personenzusammenschlüssen sowie die jeweiligen Modi Operandi. Nur auf der Basis aktueller Lagebilder können illegale Migrationsbewegungen antizipiert bzw. nachvollzogen werden.

Buchstabe f)

Die illegale Weiterverbreitung von Kriegswaffen sowie von Waren und technischen Unterstützungsleistungen mit ziviler und militärischer Verwendung in Fällen von erheblicher Bedeutung) nach Nummer 6 trägt zur Destabilisierung von Staaten und ganzen Regionen bei und begünstigt die Entstehung neuer Krisen- und Konfliktlagen. Die Umsetzung des Kriegswaffenkontrollgesetzes dient der Friedenssicherung und Kriegsverhütung. Die Aufklärung von Proliferation von Kriegswaffen in diesem Sinne soll friedensstörende Handlungen verhindern, das friedliche Zusammenleben der Völker schützen sowie die Gefahren für den Völkerfrieden und die internationale Sicherheit abwehren. Artikel 26 Absatz 2 GG normiert zu diesem Zweck, dass Kriegswaffen nur mit Genehmigung der Bundesregierung hergestellt, befördert und in den Verkehr gebracht

werden dürfen. Neben den Kriegswaffen stehen auch Rüstungsgüter im Fokus der Aufklärung, um eine destabilisierende Anhäufung konventioneller Rüstungsgüter in Krisenregionen oder einen Missbrauch zur internen Repression zu verhindern.

Der Bundesnachrichtendienst betrachtet neben der illegalen Verbreitung von Kriegswaffen auch legale Geschäfte mit Kriegswaffen in Staaten, in denen der Erwerb zur Destabilisierung anderer Länder oder Regionen beitragen kann oder wenn zu befürchten ist, dass Waffen im Empfängerstaat zwar legal erworben werden, jedoch aufgrund der dortigen Strukturen die Gefahr der Weitergabe der Waffen an Akteure besteht, von denen internationales Gefährdungspotential ausgeht. Eine solche Situation kann insbesondere in Staaten eintreten, die im Auftragsprofil der Bundesregierung als durch den Bundesnachrichtendienst priorisiert aufzuklären deklariert wurden.

Umfasst von der Regelung nach Buchstabe f) ist darüber hinaus aufgrund des besonderen Gefährdungspotentials auch die Aufklärung von Programmen nuklearer, biologischer und chemischer Waffen und ihrer Trägersysteme sowie deren Weiterverbreitung. Da in diesem Bereich regelmäßig unter Einsatz erheblicher Verschleierungsbemühungen agiert wird, werden auch Vor- und Umfeldaktivitäten wie Zulieferungen zu solchen Programmen aufgeklärt. Dies gilt auch dann, wenn noch keine konkrete Proliferationsabsicht nachweisbar ist.

Die Aufklärung solcher Programme für und Proliferation von Massenvernichtungswaffen ist für die Auftragserfüllung des Bundesnachrichtendienstes von herausragender Bedeutung. Ziel ist es, eine Bedrohung Deutschlands oder seiner Bündnispartner durch Massenvernichtungswaffen zu verhindern. Zur Erreichung dieses außen- und sicherheitspolitischen Ziels richtet sich die Aufklärung vorrangig gegen Länder, die sich um Massenvernichtungswaffen bemühen. Daneben können auch nicht-staatliche Akteure im Fokus stehen. Die Proliferation strategischer Güter in solche ABC-Programme und Trägersysteme wird oft durch Tarnfirmen, Zwischenhändler und gezielt komplizierte Handels(um)wege und entsprechend verschleierter Finanzströme ermöglicht.

Auch die Aufklärung des unerlaubten Außenwirtschaftsverkehrs mit Waren und technischen Unterstützungsleistungen ist wesentliche Aufgabe des Bundesnachrichtendienstes, dies umfasst auch den Verkehr mit sog. Dual-Use-Gütern. Erfasst sind nur Sachverhalte von erheblicher Bedeutung, die Aufklärung rein regionale Sachverhalte mit beschränktem Risikopotential ist durch Maßnahmen der strategischen Ausland-Fernmeldeaufklärung nicht möglich.

Buchstabe g)

Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Zu den Kritischen Infrastrukturen zählen also alle für die Funktionsfähigkeit der Gesellschaft bedeutsamen Basisdienste. Auf die Bestimmungen der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) wird verwiesen. Unter hybriden Bedrohungen versteht man die interessensgeleitete Einflussnahme auf Staaten oder Staatenverbünde, insbesondere zentrale Akteure, deren Netzwerke und die von ihnen genutzten Instrumente. Ziel ist die Störung des gesamtgesellschaftlichen und politischen Gefüges eines Staates durch die Anwendung konventioneller und nicht konventioneller Mittel unter gezielter Verschleierung der eigenen Urheberchaft.

Buchstabe h)

Unter hybriden Bedrohungen versteht man die interessensgeleitete Einflussnahme auf Staaten oder Staatenverbünde, insbesondere zentrale Akteure, deren Netzwerke und

die von ihnen genutzten Instrumente. 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.

Der Schutz vor hybriden Bedrohungen ist für die Auftragserfüllung des Bundesnachrichtendienstes von herausragender Bedeutung, da eine in der Folge der Beeinträchtigung möglicherweise einsetzende Destabilisierung der Gesellschaft von anderen Staaten – unabhängig davon, ob sie diese Beeinträchtigung selbst herbeigeführt haben oder nicht – für eigene, insbesondere machtpolitische Zwecke genutzt werden kann. Diese können auf einen Sturz der aktuellen Regierung (mit dem Ziel, eine neue besser kontrollieren zu können) ausgerichtet sein oder auch im Zusammenhang mit der Vorbereitung eines Angriffskrieges stehen, in dem Risiken und eigener Kräfteinsatz durch vorbereitende Maßnahmen reduziert werden.

Nummer 2 und 3

Strategische Aufklärungsmaßnahmen des Bundesnachrichtendienstes sind ferner dann zulässig, wenn durch sie im Einklang mit den von der Bundesregierung vorgegebenen Aufklärungsaufträgen Erkenntnisse zum Schutz der nachfolgend genannten Rechtsgüter gewonnen werden können.

Nummer 2, Buchstabe a)

Buchstabe a) betrifft Gefährdungen von Leib, Leben oder Freiheit einer natürlichen Person. Die Regelung ist nicht auf eine Gefährdung deutscher Staatsangehöriger begrenzt. Der Schutz von Leib, Leben und Freiheit natürlicher Personen muss vordringlichste Aufgabe aller staatlichen Stellen sein. Eine Gefahr für Leib, Leben oder Freiheit ist insbesondere bei Entführungsfällen gegeben. Hier können Erkenntnisse, die aus der strategischen Ausland-Fernmeldeaufklärung – z.B. aus der Telekommunikation von Beteiligten oder Mittelsmännern – gewonnen werden, zusammen mit dem Erkenntnisaustausch mit anderen Nachrichtendiensten und deren Unterstützung durch eigene nachrichtendienstliche Zugänge ganz wesentlich zur Lösung solcher Fälle und damit zur unmittelbaren Rettung von Menschenleben beitragen.

Nummer 2, Buchstabe b)

Buchstabe b) umfasst den Bestand oder die Sicherheit des Bundes oder eines Landes. Dies betrifft beispielsweise die Funktionsfähigkeit staatlicher Einrichtungen, deren Beeinträchtigung die Sicherheit des Bundes oder im Extremfall sogar seinen Bestand bedrohen würde.

Ziel der Aufklärungsmaßnahmen des Bundesnachrichtendienstes mittels der strategischen Ausland-Fernmeldeaufklärung sind auch wehrtechnische Technologien und dazugehörige Programme sowie aufkommende und disruptive Technologien, soweit diese nicht bereits in Nummer 1 f) erfasst sind. Zum Schutz des Bestands oder der Sicherheit des Bundes und eines Landes gehört auch das Beobachten (wehr-)technischer Forschung und Entwicklung auf dem Gebiet neuartiger Waffentechnik und nicht-letaler Systemtechnik, die zur Förderung hybrider Bedrohungen genutzt werden kann. Ferner ist die Entwicklung fundamental bedeutsamer Technologien, die gegebenenfalls zur Verschiebung von staatlichen Machtgefügen oder Wirtschaftsstrukturen führen können (disruptive Technologien), Aufklärungsziel des Bundesnachrichtendienstes. Die Künstliche Intelligenz wirkt hier insbesondere als Schlüssel- und Querschnittstechnik, weil sie die Entwicklung und Nutzung nahezu aller aufkommenden und disruptiven Technologien signifikant beschleunigt.

Weitere Beispiele für Gefährdungen der Sicherheit des Bundes oder eines Landes sind gewichtige Bedrohungen der Sicherheit des Weltraums aus der militärischen und nachrichtendienstlichen Nutzung von Weltraumsystemen (insbesondere Satelliten), Antisatellitensystemen und im Weltraum stationierter Waffen, entsprechende Beeinträchtigungen des freien grenzüberschreitenden Handels mit Energie und Rohstoffen oder die Aufklärung nachrichtendienstlicher Aktivitäten staatlicher Akteure mit unmittelbarem Bezug zur Bundesrepublik Deutschland.

Nummer 2, Buchstabe c)

Buchstabe c) umfasst den Bestand oder die Sicherheit von Einrichtungen der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages sowie eines Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages. Der Schutz solcher Einrichtungen steht gleichermaßen wie der Schutz von nationalen Einrichtungen ein gewichtiges Interesse der Bundesrepublik Deutschland dar. Gefährdungen des europäischen Wirtschafts- und Wissenschaftsstandortes und diesem zugeordneter Wirtschaftssubjekte können immensen volkswirtschaftlichen Schaden begründen und in der Folge eine Gefährdung der Sicherheit von Mitgliedsstaaten der Europäischen Union bedeuten. Deutschland ist eng in internationale Handels- und Finanzströme eingebunden. Gesicherte Versorgungswege, stabile Märkte sowie funktionierende Kommunikationsströme sind hierfür unerlässlich. Die Abhängigkeit Deutschlands im globalen Handel wird weiter zunehmen. 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. Entsprechende Beeinträchtigungen können von ausländischen Unternehmen aber auch von ausländischen staatlichen Stellen, einschließlich fremder Nachrichtendienste ausgehen. 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 Kauf 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. Die Aufklärung entsprechender Aktivitäten muss dem Bundesnachrichtendienst daher auch mittels der strategischen Ausland-Fernmeldeaufklärung möglich sein.

Nummer 2, Buchstabe d)

Maßnahmen der strategischen Ausland-Fernmeldeaufklärung sind auch zulässig zum Schutz der außenpolitischen Handlungsfähigkeit der Bundesrepublik Deutschland. 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 Systeme. Solche Gefährdungen können sich auch auf das wirtschaftspolitische Geschehen auswirken oder dort ihren Ursprung haben, beispielsweise bei globalen Finanz- und Ölkrisen. Hieraus ergeben sich wichtige strategische Konsequenzen für die deutsche Außen- und Wirtschaftspolitik. Handlung ist ein zielgerichtetes Vorgehen zur Durchsetzung der eigenen Interessen. Um dies zu

gewährleisten, bedarf es zwingend einer umfassenden und zutreffenden Kenntnis des internationalen Sachverhalts. Auch die Kenntnis der Interessen der Akteure ist notwendig, um zum Beispiel kooperative Lösungen zu entwickeln. Für den Bundesnachrichtendienst erwächst hieraus die Notwendigkeit eines zielgerichteten Einsatzes der strategischen Ausland-Fernmeldeaufklärung zur Informationsdeckung.

Die außenpolitische Handlungsfähigkeit der Bundesrepublik Deutschland kann beispielsweise auch dann tangiert werden, wenn die Bundesrepublik Deutschland in internationalen Konflikten als neutrale Stelle eine Vermittlerrolle einnimmt. Die Neutralität dieser Rolle der Bundesrepublik Deutschland kann durch Einflussnahme von beteiligten oder Drittstaaten gefährdet werden und ist somit zur Erfüllung dieser politischen Verantwortung zu schützen.

Nummer 3

Auch zum Schutz von gewichtigen Rechtsgütern der Allgemeinheit, deren Grundlagen die Existenz der Menschen berührt, sind Maßnahmen der strategischen Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes zulässig. So sind entsprechende Maßnahmen insbesondere zulässig, um Gefährdungen der Energie- und Rohstoffsicherheit begegnen zu können. Der gesetzliche Auftrag des Bundesnachrichtendienstes umfasst dabei den Schutz der Versorgungslage in der Bundesrepublik Deutschland, aber auch in Mitgliedstaaten der Europäischen Union.

Zu Absatz 5

Die Erhebung von Inhaltsdaten ist im Rahmen der strategischen Ausland-Fernmeldeaufklärung unverändert nur anhand von Suchbegriffen zulässig. Suchbegriffe können u.a. Anschlusskennungen, Signaturen von Übertragungen (das heißt bestimmte technische Parameter), geografische Bereiche, inhaltliche Suchbegriffe oder ein bestimmtes Telekommunikationsnetz einer geschlossenen Nutzergruppe sein. Suchbegriffe können auch Suchmuster sein, die auf Ergebnissen vorheriger Auswertungen beruhen. In der Praxis handelt es sich bei den vom Bundesnachrichtendienst genutzten Suchbegriffen zu einem weit überwiegenden Teil um formale Suchbegriffe, also in der Regel um Telekommunikationsmerkmale. Inhaltliche Suchbegriffe, also Suchbegriffe, mittels derer nach bestimmten Begriffen im Telekommunikationsinhalt gesucht wird (z. B. Namen von bestimmten, z. B. für die Herstellung von Sprengstoffen genutzten chemischen Verbindungen) werden hingegen in geringerem Umfang eingesetzt. Auf diese Weise soll bestmöglich sichergestellt werden, dass zielgerichtet nur die Kommunikation erfasst wird, die auftragsrelevant für die Tätigkeit des Bundesnachrichtendienstes ist und nicht Kommunikation von Personen, in der die inhaltlichen Suchbegriffe lediglich zufällig bzw. aufgrund eines nicht nachrichtendienstlich relevanten Sachverhaltes verwendet werden.

Der Einsatz von Suchbegriffen erfolgt jeweils zum frühestmöglichen Zeitpunkt bei der Datenerhebung. Bei bestimmten Arten von Suchbegriffen kann diese Selektion technisch bedingt erst in einem weiteren Verarbeitungsschritt unmittelbar nach der Datenerhebung erfolgen. Es dürfen nur solche Suchbegriffe verwendet werden, die zur Erhebung von auftragsrelevanten Informationen führen, das heißt die für die Aufklärung der nach Absatz 1 bestimmten Vorgänge bestimmt, geeignet und erforderlich sind. Ihre Verwendung muss darüber hinaus im Einklang mit den außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland stehen.

Im Rahmen der Prüfung der Erforderlichkeit ist sicherzustellen, dass – soweit Suchbegriffe von bestimmten Personen verwendet werden – die Verwendung von Suchbegriffen von

Verursachern von Gefahren, Nachrichtennetzern oder sonst näher qualifizierten Informanten gegenüber der Verwendung von Suchbegriffen völlig unbeteiligter Personen vorrangig erfolgt (vgl. BVerfG, a.a.O., Randnummer 187). Die Befugnisse aus § 24 bleiben unberührt.

Im Verhältnis zur Überwachung individueller Telekommunikation weist die strategische Fernmeldeaufklärung allerdings insoweit ein geringeres Eingriffsgewicht auf, als sie sich auf Datenströme bezieht, deren Ergiebigkeit im Einzelnen nicht vorhersehbar ist. Auch soweit sie mittels formaler Suchbegriffe auf die Überwachung einzelner Personen gerichtet ist, ist sie typischerweise weniger zielgenau und nicht vollständig, da die für eine konkrete Kommunikationsverbindung genutzten Netze und Übertragungstrecken (sogenanntes Routing) je nach Verfügbarkeit weithin spontan bestimmt werden und nur ein geringer Bruchteil der deutschlandweit und weltweit vorhandenen Netze von Erfassungsmaßnahmen des Bundesnachrichtendienstes erfasst wird. Die strategische Fernmeldeaufklärung unterscheidet sich in ihrem Eingriffsgewicht damit grundsätzlich von einer Beschränkung im Einzelfall, wie sie etwa durch § 3 des Artikel 10-Gesetzes ermöglicht wird (vgl. BVerfG, a.a.O., Randnummer 148).

Hinsichtlich des Schutzes von Vertraulichkeitsbeziehungen sind die Vorgaben nach § 21 zu beachten. Eine Erhebung von Daten zum Zweck der Erlangung von Erkenntnissen zum Kernbereich privater Lebensgestaltung ist unzulässig (vgl. § 22 Absatz 1). Weitere Vorgaben zur Verwendung von Suchbegriffen von bestimmten Personengruppen enthält § 20.

Zu Absatz 6

Im Rahmen der strategischen Ausland-Fernmeldeaufklärung kann der Bundesnachrichtendienst auftragsrelevante nachrichtendienstliche Informationen nicht ausschließlich durch eigene Erfassungsanlagen oder durch Verpflichtung eines Telekommunikationsunternehmens nach § 25 erheben. Auftragsrelevante Kommunikation wird zu einem erheblichen Anteil auch über ausländische Vermittlungsanlagen, Telekommunikationsinfrastruktur oder vergleichbare informationstechnische Systeme von Telekommunikationsdiensteanbietern geführt, auf denen der Bundesnachrichtendienst keinen kooperativen Zugang einrichten kann, da das Telekommunikationsunternehmen seinen Sitz im Ausland hat und daher nicht nach § 25 zur Ausleitung von Daten an den Bundesnachrichtendienst verpflichtet werden kann.

Vor diesem Hintergrund benötigt der Bundesnachrichtendienst die Befugnis, zur Erschließung relevanter Daten mit heimlichen Mitteln und/oder unter Zugriff auf informationstechnische Systeme von Telekommunikationsanbietern Sicherungsmaßnahmen zu überwinden. Die nach erfolgreicher Zugangseinrichtung erfolgende Datenerhebung dient der Durchführung strategischer Aufklärungsmaßnahmen und richtet sich nach den Vorschriften dieses Unterabschnitts. Die Verarbeitung umfasst Daten aus der laufenden Kommunikation, also den Gegenstand des durch den Telekommunikationsdiensteanbieter erbrachten Dienstes. Darüber hinaus umfasst die Verarbeitung Daten, die Telekommunikationsunternehmen während der eigenen Verarbeitung der laufenden Kommunikation in Zwischenspeichern ihrer informationstechnischen Systeme „puffern“, z.B. für den Fall der wiederholten Zustellung bei Fehlern in der Übermittlung oder falls ein Empfänger zum Zeitpunkt des Sendens nicht erreichbar ist, sofern sie nach Anordnung der strategischen Aufklärungsmaßnahme nach Absatz 1 erhoben wurden und zum Zeitpunkt der Datenerhebung durch den Bundesnachrichtendienst nicht älter als 48 Stunden sind. Diese Daten benötigt der Bundesnachrichtendienst zur Kompensation von Ausfällen,

weil der nicht kooperative Zugang weniger stabil ist als eine Datenerhebung durch Datenausleitung durch den Bundesnachrichtendienst auf Grundlage eines nach § 25 verpflichteten Telekommunikationsunternehmens.

Die Verarbeitung umfasst darüber hinaus auch Bestandsdaten des Telekommunikationsunternehmens, wie z.B. der vom Telekommunikationsunternehmen gespeicherte Name und die Anschrift des Nutzers der bereitgestellten Anschlüsse, soweit diese anhand von Suchbegriffe nach Absatz 5 erhoben wurden oder sich auf den jeweiligen Kommunikationspartner beziehen (z.B. Gesprächspartner bei einem Telefonat). Der Bundesnachrichtendienst benötigt Informationen aus den Bestandsdaten insbesondere zur Feststellung der Nutzer dieser Anschlüsse. Diese Daten sind nur auf dem beschriebenen Weg durch den Bundesnachrichtendienst nutzbar, da – im Gegensatz zur Situation im Inland – die Einholung einer Bestandsdatenauskunft bei ausländischen Telekommunikationsdiensteanbietern nicht möglich ist.

Die Verarbeitung unselektierter Verkehrs- und sonstiger Metadaten, die auf dem oben beschriebenen Weg erlangt wurden, richtet sich nach § 26.

Für den – in der Praxis nicht relevanten – Fall, dass der Telekommunikationsbieter das informationstechnische System nicht zur Abwicklung seiner Dienstleistung, sondern ausschließlich als eigenes nutzt, richtet sich die Zulässigkeit der Datenerhebung nach § 34.

Zu Absatz 7

Absatz 7 Satz 1 grenzt die strategische Ausland-Fernmeldeaufklärung von der Verarbeitung von personenbezogenen Daten aus Telekommunikationsverkehren von deutschen Staatsangehörigen, von inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen ab. Eine solche ist ausschließlich unter dem Rechtsregime des Artikel 10-Gesetzes zulässig.

Nach Satz 2 ist durch den Einsatz automatisierter Filter dafür zu sorgen, dass solche Daten – soweit technisch möglich – bereits automatisiert ausgefiltert werden. In der Praxis verwendet der Bundesnachrichtendienst hierzu ein mehrstufiges, automatisiertes Filtersystem, um solche Verkehre zu erkennen und unwiederbringlich zu löschen, sofern keine Beschränkungsmaßnahme nach dem Artikel 10-Gesetz vorliegt. Der Einsatz automatisierter Filterprozesse soll – wie vom Bundesverfassungsgericht gefordert (BVerfG, a.a.O., Randnummer. 172) – sicherstellen, dass den Mitarbeitern des Bundesnachrichtendienstes solche Telekommunikationsverkehre nicht bekannt werden. Nach Satz 3 sind die ausgefilterten Daten unverzüglich automatisiert zu löschen. Die Verpflichtung des Bundesnachrichtendienstes, die Filtermethoden kontinuierlich fortentwickeln und auf dem jeweiligen Stand der Technik zu halten, wird vom Bundesverfassungsgericht ausdrücklich gefordert (BVerfG, a.a.O., Randnummer 162) und trägt dem Umstand Rechnung, dass Maßnahmen der strategischen Fernmeldeaufklärung einer fortwährenden technischen Entwicklung unterworfen sind.

Werden im Rahmen der strategischen Ausland-Fernmeldeaufklärung trotz der eingesetzten automatisierten Filtersysteme dennoch Telekommunikationsverkehre erhoben, an denen eine deutsche Staatsangehörige oder ein deutscher Staatsangehöriger, eine inländische juristische Person oder eine sich im Bundesgebiet aufhaltende Person beteiligt ist, und wird dieser Verkehr nicht unverzüglich gelöscht, ist dies der betroffenen Person nach § 12 des Artikel 10-Gesetzes grundsätzlich mitzuteilen. Eine Mitteilung kommt jedoch entsprechend der Vorgaben des Artikel 10-Gesetzes nur in Betracht, wenn ausgeschlossen ist, dass der Zweck der Maßnahme (zum Beispiel Aufklärung eines bestimmten Terrornetzwerks) hierdurch gefährdet wird und kein übergreifender Nachteil für das Wohl des Bundes oder eines Landes absehbar ist (zum Beispiel, wenn durch die Mitteilung besondere Aufklärungsfähigkeiten des Bundesnachrichtendienstes bekannt würden). Die Zuständigkeit in diesen

Mitteilungsfällen liegt der bisherigen Praxis entsprechend bei der G 10-Kommission. Sofern die Mitteilung nicht innerhalb von zwölf Monaten nach dem Datum der Erhebung erfolgt, entscheidet die G 10-Kommission über die weitere Zurückstellung der Mitteilung. Auch die Entscheidung über die endgültige Nichtmitteilung obliegt der G 10-Kommission. Die Entscheidung über die endgültige Nichtmitteilung darf erst fünf Jahre nach Erhebung des Verkehrs erfolgen und die Voraussetzungen für die Mitteilungen müssen mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten. Solange die Daten noch für eine Mitteilung oder eine gerichtliche Überprüfung der Erhebung erforderlich sind, darf keine Löschung erfolgen. Die Löschung erfolgt daher erst nach einer endgültigen Nichtmitteilung oder – bei Mitteilung – nach Ablauf der Rechtsmittelfrist. Die Daten werden gesperrt, um eine weitere Nutzung der Daten durch den Bundesnachrichtendienst auszuschließen.

Zu Absatz 8

Nach den Maßgaben des Bundesverfassungsgerichts ist die strategische Ausland-Fernmeldeaufklärung vor dem Hintergrund des Verhältnismäßigkeitsgrundsatzes trotz ihrer Streubreite als hinreichend fokussiertes Instrument auszugestalten und damit begrenzt zu halten. Eine globale und pauschale Überwachung lasse das Grundgesetz auch zu Zwecken der Auslandsaufklärung nicht zu (BVerfG, a.a.O., Randnummer 168). Absatz 8 trägt diesem Verbot einer globalen Überwachung durch die Volumenbegrenzung auf höchstens 30 Prozent der Übertragungskapazität aller global bestehenden Telekommunikationsnetze Rechnung. Da es durchaus Telekommunikationsnetze gibt, die in ihrer Gesamtheit auftragsrelevante Daten enthalten (z.B. Telekommunikationsnetze, die ausschließlich für die Kommunikation öffentlicher Stellen eines Krisenstaates genutzt werden), bezieht sich die angegebene Beschränkung auf maximal 30 Prozent aller bestehenden Telekommunikationsnetze weltweit und nicht auf Übertragungskapazitäten innerhalb einzelner Telekommunikationsnetze.

Darüber hinaus ergibt sich die Volumenbeschränkung bereits aus der Beschränkung auf nur solche Telekommunikationsnetze bzw. Netzbestandteile, die für strategische Aufklärungsmaßnahmen relevant sind. Zudem ist die Erhebung aus diesen Netzen wiederum ausschließlich auf nachrichtendienstlich relevante Datenarten beschränkt. Eine weitere Beschränkung ergibt sich aus der Selektion dieser Teilmenge an Daten mittels Suchbegriffen.

Zu Absatz 9

Absatz 9 stellt klar, dass eine Informationserhebung und -verarbeitung zum Zweck der Erzielung von Wettbewerbsvorteilen (Wirtschaftsspionage) – wie bei der Auftragserfüllung des Bundesnachrichtendienstes insgesamt – auch im Rahmen der strategischen Ausland-Fernmeldeaufklärung unzulässig ist. Die Regelung entspricht der Regelung im bisherigen § 6 Absatz 5.

Zu Absatz 10

Absatz 10 normiert eine Kennzeichnungspflicht für personenbezogene Daten aus der strategischen Ausland-Fernmeldeaufklärung im Rahmen der Weiterverarbeitung. Anzugeben sind der Zweck der Datenerhebung nach Absatz 1 (Nummer 1) und das Mittel der Datenerhebung (Nummer 2).

Die Kennzeichnung der nach § 19 Absatz 1 erhobenen Daten dient insbesondere der Kontrolle, der Ermöglichung von Unterrichtungen sowie der Feststellung der einschlägigen Rechtsgrundlage im Falle einer Übermittlung der Daten. Der Bundesnachrichtendienst kann selbstständig festlegen, auf welchem Wege er der Kennzeichnung für diese Zwecke

Rechnung trägt. Dies wird regelmäßig durch eine technische Kennzeichnung umgesetzt werden. Die Kennzeichnung erfolgt unmittelbar nach der Datenerhebung in einem nachgelagerten technischen Verarbeitungsschritt.

Die Kennzeichnung entfällt bei Übermittlungen. Eine Kennzeichnung nach Nummer 1 und Nummer 2 ist regelmäßig nicht für die Aufgabenerfüllung der Übermittlungsadressaten erforderlich bzw. würde keinen Mehrwert für diese darstellen (so sind z. B. die Mittel der Datenerhebung bei Adressaten, die nicht ebenfalls ein Nachrichtendienst sind, im Regelfall andere, , die auch anderen Erhebungsschwellen unterliegen, so dass die Benennung des nachrichtendienstlichen Mittels der Datenerhebung dort keinen Erkenntniszuwachs bedeuten würde). Zudem würde mit einer Angabe des Mittels der Datenerhebung jedenfalls bei einer größeren Zahl von Übermittlungen eine mittelbare Offenlegung der technischen Leistungsfähigkeit des Bundesnachrichtendienstes drohen. Diese ist jedoch besonders schutzbedürftig, da eine solche Offenlegung Rückschlüsse auf Fähigkeiten und Aufklärungspotenziale des Bundesnachrichtendienstes ermöglichen würde, die dessen zukünftige Aufklärungsmöglichkeiten negativ beeinträchtigen könnten. Zur Sicherstellung der adäquaten Weiterverarbeitung beim Empfänger fügt der Bundesnachrichtendienst jeder Übermittlung einen Hinweis bei, der Aufschluss darüber gibt, zu welchen Zwecken der Empfänger die Daten verwenden darf (vgl. § 29 Absatz 12 sowie die Verweise auf diese Verpflichtung in § 30 Absatz 9 und § 38 Absatz 12). Der Hinweis stellt daher als aliud zur Weiterleitung der internen Kennzeichnung bei der Übermittlung der Daten den korrekten Umgang des Empfängers mit den übermittelten Daten sicher, wahrt aber gleichermaßen das Interesse des Bundesnachrichtendienstes an Verhinderung einer Offenlegung seiner technischen Leistungsfähigkeit.

§ 20 (Besondere Formen der strategischen Ausland-Fernmeldeaufklärung)

Zu Absatz 1

Absatz 1 regelt die konkreten Voraussetzungen für die gezielte Erhebung personenbezogener Daten von Einrichtungen der Europäischen Union, öffentlicher Stellen ihrer Mitgliedsstaaten oder von Unionsbürgerinnen und Unionsbürgern führen. Eine gezielte Datenerhebung in diesem Sinne liegt vor, wenn die Verwendung eines bestimmten Suchbegriffs (zum Beispiel eine E-Mail-Adresse) dazu dienen soll, Telekommunikationsverkehre von Einrichtungen der Europäischen Union, öffentlichen Stellen ihrer Mitgliedsstaaten oder Unionsbürgerinnen und Unionsbürgern zu erheben. Datenerhebungen nach Absatz 1 dürfen nur in Ausnahmefällen erfolgen, wenn die engen Voraussetzungen des Satzes 1 erfüllt werden. Die Datenerhebung muss entweder nach Nummer 1 zur Früherkennung von Gefahren im Sinne des § 19 Absatz 4 oder zur Informationsgewinnung nach Nummer 2 erforderlich sein. Nach Satz 1 Nummer 2 ist eine gezielte Datenerhebung zulässig, wenn dies erforderlich ist, um Informationen zur Erkennung und Begegnung von Gefahren für die innere oder äußere Sicherheit der Bundesrepublik Deutschland, zur Wahrung der Handlungsfähigkeit der Bundesrepublik Deutschland oder zur Gewinnung von sonstigen Erkenntnissen von außen- und sicherheitspolitischer Bedeutung zu erlangen. Weitere Voraussetzung ist, dass ausschließlich Daten über Vorgänge in Drittstaaten gesammelt werden sollen, die von besonderer Relevanz für die Sicherheit der Bundesrepublik Deutschland sind.

Satz 2 regelt den Fall der nachträglichen Erkennung der gezielten Erhebung von Daten nach Satz 1. Solche Daten dürfen nur weiterverarbeitet werden, wenn die Voraussetzungen des Satzes 1 vorliegen. Liegen diese Voraussetzungen nicht vor, müssen die Daten unverzüglich gelöscht werden.

Zu Absatz 2

Gegenüber Personen, die als mögliche Verursacher von Gefahren mit Blick auf gegenüber ihnen zu ergreifenden Folgemaßnahmen im unmittelbaren Interesse des Bundesnachrichtendienstes stehen, hat der Gesetzgeber insoweit einen eigenen Schutzmechanismus vorzusehen. Gegenüber ihnen hat die Überwachung eine besondere Intensität und es besteht eine gesteigerte Wahrscheinlichkeit von belastenden Folgen (BVerfG, a.a.O., Randnummer 188). Absatz 2 trägt dem besonderen Schutzbedürfnis dieses Personenkreises Rechnung, wobei auf die konkrete Absicht der Übermittlung erhobener Daten zu Zwecken der Gefahrenabwehr und Strafverfolgung abzustellen ist. Die gezielte Datenerhebung zu diesen Personen bzw. Personengruppen unterliegt bei Absicht der Datenübermittlung zu Zwecken der Gefahrenabwehr oder Strafverfolgung der Anordnung der Leitung des Bundesnachrichtendienstes sowie grundsätzlich der Prüfung der Rechtmäßigkeit durch den Unabhängigen Kontrollrat vor deren Vollzug (vgl. § 23 Absatz 5 und 7). Zusätzlich zu diesem besonderen formellen Schutzmechanismus ist materiell im Rahmen der Verhältnismäßigkeitsprüfung die gegenüber solchen Personen gesteigerte Wahrscheinlichkeit belastender Folgen besonders zu berücksichtigen.

Zu Absatz 3

Absatz 3 schließt die Überwachung der gesamten Telekommunikation einer Person aus. Eine solche würde bereits dem grundlegenden Gedanken der strategischen Ausland-Fernmeldeaufklärung widersprechen. Eine umfassende Überwachung des gesamten Telekommunikationsverkehrs einer Person ist gegeben, wenn sämtliche von einer Person genutzten Telekommunikationsmerkmale bewusst von der Maßnahme erfasst sind und der Bundesnachrichtendienst bewusst auf alle Telekommunikationsnetze, auf denen die Kommunikation geführt wird, Zugriff hat. Die Aufklärung alleine eines oder auch mehrerer Telekommunikationsmerkmale einer Person erfüllt diese Bedingung hingegen nicht von vornherein. Dies gilt auch, soweit die Umsetzung der Aufklärung der Telekommunikation derart erfolgt, dass ein im Inland ansässiges Telekommunikationsunternehmen unmittelbar die Ausleitung der Telekommunikation des Betroffenen anhand einzelner Suchbegriffe für den Bundesnachrichtendienst durchführt. So kann die Umsetzung einer Maßnahme nach § 19 bei der besonderen Form der Nutzung von Suchbegriffen nach § 20 auch gerichtet sein auf die Ausleitung der Telekommunikation des Betroffenen durch ein verpflichtetes Telekommunikationsunternehmen auf Grundlage einzelner Telekommunikationsmerkmale des Betroffenen. Hierbei wird dann durch das verpflichtete Telekommunikationsunternehmen nicht übergreifend die gesamte, durch das Unternehmen ermöglichte Telekommunikation bzw. die Gesamtheit seiner angebotenen Dienste dem Bundesnachrichtendienst zugänglich gemacht, sondern lediglich – als Teilmenge – die Telekommunikation, die über eine als Suchbegriff verwendete Anschlusskennung übermittelt wird und dies auch nur in dem Umfang, als sie über das jeweilige Telekommunikationsnetz geführt wird. Beispielsweise kann es bei der Früherkennung der Gefahr von internationalen kriminellen, terroristischen oder staatlichen Angriffen mittels Schadprogrammen oder vergleichbar schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen zur Auftragserfüllung des Bundesnachrichtendienstes erforderlich, aber auch ausreichend sein, die über einen in Deutschland ansässigen Serverbetreiber vermittelten Datenverkehre betreffend eine bestimmte IP-Adresse eines erkannten oder mutmaßlichen ausländischer Cyberangreifer aufzuklären. Hierbei genügt der Zugriff auf die Datenverkehre, die über die erkannte IP-Adresse des Cyberangreifers geleitet werden. Es werden aber gerade nicht alle Datenverkehre der jeweiligen Person erfasst.

§ 21 (Schutz von Vertraulichkeitsbeziehungen)

Zu Absatz 1

Gegenüber Berufs- und Personengruppen, deren Kommunikationsbeziehungen einen besonderen Schutz der Vertraulichkeit verlangen, ist zunächst deren gezielte Überwachung zu begrenzen. Die Nutzung von Suchbegriffen, die zu einer gezielten Erfassung der Telekommunikationsanschlüsse solcher Personen führen, kann nicht schon allein damit gerechtfertigt werden, dass hierdurch potentiell nachrichtendienstlich relevante Informationen erlangt werden können. Insbesondere die journalistische Tätigkeit rechtfertigt nicht, Personen einem höheren Risiko der Überwachung auszusetzen als andere Grundrechtsträger und sie wegen ihrer Kontakte und Recherchen zum Objekt der Informationsabschöpfung zur Verfolgung von Sicherheitsinteressen zu machen. Entsprechendes gilt für Rechtsanwältinnen und Rechtsanwälte (vgl. BVerfG, a.a.O., Randnummer 194) sowie für Geistliche.

Diesen Vorgaben des Bundesverfassungsgerichts trägt Absatz 1 Rechnung, indem er bestimmt, dass die Verwendung von Suchbegriffen zur gezielten Erhebung personenbezogener Daten von Rechtsanwältinnen und Rechtsanwälten, Journalistinnen und Journalisten sowie Geistlichen zum Zweck der Erlangung von Erkenntnissen, die dem Zeugnisverweigerungsrecht unterfallen, unzulässig ist. Die Bestimmung bezweckt somit im Hinblick auf Rechtsanwältinnen und Rechtsanwälte den Schutz der Vertraulichkeitsbeziehung zum Mandanten und der ihnen in dieser Eigenschaft anvertrauten Informationen. Im Hinblick auf Journalistinnen und Journalisten dient die Bestimmung dem Schutz der Vertraulichkeitsbeziehung dieser Personen zu ihren Informanten und des Redaktionsgeheimnisses. Der Schutz beschränkt sich auf Tätigkeiten, die dem Schutz des Artikel 5 Absatz 1 GG unterfallen. Dies ist insbesondere bei als Journalisten getarnten Vertreterinnen oder Vertreter fremder Nachrichtendienste oder Personen, die mediale Propaganda für journalistisch und extremistische Gruppierungen betreiben, nicht der Fall, da für diese bereits der persönliche Schutzbereich des Artikel 5 Absatz 1 GG nicht eröffnet ist. Gleiches gilt für Geistliche, die in ihrer Eigenschaft als Seelsorger zur Radikalisierung beitragen oder anstiften.

Im Gegensatz zu Geistlichen und Rechtsanwälten ist der Begriff „Journalist“ nicht eindeutig an institutionelle Zugehörigkeiten oder eine staatliche Zulassung gebunden. Nähere Vorgaben zur Bewertung durch den Bundesnachrichtendienst sind daher in einer Dienstvorschrift zu regeln, die der Kontrolle durch den Unabhängigen Kontrollrat unterliegt

Zu Absatz 2

Die gezielte Aufklärung besonderer Vertraulichkeitsbeziehungen ist in Ausnahmefällen möglich, jedoch auch im Rahmen der strategischen Ausland-Fernmeldeaufklärung an qualifizierte Eingriffsschwellen zu binden. Danach ist die Verwendung von Suchbegriffen entgegen Absatz 1 möglich, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass die zeugnisverweigerungsberechtigte Person Täter oder Teilnehmer einer der in § 29 Absatz 3 genannten Straftaten ist, sowie zur Verhinderung der in Absatz 2 beschriebenen schwersten Gefahren. Im erstgenannten Fall entfällt die Schutzbedürftigkeit, da die betroffene Person insoweit keinen die Schutzbedürftigkeit der Vertraulichkeitsbeziehung begründenden Zweck verfolgt (Verstrickungsregelung). Die Entscheidung hierüber ist nach § 23 Absatz 5 Nummer 3 dem Präsidenten des Bundesnachrichtendienstes zugewiesen. § 23 Absatz 7 sieht zudem vor, dass der Unabhängige Kontrollrat die Rechtmäßigkeit der Anordnungen der Suchbegriffe vor deren Verwendung prüft. Damit wird der verfassungsrechtlichen Vorgabe, den Schutz von Vertraulichkeitsbeziehungen durch eine gerichtsähnliche ex ante-Kontrolle abzusichern, umfassend Rechnung getragen.

Zu Absatz 3

Soweit die Erhebung von besonders schutzwürdigen Vertraulichkeitsbeziehungen erst im Rahmen der Auswertung bemerkt wird, bedarf es einer Prüfung, ob eine Erhebung dieser Daten nach den Voraussetzungen des Absatzes 2 materiell zulässig gewesen wäre, das heißt, ob die Weiterverarbeitung der erhobenen Daten notwendig ist zur Verhinderung der in Absatz 2 genannten schweren Straftaten und Gefahren. Auch diese Entscheidung unterliegt der umfassenden Rechtskontrolle durch den Unabhängigen Kontrollrat (vgl. BVerfG, a.a.O., Randnummer 195). Die Sätze 3 bis 5 regeln Einzelheiten zur Protokollierung der Löschung.

§ 22 (Kernbereichsschutz)

§ 22 regelt den Schutz des Kernbereichs privater Lebensgestaltung im Rahmen der strategischen Ausland-Fernmeldeaufklärung. Die Vorschrift sieht ebenso wie andere Regelungen (vgl. etwa § 100a Absatz 4 StPO und § 5a G 10) zum Kernbereichsschutz im Bereich der Telekommunikationsüberwachung ein zweistufiges Schutzkonzept vor, um den Betroffenen vor Eingriffen in den absolut geschützten Kernbereich privater Lebensgestaltung zu bewahren.

Der Schutz des Kernbereichs privater Lebensgestaltung gewährleistet dem Individuum einen Bereich höchstpersönlicher Privatheit und sichert einen dem Staat nicht verfügbaren Menschenwürdekern grundrechtlichen Schutzes gegenüber Überwachung. Selbst überragende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Bereich privater Lebensgestaltung nicht rechtfertigen. Dies gilt auch gegenüber Nachrichtendiensten und auch für Aufklärungsmaßnahmen im Ausland. Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge, Überlegungen und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen. Geschützt ist insbesondere die nicht-öffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens, die in der berechtigten Annahme geführt wird, nicht aufgeklärt zu werden. Solche Gespräche verlieren dabei nicht schon dadurch ihren Charakter als insgesamt höchstpersönlich, dass sich in ihnen Höchstpersönliches und Alltägliches vermischen. Demgegenüber gehören z.B. die Besprechung und Planung von Straftaten nicht zum Kernbereich privater Lebensgestaltung, selbst wenn sie auch Höchstpersönliches zum Gegenstand haben. Dies bedeutet nicht, dass der Kernbereich unter einem allgemeinen Abwägungsvorbehalt in Bezug auf öffentliche Sicherheitsinteressen steht. Ein höchstpersönliches Gespräch fällt nicht dadurch aus dem Kernbereich privater Lebensgestaltung heraus, dass die Kenntnis seiner Inhalte für die Aufklärung von Straftaten oder die Abwehr von Gefahren hilfreiche Aufschlüsse geben kann. Geben Äußerungen hierbei ausschließlich innere Eindrücke und Gefühle wieder, ohne Hinweise auf konkrete Straftaten zu enthalten, gewinnen sie nicht schon dadurch einen Gemeinschaftsbezug, dass sie Ursachen oder Beweggründe eines strafbaren Verhaltens freizulegen vermögen. Auch können trotz Straftatenbezugs Situationen, in denen Einzelnen gerade ermöglicht werden soll, ein Fehlverhalten einzugestehen oder sich auf dessen Folgen einzurichten, wie Beichtgespräche oder vertrauliche Gespräche mit einem Psychotherapeuten oder einem Strafverteidiger, der höchstpersönlichen Privatsphäre unterfallen (vgl. BVerfG, a.a.O., Randnummern 200 bis 202).

Ob eine personenbezogene Kommunikation diesem Kernbereich zuzuordnen ist, hängt davon ab, ob sie nach ihrem Inhalt höchstpersönlichen Charakters ist und in welcher Art und Intensität sie aus sich heraus die Sphäre anderer oder Belange der Gemeinschaft berührt. Maßgebend sind die Besonderheiten des jeweiligen Einzelfalls. Nicht zu diesem Kernbereich gehören Kommunikationsinhalte, die in unmittelbarem Bezug zu konkreten strafbaren Handlungen stehen, wie etwa Angaben über die Planung bevorstehender oder

über begangene Straftaten. Die Frage, ob eine Information im Rahmen der nachrichtendienstlichen Aufklärung unter den Schutz des Kernbereiches privater Lebensgestaltung fällt, ist also mit Blick auf das jeweilige Aufklärungsziel zu entscheiden (vgl. BVerfG, NJW 2009, 2431, [2436]).

Zu Absatz 1

Auf Ebene der Datenerhebung bestimmt Absatz 1, dass eine zielgerichtete Erhebung kernbereichsrelevanter Daten unzulässig ist. Die Verwendung von Suchbegriffen ist danach unzulässig, wenn tatsächliche Anhaltspunkte vorliegen, dass durch ihre Nutzung ausschließlich Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden.

Für die Datenerhebung und den Einsatz von Suchbegriffen im Bereich der strategischen Ausland-Fernmeldeaufklärung sind weitere, über das Verbot der gezielten Kernbereichserfassung hinausgehende, gesetzliche Vorkehrungen nicht geboten. Da sich aus den Suchbegriffen als solchen in der Regel nicht erkennen lässt, dass mit entsprechender Wahrscheinlichkeit kernbereichsrelevante Kommunikation erfasst wird, bedarf es keiner spezifischen Regelungen, die darauf gerichtet sind, kernbereichsrelevante Suchbegriffe im Vorfeld auszusondern. Dies lässt unberührt, dass, soweit der Einsatz von Suchbegriffen erkennbar eine erhebliche Wahrscheinlichkeit der Erfassung kernbereichsrelevanter Kommunikation birgt, diese nach Möglichkeit informationstechnisch schon im Vorfeld von der Erhebung ausgeschlossen werden müssen (vgl. BVerfG, a.a.O., Randnummer 206).

Zu Absatz 2

Kommt es trotz Absatz 1 zur Erhebung kernbereichsrelevanter Daten, schreibt Absatz 2 ein umfassendes Verwertungsverbot, ein unverzügliches Lösungsgebot sowie eine entsprechende Pflicht zur Protokollierung der Löschung vor.

Zu Absatz 3

Auf der Ebene der händischen Datenauswertung ist gesetzlich sicherzustellen, dass die weitere Auswertung unverzüglich unterbrochen werden muss, wenn erkennbar wird, dass eine Überwachung in den Kernbereich persönlicher Lebensgestaltung eindringt. Schon bei Zweifeln darf ihre Fortsetzung – vorbehaltlich von Regelungen für Eilfälle – nur in Form von Aufzeichnungen erlaubt werden, die vor ihrer Auswertung von einer unabhängigen Stelle zu sichten sind. Dabei ist klarzustellen, dass Erkenntnisse aus dem höchstpersönlichen Lebensbereich nicht verwertet werden dürfen und unverzüglich zu löschen sind. Dies ist zu protokollieren und die Lösungsprotokolle müssen zur Gewährleistung einer datenschutzrechtlichen Kontrolle hinreichend lange aufbewahrt werden (vgl. BVerfG, a.a.O., Randnummer 200 bis 207).

Absatz 3 enthält vor diesem Hintergrund eine Regelung für Fälle, in denen Zweifel bestehen, ob die erhobenen Daten dem Kernbereich privater Lebensgestaltung zuzuordnen sind und die Weiterverarbeitung der Daten erforderlich ist. Der Bundesnachrichtendienst hat die relevanten Daten in diesen Fällen dem Unabhängigen Kontrollrat vorzulegen, der die Rechtmäßigkeit der Weiterverarbeitung prüft. Stellt dieser fest, dass die Daten dem Kernbereich privater Lebensgestaltung zuzuordnen sind, gilt ein umfassendes Verwertungsverbot, ein unverzügliches Lösungsgebot sowie eine entsprechende Pflicht zur Protokollierung der Löschung.

§ 23 (Anordnung)

Zu Absatz 1

Die Durchführung strategischer Aufklärungsmaßnahmen ist durch die Präsidentin oder den Präsidenten des Bundesnachrichtendienstes oder durch sie oder ihn bestimmte Vertretung anzuordnen. Die Präsidentin oder der Präsident des Bundesnachrichtendienstes kann mithin die Antragsbefugnis auch dauerhaft auf einen von ihr oder ihm bestimmte Vertreterin oder Vertreter delegieren. Verlängerungen der Anordnungen sind – auch mehrfach – zulässig, soweit das Ziel der strategischen Aufklärungsmaßnahme weiterhin besteht.

Zu Absatz 2

Für Anordnungen nach Absatz 1 gilt das Schriftformerfordernis. Zu benennen sind der Aufklärungszweck, das Aufklärungsthema, der geografische Fokus der Aufklärungsmaßnahme, deren Dauer sowie eine Begründung mit Erläuterungen zu den Hintergründen und den angestrebten Zielen der strategischen Aufklärungsmaßnahme.

Zu Absatz 3

In der Anordnung von strategischen Aufklärungsmaßnahmen zum Zweck der Gefahrenfrüherkennung ist über die in Absatz 2 genannten Angaben die Art der Gefahr im Sinne des § 19 Absatz 4 zu benennen.

Zu Absatz 4

Absatz 4 enthält eine Verpflichtung zur Prüfung der Rechtmäßigkeit der Anordnung von strategischen Aufklärungsmaßnahmen durch den Unabhängigen Kontrollrat vor deren Vollzug. Die Möglichkeit des Vollzugs der Anordnung nach vorläufiger Prüfung der Rechtmäßigkeit durch ein Mitglied des Unabhängigen Kontrollrats ist vorgesehen, wenn die Gefahr besteht, dass das Ziel der strategischen Aufklärungsmaßnahme durch die Verzögerung aufgrund des zusätzlichen Verfahrens ansonsten vereitelt oder wesentlich erschwert würde. Um der Bundesregierung beispielsweise bei Entführungsfällen im Ausland, bei denen Kommunikation erhoben werden soll, die nicht dem Artikel 10-Gesetz unterfällt, oder in anderen Ausnahmesituationen unverzüglich Informationen über neue krisenhafte Entwicklungen zur Verfügung stellen zu können, müssen die strategischen Aufklärungsmaßnahmen des Bundesnachrichtendienstes kurzfristig angepasst werden können. Sofern eine Anordnung nach vorläufiger Bestätigung der Rechtmäßigkeit durch ein Mitglied des Unabhängigen Kontrollrats vollzogen wurde, im Anschluss jedoch durch den Unabhängigen Kontrollrat für rechtswidrig erklärt wird, sind die aufgrund der Anordnung bereits erhobenen personenbezogenen Daten im Bundesnachrichtendienst unverzüglich zu löschen.

Zu Absatz 5

Die gezielte Erhebung von Zielen bedarf in den in Absatz 5 genannten Fällen der Anordnung durch die Präsidentin oder den Präsidenten des Bundesnachrichtendienstes oder eine durch sie oder ihn bestimmte Vertretung. Soweit im Einzelfall gegen die betroffene Person bereits eine Beschränkungsanordnung nach dem Artikel 10-Gesetz vorliegt, bedarf die Erhebung von Kommunikationen dieser Person ohne Deutschlandbezug keiner separaten Anordnung nach dieser Vorschrift. Der Unabhängige Kontrollrat ist jedoch über entsprechende Anordnungen zu unterrichten. Der Unabhängige Kontrollrat kann in diesem Fall auch jederzeit stichprobenartige Kontrollen der auf Basis der Anordnung erhobenen Auslandskommunikationen vornehmen.

Zu Absatz 6

Für Anordnungen nach Absatz 5 gilt das Schriftformerfordernis. Zu benennen sind die strategische Aufklärungsmaßnahme, in deren Rahmen die gezielte Datenerhebung erfolgt, (soweit bekannt), das Ziel der Datenerhebung, die geplante Dauer der gezielten

Datenerhebung sowie eine Begründung. Verlängerungen der Anordnungen sind – auch mehrfach – zulässig, soweit das Ziel der Verwendung der Suchbegriffe weiterhin besteht. Mehrere Telekommunikationsteilnehmer, die hinsichtlich des gleichen Sachverhaltes im Interesse des Bundesnachrichtendienstes stehen und zu denen eine gezielte Datenerhebung im Sinne des § 20 erfolgen soll, sollen zusammengefasst mit Bezug zum jeweiligen Sachverhalt angeordnet werden.

Zu Absatz 7

Der Unabhängige Kontrollrat prüft alle Anordnungen nach Absatz 5 vor deren Vollzug. Suchbegriffe, die nicht § 20 oder § 21 unterfallen und damit nicht auf Grundlage einer Anordnung zur gezielten Datenerhebung verwendet werden, kann der Unabhängige Kontrollrat jederzeit stichprobenartig überprüfen. Bei dieser Prüfung kann der Unabhängige Kontrollrat beispielsweise eine Erläuterung zu ausgewählten Suchbegriffen verlangen. Die Möglichkeit des Vollzugs der Anordnung nach vorläufiger Bestätigung der Rechtmäßigkeit durch ein Mitglied des Unabhängigen Kontrollrats ist vorgesehen, wenn die Gefahr besteht, dass das Ziel der Verwendung der Suchbegriffe durch die Verzögerung aufgrund des zusätzlichen Verfahrens ansonsten vereitelt oder wesentlich erschwert wird. Sofern eine Anordnung nach vorläufiger Bestätigung der Rechtmäßigkeit durch ein Mitglied des Unabhängigen Kontrollrats vollzogen und im Anschluss durch den Unabhängigen Kontrollrat für rechtswidrig erklärt wird, sind die aufgrund der Anordnung bereits erhobenen personenbezogenen Daten unverzüglich zu löschen.

Zu Absatz 8

Der Bundesnachrichtendienst ist verpflichtet, das Bundeskanzleramt in regelmäßigen Abständen über entsprechende Anordnungen zu unterrichten. Eine ähnliche Regelung ist im bisherigen § 9 Absatz 2 Satz enthalten.

§ 24 (Eignungsprüfung)

Im Rahmen der Eignungsprüfung werden personenbezogene Inhaltsdaten durch den Bundesnachrichtendienst abweichend von § 19 Absatz 5 ohne vorherigen Einsatz von Suchbegriffen erhoben und auf zwei Kriterien hin geprüft: Zum einen wird der Datenstrom genutzt, um geeignete neue Suchbegriffe für strategische Aufklärungsmaßnahmen zu generieren. Durch die Sichtung des Datenstroms können zum Beispiel neue Kommunikationsmittel erkannt werden, die zur Generierung neuer Suchbegriffe für strategische Aufklärungsmaßnahmen genutzt werden können. Würden ausschließlich auf Basis von Suchbegriffen erhobene Daten durch den Bundesnachrichtendienst betrachtet, würden dessen Datenerhebungsmöglichkeiten massiv eingeschränkt werden. Darüber hinaus wird im Rahmen der Eignungsprüfung auch die Relevanz bekannter Suchbegriffe für strategische Aufklärungsmaßnahmen geprüft. Der Datenstrom kann zum anderen daraufhin geprüft werden, ob sich bestimmte Telekommunikationsnetze für strategische Aufklärungsmaßnahmen eignen. Für diese Zwecke werden im Rahmen der Eignungsprüfung auch personenbezogene Verkehrs- und sonstige Metadaten erhoben. In diesem Fall wird geprüft, ob sich in diesen Daten befinden, die für strategische Aufklärungsmaßnahmen relevant sind. Wenn dies bereits bekannt ist, muss keine Eignungsprüfung erfolgen. Die Telekommunikationsnetze können in diesem Fall auch unmittelbar auf Grundlage des § 19 unter den dort genannten Voraussetzungen genutzt werden.

Zu Absatz 1

Absatz 1 legt fest, zu welchen Zwecken die Eignungsprüfung erfolgen darf: Bei der Eignungsprüfung dürfen aus Telekommunikationsnetzen ohne Einsatz von Suchbegriffen Daten erhoben werden, um geeignete Suchbegriffe oder geeignete

Telekommunikationsnetze für strategische Aufklärungsmaßnahmen zu bestimmen. Die Regelung entspricht weitgehend der Regelung im bisherigen § 12 Absatz 1. Eine Eignungsprüfung zur Bestimmung neuer Suchbegriffe kann sowohl in Bezug auf Daten erfolgen, die aus Telekommunikationsnetzen erhoben werden, die bereits für strategische Aufklärungsmaßnahmen genutzt werden, als auch auf Daten, die aus Telekommunikationsnetzen erhoben werden, die ihrerseits im Rahmen der Eignungsprüfung erhoben werden.

Zu Absatz 2

Voraussetzung für die Durchführung der Eignungsprüfung ist, dass tatsächliche Anhaltspunkte dafür vorliegen, dass in dem jeweiligen Telekommunikationsnetz Daten übertragen werden, die für die Durchführung strategischer Aufklärungsmaßnahmen relevant sind.

Zu Absatz 3

Die Eignungsprüfung zur Bestimmung geeigneter Telekommunikationsnetze nach Absatz 1 Nummer 1 muss durch die Präsidentin oder den Präsidenten des Bundesnachrichtendienstes durch eine durch sie oder ihn bestimmte Vertretung angeordnet werden. Die Anordnung muss sich nicht auf einzelne Telekommunikationsnetze beziehen, die im Rahmen der Eignungsprüfung betrachtet werden, sondern kann auf übergeordneter Ebene erfolgen.

Zu Absatz 4

Absatz 4 regelt die Möglichkeit der Verpflichtung von Anbietern von Telekommunikationsdiensten zur Datenausleitung auch im Rahmen der Eignungsprüfung und orientiert sich an der Regelung im bisherigen § 12 Absatz 2 Satz 3.

Zu Absatz 5

Absatz 5 regelt die Zweckbindung für die erhobenen personenbezogenen Daten. Eine anderweitige Nutzung als in Absatz 1 benannt, ist nur in Ausnahmefällen zulässig. Der Kernbereichsschutz wird durch einen Verweis auf eine Regelung im BSI-Gesetz sichergestellt. Danach gilt auch für Daten, die im Rahmen der Eignungsprüfung erhoben wurden, § 5 Absatz 7 Satz 2 bis 8 BSI-Gesetz entsprechend. Eine Speicherung der erhobenen personenbezogenen Daten ist im Rahmen der Eignungsprüfung zulässig. Die Speicherdauer wird in Absatz 6 geregelt. Die Auswertung der erhobenen Daten hat unverzüglich zu erfolgen.

Zu Absatz 6

Absatz 6 legt die Speicherdauer für personenbezogene Daten fest, die im Rahmen der Eignungsprüfung erhoben wurden. Soweit die personenbezogenen Daten für die Bestimmung geeigneter Suchbegriffe ausgewertet werden sollen, dürfen diese für die Dauer von zwei Wochen gespeichert werden. Dienen die personenbezogenen Daten der Bestimmung geeigneter Telekommunikationsnetze, darf die Speicherung für höchstens vier Wochen erfolgen. Für die Löschung der personenbezogenen Daten gelten die in Satz 4 geregelten Protokollierungspflichten und in die Satz 5 geregelte Zweckbindung.

Ausgenommen von diesen Löschfristen und Speicherdauern sind die entsprechenden Daten, solange der Bundesnachrichtendienst ihren Inhalt aus technischen Gründen nicht lesbar machen kann. Dies ist der Fall, wenn er Daten zu bisher unbekanntem Modulationsverfahren, Protokollen oder Verschlüsselungen erhebt. Aufgrund der heute verwendeten komplizierten Techniken in der Telekommunikation ist es oft erst nach Jahren möglich, solche Verfahren, insbesondere neue Verschlüsselungsverfahren, zu lösen. Hierfür ist die Vorhaltung ausreichender Datenmengen über längere Zeiträume zwingend

notwendig. Zur Analyse der Daten müssen auch die darin gegebenenfalls enthaltenen personenbezogenen Daten erhalten bleiben. Da die Inhalte der Daten nicht lesbar sind, sind auch die darin etwaig enthaltenen personenbezogenen Daten nicht lesbar. Somit entsteht aus der längeren Speicherung von 10 Jahren für die Betroffenen keine relevante datenschutzrechtliche Beschwer.

Lesbar können ausschließlich die Verkehrsdaten der Erfassung, zum Beispiel Sender und Empfänger, sein. Hier treten regelmäßig IP-Adressen als mögliche personenbezogene Daten auf. Die Löschung dieser Verkehrsdaten würde eine weitere Analyse zu Zwecken der Erarbeitung neuer Entschlüsselungsfähigkeiten jedoch unmöglich machen, da auftragsrelevante Nutzer nicht erkannt werden könnten. Da es sich bei den hier in Rede stehenden Daten lediglich um einzelne Verkehrsdaten der Betroffenen handelt und die Daten einer engen Zweckbindung unterliegen, entsteht auch hier keine relevante datenschutzrechtliche Beschwer der Betroffenen.

Die 10-Jahresfrist orientiert sich an der Regelung in § 7, der vorsieht, dass die Frist zur Prüfung der weiterhin gegebenen Erforderlichkeit der Daten für die Aufgabenerfüllung 10 Jahre beträgt. Im Gegensatz zur vorgenannten Prüffrist werden die nicht lesbaren Daten allerdings in jedem Fall nach Ablauf der 10 Jahre gelöscht.

Sobald der Bundesnachrichtendienst die Daten lesbar machen kann, gelten dieselben Fristen für Speicherung, Löschung und Protokollierung wie für personenbezogene lesbare Daten, die im Rahmen der Eignungsprüfung erhoben wurden. Das heißt, die Daten sind nach zwei bzw. vier Wochen zu löschen. Die durch die Analyse gewonnenen Erkenntnisse – Sachinformationen zu den verwendeten Protokollen oder Verschlüsselungsverfahren – darf der Bundesnachrichtendienst für seine weitere Arbeit nutzen, die konkreten Inhalte der erhobenen Daten nur unter den Voraussetzungen des Absatz 7.

Zu Absatz 7

Absatz 7 ermöglicht ausnahmsweise eine zweckändernde Verarbeitung von Daten, die im Rahmen der Eignungsprüfung erhoben wurden.

Nummer 1

Nummer 1 erlaubt eine zweckändernde Verarbeitung von Daten für den Fall, dass tatsächliche Anhaltspunkte dafür vorliegen, dass hierdurch eine erhebliche Gefahr für Leib, Leben oder Freiheit einer Person oder für die Sicherheit Deutschlands oder die Sicherheit der Mitgliedstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages besteht.

Nummer 2

Als einziger mit der zivilen und militärischen Aufklärung beauftragter Auslandsnachrichtendienst der Bundesrepublik Deutschland übernimmt der Bundesnachrichtendienst auch die Funktion eines militärischen Auslandsnachrichtendienstes. Als solcher arbeitet er in vielfältiger Weise sehr eng mit der Bundeswehr zusammen und muss erhobene Erkenntnisse, einschließlich personenbezogener Daten, effektiv und ohne Verzögerung an die entsprechend besonders ermächtigten Stellen der Bundeswehr bzw. zur dortigen Auswertung übermitteln können, um seiner Warn-, Schutz-, Informations- und Einsatzunterstützungsfunktion in Bezug auf die Aufgabenwahrnehmung der Bundeswehr gerecht zu werden. Häufig ist hierfür, insbesondere mit Blick auf die sog. Force Protection, also dem Schutz der Soldatinnen und Soldaten im Ausland, eine automatisierte Datenübermittlung an die Bundeswehr erforderlich. Nummer 2 gestattet dem Bundesnachrichtendienst daher die automatisierte Übermittlung von Daten an die Bundeswehr. Die Übermittlung umfasst sowohl Inhalts- als

auch Verkehrs- und sonstige Metadaten, darf jedoch ausschließlich zu den dort genannten Zwecken erfolgen. Vergleichbar mit den Regelungen in § 12 sowie § 29 Absatz 4 stellt auch die Regelung in Nummer 2 einen Baustein der privilegierten Zusammenarbeit zwischen dem Bundesnachrichtendienst und der Bundeswehr im Rahmen der Funktion des Bundesnachrichtendienstes als militärischer Auslandsnachrichtendienst dar (auf die dortigen Ausführungen wird verwiesen). Nummer 2 gestattet dem Bundesnachrichtendienst die automatisierte Übermittlung von Daten, die auf Grundlage von Absatz 1 erhoben wurden, an die Bundeswehr. Die Übermittlung darf jedoch ausschließlich zu den dort genannten Zwecken erfolgen.

Der Bundesnachrichtendienst verfolgt bei der Erhebung von Daten im Rahmen der strategischen Ausland-Fernmeldeaufklärung einen strategischen und überregionalen Aufklärungsansatz. Hierbei ist ihm die Erhebung von Inhaltsdaten grundsätzlich nur anhand von konkreten und hinreichend bestimmten Suchbegriffen gestattet (vgl. § 19 Absatz 5). Im Gegensatz dazu benötigt die Bundeswehr personenbezogene Daten zu bestimmten geografischen Gebieten bzw. Regionen. Insbesondere betrifft dies Daten mit räumlichem Bezug zu Bundeswehr Camps oder Einsatzgebieten der Bundeswehr. Die Daten dienen insbesondere dem Schutz der Funktionsfähigkeit der Bundeswehr mit dem Zweck der Verhinderung von Gefahren für Leib und Leben deutscher Soldatinnen und Soldaten. Es handelt sich zum Beispiel um Daten im Zusammenhang mit Anschlagdrohungen auf Bundeswehr Camps. Dem Schutz der Funktionsfähigkeit dienen aber auch Daten, die der Bundeswehr als Grundlage für taktisch-operative Entscheidungen im Auslandseinsatz dienen. So kann beispielsweise die Übermittlung von Daten zu gegnerischen Kräften, z.B. Rebellengruppen, sowie zu deren Planungen der Bundeswehr ermöglichen, vor Ort bereits im Vorfeld einer Gefahr für Leib und Leben die erforderlichen Gegenmaßnahmen zu veranlassen. Bei diesen regional und thematisch begrenzten Aufgaben der Bundeswehr ist zudem stets ein unverzügliches Handeln angezeigt. Daher besteht nicht in allen Fällen die Möglichkeit, hinreichend bestimmte Suchbegriffe für die Aufklärung eines entsprechenden Sachverhaltes bzw. relevanter Personen zu benennen. Entsprechende Suchbegriffe müssten zunächst ermittelt bzw. generiert werden, was mit einer erheblichen Zeitverzögerung einherginge. Auch sind derartige zeitkritische Informationen meist nur zu einem bestimmten Zeitpunkt von Relevanz, so dass eine nachträgliche Verwendung entsprechender Suchbegriffe nicht zu demselben Ergebnis führen würde (zum Beispiel Informationen zu Hindernissen auf Patrouillenwegen, Demonstrationen vor Ort, die für die Einsatzplanung erforderlich sind). Eine nachträgliche Verwendung entsprechender Suchbegriffe würde daher dem Bedarf der Bundeswehr an schnellstmöglicher Übermittlung relevanter Daten widersprechen. Vor diesem Hintergrund ist dem Bundesnachrichtendienst ausnahmsweise in Abweichung von den Vorgaben in Absatz 5 Satz 1 eine Übermittlung von personenbezogenen Inhalts-, Verkehrs- und sonstigen Metadaten, die im Rahmen der Eignungsprüfung – und damit nicht auf Grundlage von entsprechenden Suchbegriffen – erhoben wurden, zu den dort genannten Zwecken gestattet. Die Übermittlung darf in diesen durch die Übermittlungszwecke streng begrenzten und häufig zeitkritischen Fällen auch automatisiert erfolgen.

Die Übermittlung zur Sicherstellung der Funktionsfähigkeit der Bundeswehr im Rahmen der Landes- oder Bündnisverteidigung und bei Auslandseinsätzen nimmt Bezug auf die vorgenannten Funktionen des Bundesnachrichtendienstes. Die Landes- und Bündnisverteidigung umfasst spiegelbildlich zu § 19 Absatz 4 Nummer 1 einerseits nationale Verteidigungsinteressen der Bundesrepublik Deutschland und andererseits Verteidigungsinteressen internationaler Bündnisse bzw. Systeme gegenseitiger kollektiver Sicherheit, an denen die Bundesrepublik Deutschland beteiligt ist und stellt einen verfassungsunmittelbaren Kernauftrag der Bundeswehr dar (Artikel 87a Absatz 1 GG).

Auslandseinsätze der Bundeswehr im Sinne dieses Gesetzes sind alle Formen des Einsatzes deutscher Streitkräfte. Dazu zählen mandatierte Einsätze, einsatzgleiche Verpflichtungen der Bundeswehr, die Beteiligung an Missionen (NATO bzw. EU und VN), sowie besondere Einsatzformen (zum Beispiel Einsätze der Spezialkräfte oder seegehender Einheiten) oder Evakuierungsoperationen. Der Begriff der Auslandseinsätze erstreckt sich dabei auch auf den Einsatz der Streitkräfte in Gebieten jenseits nationaler Souveränität, z.B. auf der Hohen See. Für die sichere Wahrnehmung dieser Aufträge ist die Bundeswehr auf schnelle Übermittlungen von Informationsaufkommen aus der Ausland-Fernmeldeaufklärung zwingend angewiesen.

Die politischen und rechtlichen Verpflichtungen, die aus der Mitgliedschaft in Bündnissen, Systemen gegenseitiger kollektiver Sicherheit im Sinne des Artikels 24 Absatz 2 GG und ähnlichen Kooperationen einhergehen, rechtfertigen sich, dass Übermittlungen im vorgenannten Sinne auch zum Schutz der Funktionsfähigkeit der Streitkräfte von Mitgliedstaaten der Europäischen Union, des Nordatlantikvertrages oder der Europäischen Freihandelsassoziation zulässig sind.

Zudem darf eine automatisierte Übermittlung personenbezogener Daten erfolgen, wenn dies zum Schutz von Leib, Leben oder Freiheit einer Person erforderlich ist.

§ 25 (Pflichten der Anbieter von Telekommunikationsdiensten, Entschädigung)

§ 25 regelt die Pflichten der Anbieter von Telekommunikationsdiensten. Diese sind parallel zu dem Verfahren bei Maßnahmen nach dem Artikel 10-Gesetz ausgestaltet. Die Regelung orientiert sich eng am bisherigen § 8.

Zu Absatz 1

Personen und Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen oder hieran mitwirken, sind verpflichtet, an der Durchführung der strategischen Ausland-Fernmeldeaufklärung mitzuwirken. Die hierfür erforderlichen Mitwirkungspflichten werden in Absatz 1 bestimmt: Sie haben auf Anordnung des Bundeskanzleramtes Auskunft über die näheren Umstände der Telekommunikation zu erteilen. Sendungen sind dem Bundesnachrichtendienst auszuhändigen sowie die Überwachung und Aufzeichnung zu ermöglichen. Die Pflichten der Anbieter von Telekommunikationsdiensten sind im Näheren im Telekommunikationsgesetz und in der Telekommunikations-Überwachungsverordnung geregelt.

Nach Absatz 1 sind auch solche Anbieter von Telekommunikationsdiensten verpflichtet, die in Deutschland eine Niederlassung haben oder die vorgenannten Dienste oder Mitwirkungshandlungen in Deutschland erbringen. Mit der Regelung erfolgt eine Klarstellung zum Anwendungsbereich in Bezug auf ausländische Unternehmen. Bereits die bisherige Verpflichtungsregelung in § 8 enthält keine Beschränkung auf Unternehmen mit einer (Zweig-) Niederlassung im Inland. Auch die inländische Leistungserbringung begründet die deutsche Jurisdiktion über den Sachverhalt. Um ausländischen Unternehmen im Kundenverhältnis eine eindeutige Legitimationsgrundlage für ihre Kooperation zu geben, wird das Marktortprinzip nunmehr ausdrücklich im Gesetz verankert.

Zu Absatz 2

Absatz 2 regelt den notwendigen Inhalt der Anordnung gegenüber dem Verpflichteten. Die Anordnung muss danach das verpflichtete Unternehmen, die Dauer der Verpflichtung und die betroffene Telekommunikation bezeichnen. Die betroffene Telekommunikation ist so genau zu bezeichnen, dass die erforderlichen Mitwirkungshandlungen bestimmt sind. So sind beispielsweise gegenüber dem verpflichteten Unternehmen die von der Maßnahme

erfassten Telekommunikationsnetze oder Teile hiervon eindeutig zu bezeichnen. Soweit lediglich Telekommunikation, die über einzelne Anschlusskennungen (Rufnummer, IP-Adresse etc.) vermittelt wird, aufgeklärt werden soll, sind diese anzugeben. Die rechtlichen Voraussetzungen einer solchen Verpflichtung ergeben sich aus der der Verpflichtung zugrundeliegenden Maßnahme im Sinne des § 19.

Zu Absatz 3

Die Regelung in Absatz 3 entspricht der Regelung im bisherigen § 8 Absatz 2. Verpflichtete Anbieter von Telekommunikationsdiensten haben die erforderlichen Geheimschutzvorkehrungen zu treffen. Dazu gehört u.a., dass die hiermit betrauten Mitarbeiterinnen und Mitarbeiter einer Sicherheitsüberprüfung unterzogen werden müssen und sie über die Mitteilungsverbote nach § 60 sowie die Folgen eines Verstoßes nach § 66 zu belehren sind. Darüber hinaus sind alle Geheimschutzmaßnahmen nach der Verschlusssachenanweisung des Bundesministeriums des Innern zu treffen.

Zu Absatz 4

Absatz 4 regelt die Durchführung der Sicherheitsüberprüfung. Diese richtet sich nach dem Sicherheitsüberprüfungsgesetz. Die Regelung entspricht dem bisherigen § 8 Absatz 3.

Zu Absatz 5

Die Vorschrift regelt die Entschädigung der in Anspruch genommenen Anbieter von Telekommunikationsdiensten. Die Kosten werden nicht pauschal erstattet, sondern die tatsächlich entstandenen Kosten müssen durch die Verpflichteten nachgewiesen werden und werden sodann ersetzt. Die Regelung entspricht dem bisherigen § 18.

§ 26 (Verarbeitung von personenbezogenen Verkehrsdaten)

Die Neuregelung der Verkehrsdatenverarbeitung in § 26 setzt die Kritik des Bundesverfassungsgerichts an der bisherigen Regelung zur Verkehrsdatenverarbeitung in § 6 Absatz 6 um und enthält zudem in Umsetzung zweier Urteile des Bundesverwaltungsgerichts Regelungen zur Erhebung und anonymisierten Speicherung von Verkehrsdaten von deutschen Staatsangehörigen, inländischen juristischen Personen und sich im Bundesgebiet aufhaltenden Personen.

Zu Absatz 1

In Absatz 1 wird in Umsetzung der Vorgaben des Bundesverfassungsgerichts eine klare Befugnis zur Erhebung und Verarbeitung von personenbezogenen Verkehrsdaten ausgesprochen, die die allgemeine Befugnisnorm für die strategische Ausland-Fernmeldeaufklärung in § 19 ergänzt und den spezifischen technischen Anforderungen der Verarbeitung von personenbezogenen Verkehrsdaten Rechnung trägt. Die Erhebungsgrundlage umfasst neben Verkehrsdaten auch alle weiteren personenbezogenen Metadaten, die in der strategischen Ausland-Fernmeldeaufklärung anfallen (vgl. Definitionen in der Begründung zu § 19 Absatz 1). Die Erhebung von personenbezogenen Verkehrs- und Metadaten, die nicht im Zusammenhang mit einer Individualkommunikation stehen, greift mangels unmittelbaren Bezugs zu einer Telekommunikation im Sinne des Art. 10 GG lediglich in das Recht auf informationelle Selbstbestimmung des Betroffenen ein. Da es sich hierbei im Vergleich zum Fernmeldegeheimnis des Artikels 10 GG um ein niederschwelligeres Grundrecht handelt, ist die Erhebung solcher Metadaten auf Grundlage dieser Norm erst recht möglich.

Die Verarbeitung von personenbezogenen und im Zusammenhang mit einer Individualkommunikation stehenden Verkehrsdaten von deutschen Staatsangehörigen, von inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen

ist grundsätzlich unzulässig. Ein Eingriff in deren Fernmeldegeheimnis findet nicht statt. Dies ist durch geeignete Filtermechanismen sicherzustellen (vgl. auch entsprechende Erläuterungen zu § 19 Absatz 7).

Der Verweis auf § 19 Absatz 6 stellt klar, dass der Bundesnachrichtendienst Verkehrsdaten unter den Voraussetzungen des § 26 auch aus informationstechnischen Systemen eines ausländischen Telekommunikations- oder Telemediendiensteanbieters im Ausland, zu denen er sich mit technischen Mitteln auch ohne dessen Wissen Zugang verschafft hat, erheben darf

Zu Absatz 2

Auch bei der Weiterverarbeitung von personenbezogenen Verkehrsdaten ist eine Kennzeichnung von Zweck und Mittel der Datenerhebung erforderlich. Diese erfolgt jedoch – abweichend von der Parallelregelung in § 19 Absatz 10 – nicht bereits unmittelbar nach der Datenerhebung, sondern erst bei der manuellen Auswertung der Daten. Dies ist der Tatsache geschuldet, dass bei der Erhebung der Verkehrs- und sonstigen Metadaten eine Zuordnung der erhobenen Daten zu einem Erhebungszweck nicht möglich ist, da zu diesem Zeitpunkt noch nicht bekannt ist, welchem konkreten Thema die Daten zuzuordnen sind.

Zu Absatz 3

Absatz 3 Satz 1 verbietet die Verarbeitung von personenbezogenen Verkehrsdaten von deutschen Staatsangehörigen, inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen. Satz 2 regelt eine Ausnahme vom Grundsatz des Verbots der Erhebung solcher personenbezogener Verkehrs- und sonstige Metadaten. So wird dem Bundesnachrichtendienst in Nr. 1 die Befugnis erteilt, solche Verkehrsdaten dieser Personengruppe zu erheben und weiterzuverarbeiten, die nicht dem Schutz des Fernmeldegeheimnisses aus Artikel 10 GG unterfallen. Hierbei handelt es sich ausschließlich um Verkehrsdaten, die nicht im Zusammenhang mit einem Kommunikationsvorgang der vorgenannten Personengruppe anfallen, sondern als bloße Maschine-zu-Maschine-Kommunikation einzustufen sind. Solche Daten unterfallen nach herrschender Auffassung in der Literatur nicht dem Schutz des Fernmeldegeheimnisses. Dieses schützt nur individuelle Kommunikationen von natürlichen Personen und nicht durch deren Endgeräte aus technischen Gründen und ohne unmittelbares Zutun des Nutzers automatisiert ausgelöste Kommunikationen mit anderen Geräten. In Absatz 3 Satz 2 Nummer 2 wird eine weitere Ausnahme vom Verbot der Erhebung von Daten aus Telekommunikationsverkehren von deutschen Staatsangehörigen, inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen geregelt. Die Ausnahme betrifft Verkehrsdaten, sofern die zur Identifizierung geeigneten Daten der vorgenannten Personen unverzüglich unkenntlich gemacht wurden. Jeder Telekommunikationsverkehr enthält Verkehrsdaten, der aus einzelnen Daten wie Teilnehmer- oder Anschlusskennungen beider Telekommunikationsteilnehmer, Zeitstempel und technischen Parametern besteht. Hier werden diejenigen Verkehrsdaten der Unkenntlichmachung unterworfen, die eine Identifizierung von deutschen Staatsangehörigen, inländischen juristischen Personen oder sich im Bundesgebiet aufhaltenden Personen ermöglichen. Verkehrsdaten enthalten darüber hinaus Daten, die eine solche Identifizierbarkeit nicht ermöglichen, d.h. keinen Personenbezug aufweisen, wie Zeitstempel, technische Bezeichnung der Übertragungsstrecke, etc. Diese Daten müssen mangels Personenbezug nicht unkenntlich gemacht werden.

Die unkenntlich gemachten Daten dürfen für den in Absatz 5 genannten Zeitraum von sechs Monaten gespeichert werden und für Analysen sowie zur Weiterverarbeitung zu den im Gesetz genannten Zwecken genutzt werden. Mit der konkreten Zweckbindung werden

insbesondere die Rechte der Betroffenen gewahrt sowie die Grundsätze der Normenklarheit und Bestimmtheit beachtet.

Die gespeicherten Verkehrsdaten, bei denen personenbezogene Daten von deutschen Staatsangehörigen, inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen unkenntlich gemacht wurden, dürfen demnach genutzt werden, um bestimmte ausländische Personen, das heißt die Gegenstellen der Kommunikation der unkenntlich gemachten Personen, zu erkennen (Satz 4 Nummer 1) oder geeignete Telekommunikationsnetze für die strategische Fernmeldeaufklärung nach dem Artikel 10-Gesetz zu bestimmen (Satz 4 Nummer 2). Die Erkennung der Teilnehmer beschränkt sich hier auf solche, die nicht deutsche Staatsangehörige, inländische juristische Personen oder von sich im Bundesgebiet aufhaltende Personen sind.

Verkehrsdaten von deutschen Staatsangehörigen, inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen werden unverzüglich unkenntlich gemacht. Durch die Speicherung und Auswertung von Verkehrsdaten von Telekommunikationen, an denen deutsche Rufnummern oder solche von dem Bundesnachrichtendienst bekannten deutschen Staatsangehörigen, von inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen beteiligt sind, kann der Bundesnachrichtendienst auftragsrelevante Bezüge ausländischer Akteure nach Deutschland sowie auftragsrelevante Teilnehmer und Beziehungsnetze (Netzwerke) erkennen. Beispielsweise kann anhand der Verkehrsdaten erkannt werden, dass ein Kontakt einer ausländischen Person zu Personen in Deutschland besteht. Handelt es sich bei der ausländischen Person um eine bekannte Person aus dem terroristischen Spektrum, kann es von hoher Bedeutung sein, wenn diese mit Personen in Deutschland kommuniziert. Der Bundesnachrichtendienst kann auf Grundlage dieser Erkenntnis weitere Maßnahmen einleiten, wie z.B. die Beantragung einer Beschränkungsanordnung nach § 5 des Artikel 10-Gesetzes, um weitere Informationen zu Telekommunikationspartnern aus den nach Artikel 10 GG geschützten Telekommunikationsverkehren zu gewinnen und gegebenenfalls in der Folge Beschränkungsanordnungen nach § 3 des Artikel 10-Gesetzes zu erwirken. Die Analyse von Verkehrsdaten im Bundesnachrichtendienst dient demnach u.a. der frühzeitigen Erkennung von Teilnehmern, über die Informationen erlangt werden können, die für die Aufgabenerfüllung des Bundesnachrichtendienstes relevant sind (Satz 4 Nummer 1). Für die gesetzliche Auftragserfüllung des Bundesnachrichtendienstes nach § 1 Absatz 2 ist es essentiell, die entsprechenden Suchbegriffe der ausländischen Personen mit Deutschlandbezügen, zu erkennen.

Nach Satz 4 Nummer 2 dürfen die Daten auch zur Identifizierung von geeigneten Telekommunikationsnetzen für strategische Beschränkungsmaßnahmen des Bundesnachrichtendienstes nach § 5 des Artikel 10-Gesetzes genutzt werden. Damit soll die Zielgenauigkeit der strategischen Fernmeldeaufklärung verbessert werden. Denn die nach § 10 Absatz 4 des Artikel 10-Gesetzes zu bezeichnenden Telekommunikationsnetze müssen Telekommunikation enthalten, deren Ausgangspunkt oder Ziel in Deutschland liegt. Die Feststellung, bei welchen Telekommunikationsnetzen dies der Fall ist, ist dem Bundesnachrichtendienst jedoch nur möglich, wenn er auch im Vorfeld einer Beschränkungsmaßnahme nach dem Artikel 10-Gesetz potenziell geeignete Telekommunikationsnetze statistisch daraufhin untersuchen darf, ob hier auch tatsächlich maßgeblich solche Telekommunikationen mit einem Endpunkt in Deutschland enthalten sind. Diese statistische Untersuchung ist ihm nur möglich unter Nutzung von - unkenntlich gemachten - Verkehrsdaten von Telekommunikationen, an deutsche Staatsangehörige, inländische juristische oder sich im Bundesgebiet aufhaltende Personen beteiligt sind.

Bei der Analyse der entsprechenden Verkehrsdaten zu den beiden genannten Zwecken besteht damit ein erheblicher Mehrwert für den Bundesnachrichtendienst gerade darin, den vorliegenden Deutschlandbezug des ausländischen Akteurs erkennen zu können. Auch ohne Kenntnis über die Identität der betroffenen deutschen Staatsangehörigen, inländischen juristischen Personen oder sich im Bundesgebiet aufhaltenden Personen kann der Bundesnachrichtendienst wertvolle Erkenntnisse durch die Analyse der Verkehrsdaten gewinnen. Deshalb werden Verkehrsdaten von deutschen Staatsangehörigen, inländischen juristischen Personen oder sich im Bundesgebiet aufhaltenden Personen nach ihrer Erhebung unverzüglich automatisiert auf eine Weise unkenntlich gemacht, die die Eindeutigkeit der Daten, also die Unverwechselbarkeit einzelner Daten, erhält, aber die Identifizierung der Telekommunikationsteilnehmer oder Anschlussnehmer auch rückwirkend ohne unverhältnismäßig hohen Aufwand unmöglich macht (Absatz 3 Satz 2 und 3).

Die personenbezogenen Daten der Gegenseite, also zum Beispiel des Gesprächspartners, werden nicht unkenntlich gemacht, sofern der Telekommunikationsteilnehmer nicht deutscher Staatsangehöriger, inländische juristische Person oder eine sich im Bundesgebiet aufhaltende Person ist.

Die Unkenntlichmachung soll durch eine sogenannte Verhashung erfolgen. Dabei wird jeder Suchbegriff so durch eine Zeichenfolge (Hashwert) ersetzt, dass die folgenden Eigenschaften erfüllt sind:

1. Dasselbe Telekommunikationsmerkmal hat immer denselben Hashwert.
2. Verschiedene Suchbegriffe haben verschiedene Hashwerte.
3. Vom Hashwert kann man nur mit unrealistischem und unververtretbar hohem Rechenaufwand auf Suchbegriffe zurückrechnen.

Üblicherweise werden Hashwerte in sogenannter Hexadezimaldarstellung geschrieben, d.h. die Zeichenfolgen erscheinen als eine Kombination der Ziffern 0 bis 9 und der Buchstaben A bis F. Die Sicherheit der Unkenntlichmachung soll erhöht werden, indem mehrere Verhashungen hintereinander gestaffelt werden und der Adressraum vergrößert wird. Dies soll auch verhindern, dass der Suchbegriff durch einen sogenannten „Brute Force“-Angriff, bei dem alle theoretisch möglichen Suchbegriffe durchprobiert, also der Hashfunktion unterzogen werden, bis der richtige Hashwert herauskommt, bestimmt werden kann. Das Verhashen von Suchbegriffen hat folgende Auswirkungen:

Über den Hashwert ist nachvollziehbar, dass mehrere Kommunikationsvorgänge demselben Suchbegriff zuzuordnen sind. Über den Hashwert ist nicht nachvollziehbar, um welche Suchbegriffe oder Teilnehmer es sich konkret handelt. Die Suchbegriffe werden in Gänze innerhalb der „logischen Sekunde“ ihrer Erhebung automatisiert und ohne weitere Zwischenschritte der oben beschriebenen Hashfunktion unterworfen; eine Speicherung der ursprünglichen Daten erfolgt nicht. Daraus folgt, dass bei den Daten kein Personenbezug vorliegt. Die den Daten zuzuordnende Person ist auch nicht identifizierbar, da eine Umkehrrechnung zur Ermittlung des ursprünglichen Suchbegriffs aus dem Hashwert wie oben beschrieben nur mit unververtretbar hohem Aufwand, d.h. mit einem unrealistisch hohen Rechenaufwand, möglich ist. Folglich ist auch eine Mitteilung an die Betroffenen (schon aus tatsächlichen Gründen) nicht möglich.

Zu Absatz 4

Werden im Übrigen zeitlich verzögert zur Erhebung bei den im Bundesnachrichtendienst regelmäßig durchgeführten sog. Retroläufen Kommunikationsverkehre der in Absatz 1 Satz 2 genannten Personen nachträglich erkannt, werden diese ebenfalls nach der oben beschriebenen Methode unverzüglich unkenntlich gemacht, anderenfalls sind sie unverzüglich zu löschen.

Zu Absatz 5

Absatz 5 enthält eine Sonderregelung für die Speicherung der erhobenen personenbezogenen Verkehrs- und sonstige Metadaten. In dieser wird in Satz 1 die Vorgabe des Bundesverfassungsgerichts, wonach eine Höchstspeicherdauer von sechs Monaten bei der gesamthaft bevorratenden Speicherung von Verkehrsdaten nicht überschritten werden darf, umgesetzt. Eine längere Speicherung ist dann zulässig, wenn bei einer Einzelfallprüfung festgestellt wurde, dass die entsprechenden Verkehrsdaten für die Aufgabenerfüllung des Bundesnachrichtendienstes weiterhin erforderlich sind. Für diese Daten gelten dann die entsprechenden allgemeinen Vorgaben in § 27.

§ 27 (Auswertung der Daten und Prüfpflichten)

Die Regelung orientiert sich am bisherigen § 20 Absatz 1, modifiziert diesen jedoch, um den Besonderheiten der Auswertung von Daten aus der strategischen Ausland-Fernmeldeaufklärung Rechnung zu tragen.

Zu Absatz 1

Absatz 1 regelt die Pflicht zur Prüfung der Erforderlichkeit der auf Basis von Suchbegriffen nach § 19 Absatz 5 erhobenen Inhaltsdaten im Rahmen strategischer Aufklärungsmaßnahmen ohne schuldhaftes Zögern. Nach Feststellung der Erforderlichkeit der Daten müssen diese im Abstand von jeweils höchstens 7 Jahren einer erneuten Erforderlichkeitsprüfung unterzogen werden. Die Verkürzung der im bisherigen § 20 enthaltenen 10-Jahresfrist auf 7 Jahre ist erfolgt, um der besonderen Eingriffstiefe bei der Erhebung von personenbezogenen Daten mit Mitteln der strategischen Ausland-Fernmeldeaufklärung Rechnung zu tragen. Für den Fall, dass die Daten nicht erforderlich sind, ist der Bundesnachrichtendienst zur Löschung der Daten verpflichtet. 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, aber auch Kontrollen zur Prüfung des ordnungsgemäßen Funktionierens automatisierter Lösungsverfahren.

Zu Absatz 2

Absatz 2 stellt eine Ausnahme von der Löschverpflichtung für den Fall der Notwendigkeit der Daten zur Erfüllung von Mitteilungszwecken oder zu Kontrollzwecken des Unabhängigen Kontrollrats dar.

§ 28 (Datenerhebung durch eine ausländische öffentliche Stelle)

Zu Absatz 1

Zur Erfüllung seines Auftrages darf der Bundesnachrichtendienst auch ausländische öffentliche Stellen um die Durchführung strategischer Aufklärungsmaßnahmen ersuchen. Dies stellt oftmals die einzige Möglichkeit dar, auftragsrelevante Daten im Rahmen der strategischen Ausland-Fernmeldeaufklärung zu erheben, die ohne diese Möglichkeit für den Bundesnachrichtendienst nicht erreichbar wären (z.B. wegen Nichterreichbarkeit mittels der passiven Sensoren oder wegen nichtvorhandener Zugangsmöglichkeit durch Ausleitung durch einen verpflichtbaren Anbieter von Telekommunikationsdiensten nach § 25).

Zu Absatz 2

Absatz 2 enthält die Befugnis, die von der ersuchten ausländischen öffentlichen Stelle erhobenen Daten weiterzuverarbeiten. Hierbei sind die in diesem Unterabschnitt enthaltenden Vorschriften zur Weiterverarbeitung der Daten entsprechend anzuwenden.

Zu Absatz 3

Damit die ausländische öffentliche Stelle für den Bundesnachrichtendienst nur Daten erhebt und übermittelt, die er im Rahmen seines Auftrags benötigt, muss der Bundesnachrichtendienst der ausländischen öffentlichen Stelle vor der Datenerhebung in der Regel Suchbegriffe zur Verfügung stellen. Dies stellt keine Datenübermittlung im Sinne der Übermittlungsvorschriften dar, sondern ist in der Konzeption der strategischen Auslandfernmeldeaufklärung ein zwingend notwendiger vorgelagerter Schritt, um die ausländische öffentliche Stelle zur gezielten Datenerhebung zu veranlassen. Mit dem Verweis auf die Voraussetzungen der eigenen Datenverarbeitung (Absatz 2) und die Regelungen zum Einsatz von Suchbegriffen (Satz 1) werden an diese Suchbegriffe dieselben Anforderungen gestellt wie bei deren Verwendung durch den Bundesnachrichtendienst in eigenen Erfassungsansätzen. Hierdurch wird der sogenannte Ringtausch bei Datenerhebung durch eine ausländische öffentliche Stelle ausgeschlossen. In der Praxis handelt es sich um Suchbegriffe des Bundesnachrichtendienstes, die er auch im Rahmen der eigenen Datenerhebung einsetzt. Die ausländische öffentliche Stelle darf die Suchbegriffe des Bundesnachrichtendienstes jedoch grundsätzlich nur zum Zweck der Datenerhebung für den Bundesnachrichtendienst nutzen. Sollte die ausländische öffentliche Stelle die Suchbegriffe darüber hinaus auch für die Datenerhebung zu eigenen Zwecken verwenden wollen, so bedarf dies nach Absatz 3 Satz 2 der vorherigen Zustimmung des Bundesnachrichtendienstes. Dieser darf der Nutzung der Suchbegriffe durch die ausländische öffentliche Stelle nur zustimmen, wenn eine Übermittlung der Suchbegriffe nach den Übermittlungsvorschriften zulässig wäre.

Unterabschnitt 2 Übermittlung von Daten im Rahmen der strategischen Ausland-Fernmeldeaufklärung)

Die nachfolgenden Übermittlungsnormen regeln die Übermittlung personenbezogener Daten, die im Rahmen der strategischen Ausland-Fernmeldeaufklärung (§§ 19 ff.) erhoben worden sind. Da jede Übermittlung von personenbezogenen Daten für sich genommen einen eigenen Grundrechtseingriff darstellt, sind eine dem Verhältnismäßigkeitsgrundsatz Rechnung tragende, sowie dem Erfordernis der Normenklarheit genügende Ausgestaltung der Normen erforderlich (BVerfG, a.a.O., Randnummer 212 ff.). Vor diesem Hintergrund wurden mit den Übermittlungsnormen der §§ 29 f. Regelungen geschaffen, die den vorgenannten Erfordernissen bei der Erhebung von Daten durch Eingriff in das nach Artikel 10 Absatz 1 des GG geschützte Recht in der für Ausländer im Ausland geltenden Ausprägung Rechnung tragen. Sie stehen in einem Spezialitätsverhältnis zu den allgemeinen Übermittlungsnormen der §§ 10 ff. und treffen daher ausschließlich und insoweit gleichzeitig auch abschließend Regelungen in ihrem Anwendungsbereich.

Mit ihnen werden die besonderen Anforderungen an Übermittlungsnormen, die das Bundesverfassungsgericht in seinem Urteil vom 19. Mai 2020 für die Übermittlung von personenbezogenen Daten aus der strategischen Ausland-Fernmeldeaufklärung gefordert hat (BVerfG, a.a.O., Randnummer 211 ff.) umgesetzt. So knüpfen die jeweiligen Voraussetzungen in den Übermittlungstatbeständen an die Zwecke an, zu denen die personenbezogenen Daten erhoben und nach § 19 Absatz 1 oder § 26 Absatz 2 gekennzeichnet wurden. Dieser zentrale Aspekt einer Kopplung des Erhebungszwecks an einen Übermittlungs- und Weiterverarbeitungszweck, wird den Forderungen des Urteils gerecht und bildet gemeinsam mit den austarierten Übermittlungsschwellen und zu schützenden Rechtsgütern den Grundsatz der hypothetischen Datenneuerhebung ab (als zentrale Forderung formuliert in BVerfG, a.a.O., Randnummer 216).

Den vorgenannten Ausführungen folgend, gelten für die Übermittlung von personenbezogenen Daten, die mit den eingriffsintensiven Mitteln der strategischen Ausland-Fernmeldeaufklärung erhoben wurden, die Sonderregelungen dieses Abschnitts.

§ 29 (Übermittlung von personenbezogenen Daten aus der strategischen Ausland-Fernmeldeaufklärung an inländische öffentliche und andere Stellen)

Zu Absatz 1

Absatz 1 gestattet dem Bundesnachrichtendienst, personenbezogene Daten aus der strategischen Ausland-Fernmeldeaufklärung an die anderen Nachrichtendienste des Bundes oder der Länder zu übermitteln. Absatz 1 trägt dem Erfordernis des schnellen und effektiven Datenaustausches innerhalb der Nachrichtendienste Rechnung und berücksichtigt dabei den Umstand, dass die Empfängerbehörden allesamt nicht über exekutive Befugnisse verfügen. Es handelt sich aus diesem Grund um eine gegenüber den anderen inländischen öffentlichen Stellen privilegierende Vorschrift.

Bei den konkreten Übermittlungsvoraussetzungen der Nummern 1 und 2 ist die Zweckkennzeichnung der Daten bestimmend für ihre Verwendung: Nummer 1 sieht vor, dass die mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten bei Erforderlichkeit zum Schutz besonders gewichtiger Rechtsgüter übermittelt werden dürfen. Durch diese Hürde soll insbesondere im Rahmen des Verhältnismäßigkeitsgrundsatzes sichergestellt werden, dass nur die jeweils erforderlichen personenbezogenen Daten ausgetauscht werden. Dabei genügt das Vorliegen tatsächlicher Anhaltspunkte für die Erforderlichkeit der Übermittlung.

Die Nummer 2 bestimmt, dass die mit dem Zweck der politischen Unterrichtung oder der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten zum Zweck der Unterrichtung der Bundesregierung oder einer Landesregierung übermittelt werden dürfen, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung zur Erfüllung der Aufgaben des Bundesnachrichtendienstes oder der Aufgaben der Empfänger erforderlich ist.

In der Praxis wird die beschriebene Zweckbindung dem Empfänger durch den Bundesnachrichtendienst in Form einer Kennzeichnung nach Absatz 12 mitgeteilt. Dies stellt die korrekte Weiterverarbeitung beim Empfänger sicher.

Zu Absatz 2

Absatz 2 regelt die Übermittlung von im Rahmen der strategischen Ausland-Fernmeldeaufklärung erhobenen Daten an andere als die in Absatz 1 Genannten zu Zwecken der Unterrichtung der Bundesregierung oder einer Landesregierung. Hierbei ist die strikte Zweckbindung zu beachten: personenbezogene Daten, die ausschließlich mit dem Zweck der politischen Unterrichtung nach § 19 Absatz 1 Nummer 1 gekennzeichnet sind, dürfen an andere als die in Absatz 1 genannten inländische öffentliche Stellen ausschließlich zum Zweck der Unterrichtung der Bundesregierung oder einer Landesregierung übermittelt werden.

Die weiteren Voraussetzungen, um entsprechende Daten an andere inländische öffentliche Stellen übermitteln zu können, unterscheiden sich nach dem Zweck der Übermittlung: Erfolgt die Übermittlung ausschließlich zum Zweck der Unterrichtung der Bundesregierung oder einer Landesregierung, richtet sich die Übermittlung nach Absatz 2 und setzt voraus, dass tatsächliche Anhaltspunkte dafür bestehen, dass die Datenübermittlung zur Erfüllung der Aufgaben des Bundesnachrichtendienstes oder der Aufgaben der Empfänger erforderlich ist. Der Begriff der Unterrichtung dient zur Abgrenzung von exekutiven

Folgemaßnahmen gegen den Betroffenen, wie sie typischerweise im Rahmen der Gefahrenabwehr und der Strafverfolgung erfolgen. Die Empfänger dürfen die nach Absatz 2 übermittelten Daten grundsätzlich nur zu Zwecken der Unterrichtung weiterverarbeiten; insbesondere können sie die nach Absatz 2 übermittelten Daten für die Erstellung von eigenen Lagebildern nutzen. Ebenso kann sich aus diesen Daten für den Empfänger die abstrakte Erforderlichkeit ergeben, die Schwerpunkte der eigenen Arbeit aufgrund der z.B. erkennbaren politischen Veränderungen in relevanten ausländischen Staaten anzupassen. Sollte sich aus den Daten ein operativer Handlungsbedarf ergeben, greifen die Regelungen über die Zweckänderung und es müssen die Voraussetzungen der Absätze 3 oder 4 vorliegen.

Zu Absatz 3

Absatz 3 regelt die Übermittlung der mit dem Zweck der Gefahrenfrüherkennung gemäß § 19 Absatz 1 Nummer 2 gekennzeichneten personenbezogenen Daten an Strafverfolgungsbehörden. Er gestattet die Übermittlung personenbezogener Daten zur Verfolgung besonders schwerer Straftaten. Gemäß den Vorgaben aus dem Urteil des Bundesverfassungsgerichts vom 19. Mai 2020 erfolgt die nähere Konkretisierung der besonders schweren Straftaten im Rahmen eines enumerativen und abschließenden Straftatenkatalogs (BVerfG, a.a.O., Randnummer 221). Dabei wurde in Anlehnung an die vergleichbare Eingriffsintensität der Straftatenkatalog des § 100b Absatz 2 Strafprozessordnung herangezogen. Zudem ist eine Übermittlung auch zur Verfolgung vorsätzlich begangener Straftaten nach den §§ 17 und 18 des Außenwirtschaftsgesetzes. Diese Straftaten besitzen mit Blick auf den Auftrag des Bundesnachrichtendienstes besondere Relevanz.

Zu Absatz 4

Absatz 4 regelt insbesondere die Übermittlung der mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten an die in Absatz 2 genannten Stellen zum Zweck der Weiterverarbeitung der Daten für Folgemaßnahmen mit unmittelbarer Außenwirkung gegenüber dem Betroffenen, insbesondere der Gefahrenabwehr. Der Empfänger darf die so übermittelten personenbezogenen Daten dementsprechend über den bloßen Unterrichtungszweck nach Absatz 2 hinaus weiterverarbeiten. Es sind also gerade exekutive Folgemaßnahmen möglich, die eine unmittelbare Außenwirkung für den Betroffenen entfalten und diesen daher in besonderem Maße belasten.

Nummer 1

Nummer 1 eröffnet die Möglichkeit zur Datenübermittlung, wenn dies in anderen Rechtsvorschriften für den Bundesnachrichtendienst ausdrücklich vorgesehen ist. Eine vergleichbare Norm findet sich in § 25 Absatz 2 Nummer 1 Bundeskriminalamtgesetz (BKAG). Sie entspricht dem sogenannten Doppeltürmodell des Bundesverfassungsgerichts (BVerfGE 130, 151). Eine solche Übermittlungsbefugnis ist insbesondere 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 Fluggastdatengesetz (FlugDaG) 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 auch Datenübermittlungen des Bundesnachrichtendienstes im Rahmen von

Konsultationsverfahren nach § 73 Abs. 3, 3a, 3b AufenthG, Behördenerklärungen nach § 99 VwGO, Behördenerklärungen zum Zwecke der Gefahrenabwehr an Polizeibehörden, Ausländerämter, Auswärtiges Amt etc. sowie nach dem SÜG. Erfasst sind ferner Datenübermittlungen im Rahmen des Verfahrens nach Art. 36 SIS-II-Beschluss. (Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II)).

Nummer 2

Nummer 2 gestattet die Übermittlung bei dem Vorliegen von tatsächlichen Anhaltspunkten zur Abwehr einer Gefahr für besonders gewichtige Rechtsgüter oder wenn die Übermittlung zur Abwehr einer besonders schwerwiegenden Beeinträchtigung der Rechte Einzelner erforderlich ist. Bei den Rechtsgütern muss es sich um solche handeln, die als gewichtig anzuerkennen sind. Hiermit wird sichergestellt, dass der Eingriff in das Recht auf des Betroffenen aus Art. 10 GG nur durch den Schutz von hinreichend bedeutsamen Rechtsgütern gerechtfertigt wird und somit keine Übermittlungen zum Schutz von für die Allgemeinheit nicht bedeutsamen Rechtsgütern wie Eigentum, Ehre etc. erfolgen. Das Abstellen auf Rechtsgüter und nicht auf Straftatenkataloge, entspricht den Anforderungen, die das Bundesverfassungsgericht in seinem Urteil für einen Eingriff in Artikel 10 GG aufgestellt hat (BVerfG, a.a.O., Randnummer 221). Anknüpfend an ein nachrichtendienstliches Verständnis des Gefahrenbegriffs müssen tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung erforderlich ist zur Abwehr einer Gefahr für besonders gewichtige Rechtsgüter oder zur Abwehr einer besonders schwerwiegenden Beeinträchtigung der Rechte Einzelner. Dies entspricht dem Umstand, dass sich die Zuständigkeit des Bundesnachrichtendienstes im Verhältnis zu anderen Sicherheitsbehörden auf eine zeitlich vorverlagerte Gefahrenverhinderung bezieht.

Zu Absatz 5

Absatz 5 gestattet über Absatz 2 hinaus eine Übermittlung der mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten, an die Bundeswehr zu den dort genannten Zwecken. Er stellt einen Baustein der privilegierten Zusammenarbeit des Bundesnachrichtendienstes als einzigem Auslandsnachrichtendienst der Bundesrepublik Deutschland, dem somit auch die Funktion eines militärischen Nachrichtendienstes zukommt, dar. Dies setzt voraus, dass auch personenbezogene Daten aus der strategischen Ausland-Fernmeldeaufklärung, die für die Aufgabenwahrnehmung der Bundeswehr erforderlich sind, unmittelbar und ohne Zeitverzug zur Auswertung an die Bundeswehr übermittelt werden können.

Bei der Wahrnehmung ihrer Aufgaben Auslandseinsätzen und der Landes- oder Bündnisverteidigung wird die Bundeswehr zum Schutz hochrangiger Rechtsgüter und in einem eng begrenzten Aufgabenbereich auf Grundlage verfassungsunmittelbarer Befugnisnormen sowie – je nach Einzelfall – von Bundestagsmandaten und/oder völkerrechtlichen Rechtsgrundlagen, die auch als nationales Recht gelten, tätig. Die Aufgabenwahrnehmung der Bundeswehr ist insoweit nicht vergleichbar mit der von Strafverfolgungs- oder Gefahrenabwehrbehörden. Dennoch ist bei Datenübermittlungen durch den Bundesnachrichtendienst an die Bundeswehr stets ein enger Bezug zu besonders wichtigen Rechtsgütern (z. B. Leib und Leben von Soldatinnen und Soldaten im Auslandseinsatz oder Sicherstellung der Funktionsfähigkeit der Bundeswehr bzw. von Streitkräften verbündeter Staaten im Rahmen der Landes- oder Bündnisverteidigung) gegeben..

Die Bundeswehr ist insbesondere im Rahmen der „Force Protection“ bei Auslandseinsätzen und deren Vorbereitung, aber auch im Rahmen der anderen in den Ziffern 1. bis 4.

genannten Fälle auf valide und schnelle Datenübermittlung angewiesen. Diese kann in vielen Fällen nur durch einen automatisierten Datenaustausch gewährleistet werden. Daher darf der Bundesnachrichtendienst Daten aus der strategischen Ausland-Fernmeldeaufklärung auch automatisiert an die Bundeswehr übermitteln, wenn sie auf Grundlage von Suchbegriffen erhoben wurden, die strategischen Aufklärungsmaßnahmen nach § 20 Absatz 4 Nummer 1 a) - zur Landes- oder Bündnisverteidigung sowie Auslandseinsätzen der Bundeswehr oder Einsätzen verbündeter Streitkräfte – Nummer 2 a) - Leib, Leben oder Freiheit einer Person oder Nummer 2 b) - Bestand oder Sicherheit des Bundes oder eines Landes, eines Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages – zugeordnet sind. 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.

Datenübermittlungen an die Bundeswehr zu Zwecken der Unterrichtung der Bundesregierung oder einer Landesregierung sind darüber hinaus wie an alle anderen inländischen öffentlichen Stellen unter den Voraussetzungen der Absätze 2 und 7 möglich.

Zu Absatz 6

Absatz 6 gestattet dem Bundesnachrichtendienst eine Übermittlung personenbezogener Daten, die mit dem Zweck der Gefahrenfrüherkennung gekennzeichnet sind, an andere inländische Stellen und orientiert sich an der bisherigen Regelung in § 23 Absatz 2 Satz 1 in Verbindung mit § 19 Absatz 4 Bundesverfassungsschutzgesetz (BVerfSchG). Im Unterschied zu Absatz 1 bis 4 der Norm ist hier der Empfängerkreis auf nicht-öffentliche Stellen erweitert (zum Beispiel nicht-öffentliche Stiftungen, Vereine und Kapitalgesellschaften). Da der Bundesnachrichtendienst im Rahmen seiner Zuständigkeit in der Regel an andere inländische Stellen keine personenbezogenen Daten übermittelt, stellt die Norm einen Ausnahmetatbestand dar. Demensprechend hoch sind die materiellen und formellen Übermittlungshürden.

In formeller Hinsicht ist nach Satz 2 eine vorherige Zustimmung der fachaufsichtführenden Stelle im Bundeskanzleramt einzuholen. Materiell-rechtlich sind die in Satz 1 benannten Rechtsgüter, zu deren Schutz eine Übermittlung zulässig sein soll entsprechend gewichtig und entsprechend den Vorgaben des Bundesverfassungsgerichts, das eine Übermittlung zum Schutz von Rechtsgütern von besonders schweren Gewicht in der Vorgängervorschrift des § 23 Absatz 2 Satz 1 in Verbindung mit § 19 Absatz 4 BVerfSchG für zulässig erachtet hat (BVerfG, a.a.O., Randnummern 174, 313). Satz 3 gestattet ausnahmsweise eine Datenübermittlung an andere inländische Stellen über die Vorgaben in Satz 1 und 2 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 den Betroffenen gering. Der Kritik des Bundesverfassungsgerichts, das bei der Vorgängervorschrift das Fehlen einer Übermittlungsschwelle beanstandet hat (BVerfG, a.a.O., Randnummer 313), wird Rechnung getragen. Eine Übermittlung ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung zur Erreichung der vorgenannten Zwecke erforderlich ist.

Zu Absatz 7

Absatz 7 eröffnet als Ausnahmenvorschrift zu den Absätzen 1 und 2 die Möglichkeit einer Zweckänderung. Liegt der strengen Systematik der Absätze 1 und 2 das Dogma zu Grunde, dass personenbezogene Daten, die ausschließlich zu Zwecken der politischen

Unterrichtung nach § 19 Absatz 1 Nummer 1 erhoben wurden, grundsätzlich nicht für Folgemaßnahmen mit unmittelbarer Außenwirkung für den Betroffenen übermittelt und vom Empfänger genutzt werden dürfen, durchbricht dieser Absatz den Grundsatz: Ausnahmsweise ist eine Übermittlung dieser personenbezogenen Daten und deren Weiternutzung durch den Empfänger auch für Folgemaßnahmen mit unmittelbarer Außenwirkung für den Betroffenen möglich, wenn eine unmittelbar bevorstehende Gefahr für die in dem Absatz aufgezählten essentiellen Schutzgüter von höchster Wichtigkeit abgewendet werden soll. Die verfassungsrechtliche Unbedenklichkeit der Ausnahmvorschrift ergibt sich aus dem Urteil des Bundesverfassungsgerichts, das eine solche Zweckänderung ausdrücklich als zulässig ansieht (BVerfG, a.a.O., Randnummer 228). Bei Gefahr für Leib, Leben oder Freiheit einer Person ist auch eine Übermittlung an andere inländische Stellen zulässig.

Zu Absatz 8

Absatz 8 schützt besonders sensible Daten, die Journalisten, Rechtsanwälten oder Geistlichen in ihrer Funktion als Seelsorger anvertraut wurden und die dem Zeugnisverweigerungsrecht unterfallen würden. 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.

Absatz 9

Absatz 9 regelt die Voraussetzungen für die Übermittlung von personenbezogenen Daten über das Verhalten Minderjähriger an inländische öffentliche Stellen und andere inländische Stellen. Die Regelung dient damit dem Minderjährigenschutz und entspricht der Regelung in § 24 Absatz 1 BVerfSchG, die über den Verweis im bisherigen § 31 bereits aktuell für den Bundesnachrichtendienst entsprechende Anwendung findet. Eine Übermittlung ist danach nur dann zulässig, wenn von dem Minderjährigen selbst eine Gefahr für Leib oder Leben deutscher Staatsangehöriger im Ausland oder für deutsche Einrichtungen im Ausland ausgeht, oder die Gefahr für den Minderjährigen besteht und die Übermittlung dem Schutz des Minderjährigen selbst dient.

Zu Absatz 10

Absatz 10 bündelt die Übermittlungsverbote und Verweigerungsgründe in einem eigenen Absatz. Vergleichbare Regelungen sind über den bisherigen Verweis in § 31 auf § 23 BVerfSchG bereits vorhanden. Diese wurde nur geringfügig angepasst. So hat nach Nummer 1 eine 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. Nummer 2 nennt einer Übermittlung entgegenstehende überwiegende Sicherheitsinteressen als weiteren Grund. Sicherheitsinteressen im Sinne dieser Norm umfassen nicht nur die entsprechenden Interessen des Bundesnachrichtendienstes, sondern sind umfassender zu verstehen. Nach Nummer 3 hat eine Übermittlung auch zu unterbleiben, wenn gesetzliche Weiterverarbeitungsregelungen entgegenstehen. Unberührt davon bleiben jedoch Geheimhaltungspflichten, die sich aus untergesetzlichen Normen ergeben, insbesondere

die jeweils geltende Verschlussanweisung, sowie Regelung des Gesetzes über die internationale Rechtshilfe in Strafsachen.

Zu Absatz 11

Absatz 11 regelt die Verantwortlichkeit für die Zulässigkeit der Übermittlung und weist diese dem Bundesnachrichtendienst zu. Anders ist die Verantwortlichkeit verteilt, wenn der Bundesnachrichtendienst auf ein Ersuchen reagiert. Eine entsprechende Norm findet sich in § 25 Absatz 8 des BKAG und entspricht allgemeinen datenschutzrechtlichen Grundsätzen, die als solche auch der Anwendung anderer Übermittlungsvorschriften zugrunde liegen.

Zu Absatz 12

Absatz 12 schreibt die eine grundsätzliche Zweckfortgeltung, zu der die Daten übermittelt wurden, auch beim Empfänger fest. Der Bundesnachrichtendienst ist verpflichtet, hierauf im Rahmen der Übermittlung hinzuweisen. Mit Zustimmung des BND ist jedoch ausnahmsweise eine Zweckänderung zulässig, wenn dies zum Schutz vergleichbar bedeutsamer Rechtsgüter erfolgt. Danach ist eine Weiterverarbeitung also insbesondere auch für die anderen in § 29 zugelassenen Übermittlungszwecke möglich.

Zu Absatz 13

Absatz 13 setzt die bisherige Regelung des § 31 in Verbindung mit § 25 BVerfSchG fort, indem er dem Empfänger der Daten eine Prüfpflicht auferlegt. Der Empfänger hat zu prüfen, ob die übermittelten Daten für die Erfüllung seiner Aufgaben erforderlich sind. Sollten diese nicht erforderlich sein, hat eine sofortige Löschung der Daten zu erfolgen. Satz 3 macht hiervon unter bestimmten Voraussetzungen eine Ausnahme und schränkt zugleich die Weiterverarbeitung solcher Daten ein.

Zu Absatz 14

Absatz 13 löst den Konflikt zwischen effektiver Arbeitsweise und datenschutzrechtlichen Interessen Unbeteiligter. Er bildet die bisherige Regelung des § 31 in Verbindung mit § 26 BVerfSchG ab.

Zu Absatz 15

Absatz 15 verpflichtet den Bundesnachrichtendienst zur Korrektur, wenn sich Daten nach Übermittlung als berichtigungsbedürftig erweisen und entspricht der bisherigen Regelung in § 31 in Verbindung mit § 26 BVerfSchG.

Zu Absatz 16

Jede Übermittlung erfordert eine Protokollierung unter Vorhaltung spezifischer Informationen. Die Nennung der Empfänger, der Rechtsgrundlage sowie des Zeitpunktes der Übermittlung sind verpflichtend. Dies ermöglicht eine interne und externe datenschutzrechtliche Überprüfung der Übermittlungsvorgänge. Satz 2 gibt einen Aufbewahrungszeitraum sowie eine anschließende Löschpflicht verbindlich vor.

§ 30 (Übermittlung von personenbezogenen Daten aus der strategischen Ausland-Fermeldeaufklärung an ausländische öffentliche Stellen, über- und zwischenstaatliche Stellen sowie andere Stellen)

§ 30 ermöglicht 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 von Informationen an ausländische öffentliche Stellen und über- oder zwischenstaatliche Stellen zur Erfüllung der gesetzlichen Aufgaben des Bundesnachrichtendienstes regelmäßig erforderlich, um im Gegenzug von diesen nachrichtendienstlich relevanten Informationen zu erhalten (nachrichtendienstliches do-ut-des-Prinzip). Dieser nachrichtendienstliche Austausch 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 bearbeiten könnte. In verfassungsrechtlicher Hinsicht kann eine internationale Zusammenarbeit insofern an die internationale Offenheit des Grundgesetzes anknüpfen (vgl. BVerfG, a.a.O., Randnummer 247).

Zu Absatz 1

Absatz 1 regelt die Datenübermittlung an ausländische öffentliche sowie an über- und zwischenstaatliche Stellen. Eine Übermittlung der mit dem Zweck der politischen Unterrichtung gekennzeichneten Daten darf nur zum Zweck der Unterrichtung im Rahmen der internationalen politischen Zusammenarbeit erfolgen. Voraussetzung hierfür ist, dass die Übermittlung zur Aufgabenerfüllung des Bundesnachrichtendienstes erforderlich ist. Aufgrund der strikten Zweckbindung der Weiterverarbeitung durch den Empfänger dürfen auch mit dem Zweck der Gefahrenfrüherkennung gekennzeichnete Daten übermittelt werden, sofern tatsächliche Anhaltspunkte bestehen, dass dies zur Unterrichtung im Rahmen der internationalen politischen Zusammenarbeit erforderlich ist. Der Empfänger darf diese Daten im Rahmen einer Zweckänderung jedoch nur dann für Folgemaßnahmen mit unmittelbarer Außenwirkung für den Betroffenen nutzen, wenn die Voraussetzungen der für eine unmittelbare Übermittlung zum Zweck der Gefahrenabwehr oder Strafverfolgung geltenden Spezialvorschriften in den Absätzen 2 und 3 erfüllt werden.

Zu Absatz 2

Absatz 2 gestattet dem Bundesnachrichtendienst die Übermittlung der mit dem Zweck der Gefahrenfrüherkennung gekennzeichneten personenbezogenen Daten an ausländische öffentliche Stellen sowie über- und zwischenstaatliche Stellen, wenn die Übermittlung der Strafverfolgung dienen soll. Eine solche Übermittlung darf nur erfolgen, wenn die Daten mit dem Zweck der Gefahrenfrüherkennung nach § 19 Absatz 1 Nummer 2 gekennzeichnet sind und wenn tatsächliche Anhaltspunkte dafür bestehen, dass dies erforderlich ist zur Verfolgung von Straftaten, die den in § 29 Absatz 3 genannten Straftaten entsprechen. Die Regelungen des Gesetzes über die internationale Rechtshilfe in Strafsachen bleiben unberührt.

Zu Absatz 3

Eine Übermittlung von personenbezogenen Daten zum Zweck der Weiterverarbeitung für andere als die in Absatz 2 genannten Folgemaßnahmen mit unmittelbarer Außenwirkung für den Betroffenen darf an die in Absatz 1 genannten Empfängerstellen nur aus Daten erfolgen, die mit dem Zweck der Gefahrenfrüherkennung nach § 19 Absatz 1 Nummer 2 gekennzeichnet sind. Die Nummer 2 gestattet eine Übermittlung zur Wahrung erheblicher außen- und sicherheitspolitischer Belange des Bundes oder eines Landes oder bei

Erforderlichkeit für die Sicherheit des Bundes oder eines Landes oder des Empfängerstaates.

Zu Absatz 4

Nach Absatz 4 Satz 1 ist eine Übermittlung von personenbezogenen Daten an andere ausländische Stellen grundsätzlich unzulässig. Eine Ausnahme von diesem Übermittlungsverbot sieht Satz 2 vor, der eine Übermittlung von personenbezogenen Daten an andere ausländische Stellen ermöglicht, wenn Rechtsgüter von besonders schwerem Gewicht betroffen sind. Die Ausnahmetatbestände orientieren sich hierbei an Vorgaben des Bundesverfassungsgerichts (BVerfG, a.a.O., Randnummer 313). Eine weitere Ausnahme vom Grundsatz des Satzes 1 findet sich in Satz 3. Bei Gefahr für Leib, Leben oder Freiheit einer Person ist eine Übermittlung an andere ausländische Stellen zulässig.

Zu Absatz 5

Absatz 5 eröffnet als Ausnahmenvorschrift zu Absatz 1 die Möglichkeit einer Zweckänderung. In Anlehnung an die Regelung in § 29 Absatz 6 ist eine Übermittlung von ausschließlich mit dem Zweck der politischen Unterrichtung nach § 19 Absatz 1 Nummer 1 gekennzeichneten personenbezogenen Daten und deren Weiterverarbeitung durch den Empfänger auch für Folgemaßnahmen mit unmittelbarer Außenwirkung für den Betroffenen nur dann gestattet, wenn eine unmittelbar bevorstehende Gefahr für die in dem Absatz aufgezählten essentiellen Schutzgüter von höchster Wichtigkeit gegeben ist. Auf die Ausführungen zu § 29 Absatz 6 wird verwiesen.

Zu Absatz 6

Absatz 6 enthält Übermittlungsverbote und setzt damit die Vorgaben des Bundesverfassungsgerichts um. Kernelement der Sätze 1 bis 3 ist eine Abwägung zwischen den schutzwürdigen Interessen des Betroffenen und den Interessen der Allgemeinheit an einer Übermittlung der Daten. Eine Übermittlung ist unzulässig, wenn für den Bundesnachrichtendienst erkennbar ist, dass der Empfänger bei der Weiterverarbeitung keine dem Schutz elementarer Menschenrechte angemessenen Garantien gewährleistet oder zu befürchten ist, dass der Empfänger die Daten nicht im Einklang mit grundlegenden rechtstaatlichen Prinzipien verwendet. Der Bundesnachrichtendienst muss bei dieser Prognosebeurteilung auf die bei ihm zu dem Empfänger vorhandenen Erkenntnisse und Erfahrungen mit dem Umgang von personenbezogenen Daten zurückgreifen. Im Zweifelsfall ist die Zusicherung des Empfängers für die Einhaltung eines angemessenen Schutzes der übermittelten Daten nebst einer Prognose durch den Bundesnachrichtendienst, ob Anhaltspunkte dafür bestehen, dass diese nicht eingehalten wird, von maßgeblicher Bedeutung. Die Wahrung von Mindestschutzstandards erfolgt auf diese Weise in Übereinstimmungen mit den Vorgaben des Bundesverfassungsgerichts (BVerfGE, a.a.O., Randnummer 239).

Zu Absatz 7

Absatz 7 bildet die bisher geltende Regelung des § 31 in Verbindung mit § 24 Absatz 2 BVerfSchG ab und bestimmt im Grundsatz, dass personenbezogene Daten Minderjähriger vor Vollendung des 16. Lebensjahres nicht an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen und andere ausländische Stellen übermittelt werden dürfen.

Zu Absatz 8

Absatz 8 trifft in Satz 1 eine eindeutige Aussage zur Verantwortlichkeit des Bundesnachrichtendienstes für Übermittlungsvorgänge. Satz 2 bis 4 statuieren die Pflichten des Empfängers. Dabei ist die in Satz 2 genannte Fortgeltung der Zweckbindung bei der

weiteren Nutzung der personenbezogenen Daten durch den Empfänger von herausgehobener Wichtigkeit. Der Empfänger personenbezogener Daten muss sich nach Satz 3 und 4 auch dazu verpflichten, dem Bundesnachrichtendienst auf Verlangen Auskunft über die Weiterverarbeitung der Daten zu geben. Er muss darüber hinaus nach Satz 5 die verbindliche Zusage abgeben, die übermittelten Daten auf Verlangen des Bundesnachrichtendienstes zu löschen. Diese Verpflichtungen können im Wege von Einzelvereinbarungen bei jeder Übermittlung separat („Disclaimer“ u.a.) oder im Rahmen von generalisierten Vereinbarungen mit dem Empfänger 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 den Empfänger und damit verbunden auf die übermittelten personenbezogenen Daten des Bundesnachrichtendienstes erhalten bleibt. Nur so ist dem Bundesnachrichtendienst eine durch das Bundesverfassungsgericht nachvollziehende Kontrolle möglich (BVerfGE, a.a.O., Randnummer 237). Da eine Übermittlung personenbezogener Daten ins Ausland grundsätzlich ein höheres Gefahrenpotential für den Schutz der Daten birgt, sieht Satz 5 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 flankierenden Maßnahmen setzen diesbezügliche Forderungen des Bundesverfassungsgerichts (BVerfGE, a.a.O., Randnummer 231 ff.) um.

Absatz 9

Absatz 9 erklärt § 29 Absatz 8, 12 bis 16 im Rahmen von Auslandsübermittlungen für entsprechend anwendbar. Auf die dortigen Ausführungen wird verwiesen.

Unterabschnitt 3 (Kooperationen im Rahmen der strategischen Ausland-Fernmeldeaufklärung)

§ 31 Kooperationen mit ausländischen öffentlichen Stellen)

Der Bundesnachrichtendienst ist zur Erfüllung seines Auftrags nach § 1 Absatz 2 Satz 1 auf die Kooperation mit ausländischen Nachrichtendiensten angewiesen. Insbesondere auch infolge der deutschen Mitgliedschaft in der EU und der NATO hat die Bundesrepublik Deutschland eine Verantwortung, sicherheitspolitisch relevante Informationen insbesondere mit anderen EU-Partnern oder NATO-Mitgliedsstaaten zeitnah auszutauschen. Nicht zuletzt aufgrund von beschränkten personellen und finanziellen Ressourcen ist ein Datenaustausch zur gemeinsamen Erkennung von Gefahren für die Bundesrepublik Deutschland von großer Bedeutung. Dies gilt insbesondere auch im Bereich der strategischen Ausland-Fernmeldeaufklärung. Die immer stärkere Vernetzung der Welt mit dem dieser Entwicklung innewohnenden stark steigenden Kommunikationsaufkommen stellt die Fernmeldeaufklärung vor erhebliche Herausforderungen. Angesichts vielfältiger, komplexer Bedrohungen und knapper Ressourcen bietet eine Arbeitsteilung und Zusammenarbeit mit anderen Nachrichtendiensten erhebliche Vorteile für beide Seiten. Kooperationen mit ausländischen Nachrichtendiensten im Sinne einer Lastenaufteilung (sog. „Burden-Sharing“) sind daher unabdingbar. §§ 31 bis 33 treffen für die Kooperation auf dem Gebiet der strategischen Ausland-Fernmeldeaufklärung mit ausländischen öffentlichen Stellen spezielle Regelungen und gehen insoweit den §§ 19 ff. vor. Diese Kooperationen sind nur unter den normierten Voraussetzungen statthaft. Eine Umgehung dieser Vorschriften (sogenannter „Ringtausch“) ist unzulässig.

Der Gesetzgeber ermöglicht dem Bundesnachrichtendienst, die von ihm erhobenen Datenverkehre auch anhand von Suchbegriffen auszuwerten, die von ausländischen Nachrichtendiensten bestimmt werden, und die diesbezüglichen Treffer an diese automatisiert weiterzuleiten. Überdies können Verkehrsdaten auch ohne vorherige Auswertung an die Kooperationspartner weitergeleitet werden. Entsprechend soll umgekehrt der Bundesnachrichtendienst auch Daten und Kapazitäten anderer Dienste nutzen dürfen. Insgesamt sollen so im gegenseitigen Austausch die Datengrundlage für den Einsatz der Suchbegriffe verbreitert und die Kapazitäten effektiver genutzt werden. Zu diesem Zweck hat der Gesetzgeber den Bundesnachrichtendienst mit den bisherigen §§ 13 bis 15 entsprechende Befugnisse erteilt, die vom Bundesverfassungsgericht in seinem Urteil jedoch als nicht verfassungskonform eingestuft wurden.

Das Bundesverfassungsgericht hat in seinem Urteil jedoch anerkannt, dass eine möglichst effektive Zusammenarbeit mit den Sicherheitsbehörden anderer Staaten von besonderer Bedeutung sein kann. Ein funktionierender Informationsaustausch könne im Interesse des verfassungsrechtlich gebotenen Schutzes der Menschen eine Übermittlung von im Inland erhobenen Erkenntnissen voraussetzen und im Gegenzug auf Unterrichtungen durch ausländische Stellen angewiesen sein (vgl. BVerfGE 141, 220, [268]). Entsprechend sei das Grundgesetz für eine Zusammenarbeit des Bundesnachrichtendienstes auch mit anderen Nachrichtendiensten offen. Für die Wahrung der außen- und sicherheitspolitischen Interessen der Bundesrepublik und in diesem Rahmen die Früherkennung von Gefahren könne eine solche internationale Zusammenarbeit von großer Bedeutung sein und an die internationale Offenheit des Grundgesetzes anknüpfen (vgl. auch BVerfGE 143, 101, [152ff.]). Dementsprechend dürfe der Bundesnachrichtendienst auch dazu ermächtigt werden, seine Befugnisse für Erkenntnisinteressen ausländischer Dienste und Staaten zu nutzen. Maßgeblich sei hierbei, dass diese mit einem legitimen Aufklärungsinteresse des Bundesnachrichtendienstes vergleichbar sowie mit den außen- und sicherheitspolitischen Interessen der Bundesrepublik vereinbar seien. Zudem müsse die Datenverwendung in einen rechtsstaatlichen Rahmen eingebunden sein (vgl. a.a.O., Randnummer 247).

Geboten seien Regelungen zum anderen, soweit dem Bundesnachrichtendienst Aufklärungs- und Übermittlungsbefugnisse eingeräumt werden sollen, die er auch im Interesse und unter Anleitung anderer Nachrichtendienste einsetzen kann.

Diesen Vorgaben folgend sind die bereits vor dem aktuellen Urteil des Bundesverfassungsgerichts in der bisherigen Fassung des BNDG vorhandenen Vorschriften zur Kooperation mit ausländischen öffentlichen Stellen im Rahmen der strategischen Ausland-Fernmeldeaufklärung (§§ 14 und 15) grundlegend überarbeitet und an die Vorgaben des Bundesverfassungsgerichts angepasst worden.

Zu Absatz 1

Entsprechende Kooperationen des Bundesnachrichtendienstes sind – unverändert – nur mit solchen ausländischen öffentlichen Stellen zulässig, die nachrichtendienstliche Aufgaben wahrnehmen (Satz 1). Im Rahmen solcher Kooperationen dürfen auch personenbezogene Daten im Rahmen der Vorgaben der §§ 32 und 33 verarbeitet werden.

Daten von deutschen Staatsangehörigen, von inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen, dürfen in diesem Rahmen weder erhoben, noch übermittelt werden (Satz 2). Daher ist nicht nur bei der eigenen technischen Aufklärung des Bundesnachrichtendienstes, sondern auch im Rahmen von entsprechenden Kooperationen sicherzustellen, dass Telekommunikationsdaten von Inländern und deutschen Staatsangehörigen automatisiert ausgefiltert und im Falle einer

erst späteren Identifizierung unverzüglich ausgesondert werden. Dies schließt eine entsprechende Filterung der von den Partnerdiensten übernommenen Suchbegriffe ebenso ein wie die Filterung der für die automatisierte Übermittlung an ausländische Partner vorgesehenen Daten. Umfasst von dieser Filterung sind entsprechende Inhalts- aber auch Verkehrsdaten des in Satz 2 genannten Personenkreises.

Zu Absatz 2

Absatz 2 statuiert, dass die strategische Ausland-Fernmeldeaufklärung auf dem Gebiet der Bundesrepublik Deutschland im Rahmen einer solchen Kooperation nur durch den Bundesnachrichtendienst (und nicht durch die ausländische öffentliche Stelle) erfolgen darf. Eine vergleichbare Regelung war bereits im Rahmen der vorherigen Novellierung des BNDG aufgenommen worden (vgl. den bisherigen § 14 Absatz 3). Die Regelung greift das Petitum des Bundesverfassungsgerichts auf, wonach eine Zusammenarbeit bei der Telekommunikationsüberwachung so gestaltet sein muss, dass der grundrechtliche Schutz gegenüber heimlichen Aufklärungsmaßnahmen und die diesbezüglichen Anforderungen an die Datenverarbeitung nicht unterlaufen werden können. Dies gelte insbesondere für den Schutz vor Inlandsaufklärung, der nicht durch einen freien Austausch mit Erkenntnissen aus auf Deutschland bezogenen Aufklärungsmaßnahmen ausländischer Nachrichtendienste um seine Wirkung gebracht werden darf. Ein solcher „Ringtausch“ wäre insoweit verfassungsrechtlich nicht zulässig (vgl. BVerfG, a.a.O., Randnummer 248). Ausländischen Nachrichtendiensten selbst dürfe die Befugnis zu Aufklärungsmaßnahmen vom Inland aus allenfalls dann eingeräumt oder diesbezüglich eine Duldungszusage erteilt werden, wenn hierzu ein bestimmter Anlass besteht und durch detaillierte Rechtsgrundlagen die uneingeschränkte Geltung des Grundrechtsschutzes materiell-rechtlich und prozedural gesichert ist. Aus der Schutzdimension der Grundrechte folge, dass der deutsche Staat Personen, die im Inland dem Schutz seiner Rechtsordnung unterstehen, vor grundrechtswidrigen Aufklärungsmaßnahmen anderer Staaten schützen muss. Hiervon können auch Kooperationen nicht freistellen (vgl. BVerfG, a.a.O., Randnummer 249). Durch die explizite Regelung im Gesetz wird (erneut) festgeschrieben, dass der Bundesnachrichtendienst für ihn geltende rechtliche Einschränkungen nicht durch ein „Outsourcen“ entsprechender Maßnahmen der Auslandsaufklärung vom Inland aus an eine ausländische öffentliche Stelle umgehen darf. Die Einräumung einer Befugnis zu Aufklärungsmaßnahmen vom Inland aus an ausländische Nachrichtendienste ist daher unverändert nicht vorgesehen und wäre unzulässig.

Zu Absatz 3

In Absatz 3 wird geregelt, in welchen Fällen eine solche Kooperation zulässig ist. Maßgeblich hierfür ist nach Einschätzung des Bundesverfassungsgerichts (vgl. BVerfG, a.a.O., Randnummer 247), dass die Erkenntnisinteressen ausländischer Nachrichtendienste mit einem legitimen Aufklärungsinteresse des Bundesnachrichtendienstes vergleichbar sowie mit den außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland vereinbar sind. Zudem muss die Datenverarbeitung in einen rechtsstaatlichen Rahmen eingebunden sein. Dies ist zum einen der Fall, wenn die Kooperation der Erkennung und Begegnung von erheblichen Gefahren für die innere und äußere Sicherheit der Bundesrepublik Deutschland, die Verteidigung oder das Gemeinwohl dient (Nummer 1). Durch die Begrenzung auf erhebliche Gefahren wird zum Ausdruck gebracht, dass eine Kooperation nur dann eingegangen werden darf, wenn diese einen signifikanten Mehrwert für die vorgenannten Rechtsgüter verspricht.

Darüber hinaus ist eine Kooperation zulässig, wenn sie der Wahrung der außen- und sicherheitspolitischen Handlungsfähigkeit der Bundesrepublik Deutschland dienen soll

(Nummer 2). Die außen- und sicherheitspolitische Handlungsfähigkeit der Bundesregierung und damit einhergehend die Handlungsfähigkeit Deutschlands in der Staatengemeinschaft liegt auch nach Auffassung des Bundesverfassungsgerichts im gesamtstaatlichen Interesse und stellt ein Verfassungsgut von hohem Rang dar (vgl. BVerfG, a.a.O., Randnummer 162). Daher ist es nur folgerichtig, die Gewinnung von Informationen zur Wahrung dieser Handlungsfähigkeit nicht nur mittels eigener Maßnahmen der strategischen Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes, sondern auch im Rahmen von Kooperationen mit ausländischen öffentlichen Stellen zu ermöglichen.

Eine Kooperation kann auch dann eingegangen werden, wenn ohne eine solche die Aufgabenerfüllung des Bundesnachrichtendienstes wesentlich erschwert oder unmöglich würde (Nummer 3). Die Regelung entspricht der Regelung im bisherigen § 13 Absatz 2 Nummer 2.

Zu Absatz 4

Die Kooperationen sind gemäß Vorgabe des Bundesverfassungsgerichts (vgl. BVerfG, a.a.O., Randnummer 253) auf der Grundlage einer formalisierten Festlegung differenzierter Aufklärungsmaßnahmen nach Erkenntnisziel, Gegenstand und Dauer aufzugliedern und verfahrensrechtlich zu strukturieren. Das schließt nach Einschätzung des Bundesverfassungsgerichts die Einbindung solcher gemeinsam durchgeführter Aufklärungsmaßnahmen in eine längerfristige und breite angelegte Zusammenarbeit – gegebenenfalls auf der Grundlage möglicher Rahmenvereinbarungen – nicht aus. Absatz 4 regelt daher, dass vor Abschluss einer Kooperation die Rahmenbedingungen derselben in einer Vereinbarung mit der ausländischen öffentlichen Stelle festzulegen sind. Zwingende Bestandteile dieser Vereinbarung werden in Absatz 4 vorgegeben. So müssen Zweck und Dauer der Kooperation schriftlich festgelegt werden (Nummern 1 und 2). Auch ist eine verbindliche Zusicherung der ausländischen öffentlichen Stelle einzuholen, deren Inhalt in Nummer 3 vorgegeben wird. So muss in der Zusicherung u.a. geregelt werden, dass die im Rahmen der Kooperation erhobenen Daten grundsätzlich nur zu dem Zweck verwendet werden dürfen, zu dem sie erhoben wurden und eine Weitergabe an Dritte grundsätzlich nur mit Zustimmung des Bundesnachrichtendienstes erfolgt darf (Nummer 3 a)). Darüber hinaus muss vereinbart werden, dass Daten aus Telekommunikationsverkehren von deutschen Staatsangehörigen, von inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen, die unbeabsichtigt entgegen § 19 Absatz 7 verarbeitet wurden und von der ausländischen öffentlichen Stelle bei der Datenauswertung als solche erkannt werden, unverzüglich gelöscht werden (Nummer 3 b)). Gleiches gilt für Daten von schutzwürdigen Personen (Nummer 3 c)) sowie für Daten betreffend den Kernbereich privater Lebensgestaltung (Nummer 3 d)). Ebenso muss verpflichtend festgehalten werden, dass die Verwendung der Daten mit grundlegenden rechtstaatlichen Prinzipien vereinbar ist und die Daten insbesondere weder zu politischer Verfolgung noch zu unmenschlicher oder erniedrigender Bestrafung oder Behandlung oder zur Unterdrückung Oppositioneller oder bestimmter Bevölkerungsgruppen eingesetzt werden (Nummer 3 e)). Der Kooperationspartner muss sich ferner bereit erklären, auf Ersuchen des Bundesnachrichtendienstes Auskunft über die vorgenommene Verwendung der Daten zu erteilen (Nummer 3 f)) sowie eine verbindliche Zusicherung abgeben, einer Löschungsaufforderung des Bundesnachrichtendienstes Folge zu leisten (Nummer 3 g)). Im Falle einer Kooperation mit dem Ziel der Datenübermittlung von Verkehrsdaten nach § 33 ist in die Vereinbarung ferner eine verbindliche Zusage des Kooperationspartners aufzunehmen, dass die Verkehrsdaten nicht über einen längeren Zeitraum als sechs Monate bevorratend gespeichert werden (Nummer 3 h)). Für jede der gemeinsam durchgeführten Kooperationen sind die vorgenannten

verbindlichen Zusicherungen jeweils einmal sicherzustellen. Soweit es im Laufe der Zusammenarbeit hierfür Anlass gibt, ist die Vereinbarung zu aktualisieren.

Zu Absatz 5

Eine strategische Auslands-Fernmeldeaufklärung im Zusammenwirken des Bundesnachrichtendienstes mit ausländischen Nachrichtendiensten ist nur zum Schutz hochrangiger Rechtsgüter zulässig (vgl. BVerfG, a.a.O., Randnummer. 253). In Absatz 5 werden in Form von Regelbeispielen die Zwecke, die dem Schutz solcher hochrangigen Rechtsgüter dienen sollen, aufgeführt. So ist eine Kooperation nur zur Früherkennung der in den Nummern 1 bis 10 genannten sowie vergleichbaren (Nummer 11) Gefahren zulässig. Legitimer Zweck einer solchen Kooperation ist auch die Herstellung oder der Erhalt wesentlicher Fähigkeiten des Bundesnachrichtendienstes oder des Kooperationspartners (Nummer 9). Mittels dieser Regelung sollen Kooperationen ermöglicht werden, in denen Daten ausgetauscht werden, die erforderlich sind, um technische Fähigkeiten des Bundesnachrichtendienstes und des Kooperationspartner im Zusammenhang mit der Fernmeldeaufklärung fortzuentwickeln und an die sich ständig ändernden technischen Rahmenbedingungen der Fernmeldeaufklärung in Zeiten der modernen Digitalisierung anzupassen.

Zu Absatz 6

Absatz 6 regelt die Zustimmungspflicht des Bundeskanzleramtes bei entsprechenden Absichtserklärungen des Bundesnachrichtendienstes mit ausländischen Nachrichtendiensten und entspricht dem bisherigen § 13 Absatz 5.

Zu Absatz 7

Gemäß Absatz 7 sind für einzelne Kooperationszwecke nach Absatz 5 innerhalb solcher Kooperationen Erkenntnisziel und Dauer hinreichend bestimmt schriftlich festzulegen. Dies entspricht einer Vorgabe des Bundesverfassungsgerichts, das eine dezidierte Festlegung der Zwecke als erforderlich erachtet hat. Die Erkenntnisziele dürfen den außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland nicht entgegenstehen. Die schriftliche Festlegung ist dem Bundeskanzleramt zur Kenntnis zu geben.

§ 32 (Verarbeitung von selektierten Daten im Rahmen von Kooperationen)

Zu Absatz 1

Absatz 1 beinhaltet die Befugnis des Bundesnachrichtendienstes, im Rahmen von Kooperationen mit ausländischen Nachrichtendiensten nach § 31 selektierte Inhalts- und Verkehrs- und sonstige Metadaten zu erheben und weiterzuverarbeiten. Eine Spezialregelung für die Verarbeitung von unselektierten – also nicht auf Grundlage von Suchbegriffen erhobenen – Verkehrs- und sonstigen Metadaten enthält § 33 (vgl. Erläuterungen zu § 33), so dass diese Daten vom Anwendungsbereich des § 32 nicht umfasst sind.

Die Erhebung und Verarbeitung von selektierten Daten ist nur zulässig, wenn sie erforderlich ist, um die in der Absichtserklärung mit dem Kooperationspartner vereinbarten Kooperationszwecke zu erreichen. Ferner dürfen bei der Erhebung von Inhaltsdaten nur solche Suchbegriffe verwendet werden, die zur Erreichung der vereinbarten Kooperationszwecke geeignet sind. Dies ist aufgrund einer automatisierten Prüfung der vom Kooperationspartner zur Verfügung gestellten Suchbegriffe durch den Bundesnachrichtendienst festzustellen. Der Kooperationspartner ist verpflichtet, dem Bundesnachrichtendienst für jeden Suchbegriff eine hinreichende Plausibilisierung der Erforderlichkeit und Zulässigkeit der Verwendung des Suchbegriffs im Rahmen der

Kooperation zur Verfügung zu stellen. Die Plausibilisierung erfolgt auf Grundlage vorab mit dem Kooperationspartner definierter weitgehend standardisierter Datenfelder, die als zusätzliche Information zum Suchbegriff übermittelt werden. Auf dieser Grundlage führt der Bundesnachrichtendienst dann die vorgenannte Prüfung durch. Sofern die vom Kooperationspartner zur Verfügung gestellten Datenfelder nicht ausreichen, um diese Prüfung durchzuführen, erfolgt keine Verwendung der Suchbegriffe (nähere Aussagen zu Umfang und Inhalt der Prüfung erfolgen unter Absatz 3). Dieses Verfahren wird bereits aktuell im Bundesnachrichtendienst praktiziert (vgl. auch BVerfG, a.a.O., Randnummer 256). Die Plausibilitätsprüfung basiert auf dem Grundgedanken gegenseitigen Vertrauens auf die Einhaltung der im Rahmen der Kooperation vereinbarten Regelungen. Eine fachliche Prüfung der Richtigkeit der Suchbegriffe, deren tatsächliche Erforderlichkeit für die Aufgabenerfüllung des Kooperationspartners oder deren Zuordnung zu bestimmten Zielen ist dem Bundesnachrichtendienst nicht möglich. Der Bundesnachrichtendienst ist gehalten, sich um eine optimale automatisierte Filterung zu bemühen und diese stets weiterzuentwickeln, vgl. hierzu auch Absatz 5. Insbesondere Daten, die den Kernbereich privater Lebensgestaltung betreffen, sind jedoch regelmäßig nur im Rahmen der manuellen Stichproben nach Absatz 7 erkennbar, da sich entsprechende Erkenntnisse erst aus dem Inhalt der erhobenen Daten ergeben. Sofern solche kernbereichsrelevanten Daten erkannt werden, unterliegen sie der unverzüglichen Löschung (vgl. § 22).

Die Verarbeitung der Daten muss ferner im Einklang mit den außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland stehen. Auch dies ist im Rahmen der Prüfung der Suchbegriffe zu berücksichtigen. Suchbegriffe, bei denen Zweifel an der Vereinbarkeit mit den außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland bestehen, dürften nicht verwendet werden. Dies ist zum Beispiel der Fall, wenn der Kooperationspartner Suchbegriffe verwendet, die menschlichen Quellen des Bundesnachrichtendienstes zugeordnet sind.

Im Übrigen gelten bei der Prüfung der vom Kooperationspartner zur Verfügung gestellten Suchbegriffe die gleichen Vorgaben wie für die Verwendung eigener Suchbegriffe des Bundesnachrichtendienstes. Daher gelten die Vorgaben für eine Verarbeitung von Inhaltsdaten durch den Bundesnachrichtendienst außerhalb von Kooperationen. So finden die diesbezüglichen Regelungen in § 19 Absatz 7 (Unzulässigkeit der Verarbeitung von Telekommunikationsverkehren von deutschen Staatsangehörigen, von inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen), § 19 Absatz 9 (Verbot der Wirtschaftsspionage), § 20 Absatz 1 (Schutz von Einrichtungen der Europäischen Union, von öffentlichen Stellen ihrer Mitgliedstaaten oder von Unionsbürgerinnen oder Unionsbürgern), § 21 Absatz 1 und 2 (Schutz von Vertraulichkeitsbeziehungen) und § 22 (Kernbereichsschutz) entsprechende Anwendung.

Zu Absatz 2

Absatz 2 greift die Forderung des Bundesverfassungsgerichts auf, wonach der Gesetzgeber Regeln schaffen muss, die die grundrechtliche Verantwortung des Bundesnachrichtendienstes für die von ihm erhobenen Daten und deren Verarbeitung sicherstellen (vgl. BVerfG, a.a.O., Randnummer 254). Daher wird die Verantwortung für die Zulässigkeit der Kooperation dem Bundesnachrichtendienst auferlegt. Sofern Anhaltspunkte dafür bestehen, dass der Kooperationspartner die abgegebenen Zusicherungen oder Absprachen nicht einhält, hat der Bundesnachrichtendienst gegenüber dem Kooperationspartner auf eine Einhaltung dieser Zusagen hinzuwirken und erforderlichenfalls die Kooperation zu beenden.

Zu Absatz 3

Absatz 3 gestattet dem Bundesnachrichtendienst eine automatisierte Übermittlung der im Rahmen der Kooperation auf Grundlage der vom Kooperationspartner zur Verfügung gestellten Suchbegriffe erhobenen Daten an den Kooperationspartner. Eine solche automatisierte Übermittlung ist jedoch nur dann zulässig, wenn sowohl die Verwendung der vom Kooperationspartner zur Verfügung gestellten Suchbegriffe als auch die auf Grundlage dieser Suchbegriffe erhobenen Daten keinen rechtlichen Bedenken unterliegen. Im Rahmen dieser Prüfung ist zunächst zu prüfen, ob die Ausrichtung dieser Suchbegriffe an den Kooperationszielen und -inhalten mittels der dem Bundesnachrichtendienst zur Verfügung gestellten Angaben ausreichend plausibel gemacht wird. Auch dürfen weder tatsächliche Anhaltspunkte dafür bestehen, dass durch die Verwendung der Suchbegriffe Erkenntnisse auf dem Kernbereich privater Lebensgestaltung erlangt werden, noch dass in unzulässiger Weise Suchbegriffe einer besonders schutzwürdigen Person verwendet werden.

Zu Absatz 4

Die auf Grundlage dieser Suchbegriffe erhobenen Daten sind vor Übermittlung an den Kooperationspartner einer automatisierten Prüfung zu unterziehen. Hierbei wird insbesondere geprüft, ob Daten aus Telekommunikationsverkehren von deutschen Staatsangehörigen, von inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen erhoben wurden. Auch ist zu prüfen, ob der Übermittlung der erhobenen Daten nationale Interessen der Bundesrepublik Deutschland entgegenstehen. Soweit dies der Fall ist, sind die Daten jeweils nicht zu übermitteln. Gleiches gilt, falls im Rahmen der automatisierten Prüfung erkannt wird, dass Daten erhoben werden, die zum Kernbereich privater Lebensgestaltung gehören oder einer besonders schutzwürdigen Person nach § 21 zuzuordnen sind, sofern nicht die Voraussetzungen des § 21 Absatz 2 vorliegen und der Unabhängige Kontrollrat der Datenübermittlung zugestimmt hat. Der Bundesnachrichtendienst ist gehalten, eine optimale automatisierte Filterung sicherzustellen und diese stets weiterzuentwickeln, vgl. auch Absatz 5. Insbesondere Daten, die den Kernbereich privater Lebensgestaltung betreffen, sind jedoch trotz entsprechender Bemühungen des Bundesnachrichtendienstes regelmäßig nur im Rahmen der manuellen Stichproben nach Absatz 7 erkennbar (vgl. auch Ausführungen zu Absatz 1).

Zu Absatz 5

Das Bundesverfassungsgericht hat gefordert, dem Bundesnachrichtendienst gesetzlich aufzugeben, unter Nutzung der Ergebnisse und Erfahrungen seiner Arbeit etwaige Hinweise auf eine besondere Schutzwürdigkeit und Schutzbedürftigkeit bestimmter Personen zu sammeln und auf sie bezogene Suchbegriffe in einer Weise zusammenzuführen, die die Filterung der Suchbegriffe und der für die Übermittlung vorgesehenen Daten ermöglicht (vgl. BVerfG, a.a.O., Randnummer 258). Die diesbezüglichen Datenbanken und Filterverfahren seien kontinuierlich zu aktualisieren und fortzuentwickeln. Die Regelung in Absatz 5 greift diese Forderung auf und verpflichtet den Bundesnachrichtendienst, die bereits vorhandenen Schutzlisten auf Basis bei der Tätigkeit anfallender Erkenntnisse auszuweiten und Verfahren zu entwickeln, mit denen diese routinemäßig aktualisiert und gepflegt werden.

Zu Absatz 6

Die automatisierten Übermittlungen an den Kooperationspartner sind zu protokollieren. Die Protokolldaten unterliegen einer strengen Zweckbindung und dürfen nur zu Kontrollzwecken sowie zur Umsetzung der Löschungsaufforderung aus Absatz 7 Satz 3 verwendet werden. Nach Ablauf der Speicherfrist sind die Daten unverzüglich zu löschen.

Zu Absatz 7

Durch Absatz 7 wird der Bundesnachrichtendienst verpflichtet, das ordnungsgemäße Funktionieren der automatisierten Prüfung nach Absatz 3 und Absatz 4 stichprobenartig unter Aufsicht einer oder eines Bediensteten mit der Befähigung zum Richteramt zu überprüfen. Sofern nachträglich erkannt wird, dass Daten entgegen dieser Vorgaben an den Kooperationspartner übermittelt wurden, ist der Kooperationspartner zur Löschung der Daten aufzufordern. Hiermit wird die Regelung des bisherigen § 15 Absatz 3 aufrechterhalten und eine Forderung des Bundesverfassungsgerichts umgesetzt, das eine Ergänzung der automatisierten Prüfung der Datenübermittlung durch ein manuelles Verfahren gefordert hatte (vgl. BVerfG, a.a.O., Randnummer 258).

Das Bundeskanzleramt ist in Abständen von höchstens sechs Monaten über die Durchführung der Prüfung nach Satz 1 zu unterrichten. Auf diese Weise wird sichergestellt, dass ergänzend zur vorgenannten internen Kontrolle im Bundesnachrichtendienst eine Kontrolle durch die dienst- und fachaufsichtführende Stelle im Bundeskanzleramt erfolgt.

Zu Absatz 8

Die auf Grundlage der Suchbegriffe des Kooperationspartners erhobenen Daten dürfen vom Bundesnachrichtendienst für zwei Wochen gespeichert werden und sind nach Ablauf dieser Frist automatisiert zu löschen.

§ 33 (Weiterverarbeitung von unselektierten Verkehrsdaten im Rahmen von Kooperationen)

Die Schaffung einer eigenen Befugnisnorm für den Austausch von unselektierten Verkehrsdaten geht auf eine Forderung des Bundesverfassungsgerichts zurück. Dieses hatte die Schaffung einer eigenen Regelung als geboten angesehen, soweit im Rahmen von Kooperationen ohne vorangehende Selektion anhand bestimmter Suchbegriffe gesamthaft Verkehrsdaten an ausländische Nachrichtendienste übermittelt werden sollen und vom ausländischen Nachrichtendienst bevorratend gespeichert werden können (vgl. BVerfG, a.a.O., Randnummer 262).

Zu Absatz 1

Eine automatisierte Übermittlung von unselektierten - also nicht auf Grundlage von Suchbegriffen erhobenen - Verkehrsdaten an den Kooperationspartner ist nur dann zulässig, wenn zusätzlich zu den Voraussetzungen des § 31 ein qualifizierter Aufklärungsbedarf vorliegt. Diese Regelung setzt ebenfalls eine Vorgabe des Bundesverfassungsgerichts um, das einen qualifizierten Aufklärungsbedarf im Hinblick auf eine spezifisch konkretisierte Gefahrenlage für derartige Kooperationen gefordert hatte (vgl. BVerfG, a.a.O., Randnummer 263).

Zu Absatz 2

Ein solcher Aufklärungsbedarf setzt nach Auffassung des Bundesverfassungsgerichts voraus, dass über das Bestehen allgemeiner Gefährdungslagen hinaus aufgrund bestimmter Ereignisse Anlass bestehe, durch Aufklärungsmaßnahmen konkreten Bedrohungen entgegenwirken zu können und die Handlungsfähigkeit der Bundesrepublik sicherzustellen. Das könne etwa der Fall sein, wenn tatsächliche Anhaltspunkte für die Vorbereitung terroristischer Anschläge vorliegen, für Verschiebungen von Kriegswaffen auf einer bestimmten Route oder für koordinierte Cyberangriffe gegenüber bestimmten Staaten oder Einrichtungen (vgl. BVerfG, a.a.O., Randnummer 263).

Diesem Petitum folgend, regelt Absatz 2 die Voraussetzungen, die an einen solchen qualifizierten Aufklärungsbedarf zu stellen sind. So ist die automatisierte Übermittlung von Verkehrsdaten im Rahmen einer Kooperation nach Satz 1 nur dann zulässig, wenn die

Übermittlung der Daten erforderlich ist, um konkreten Bedrohungen entgegenzuwirken und die Handlungsfähigkeit der Bundesrepublik Deutschland oder des Kooperationspartners sicherzustellen. Von einer solchen Erforderlichkeit ist insbesondere dann auszugehen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung zum Schutz vor konkreten, gravierenden Bedrohungen erforderlich ist. Hierbei kann auch eine Prognose anhand vergangener Ereignisse maßgeblich sein.

Bedrohungen in diesem Sinne werden in Satz 2 benannt. Neben den bereits vom Bundesverfassungsgericht als zulässig erachteten Bedrohungsszenarien werden auch die Vorbereitung eines bewaffneten Angriffs auf die Bundesrepublik, verbündete Nationen oder den Kooperationspartner, nachrichtendienstliche gesteuerte, auf Destabilisierung angelegter Desinformationskampagnen mit unmittelbarem Bezug zur Bundesrepublik Deutschland oder mit dem Ziel der Vorbereitung oder Durchführung von staatsterroristischen Aktivitäten und die Vorbereitung von Angriffen auf elementarste Rechtsgüter der Allgemeinheit als ausreichend erachtet.

Der qualifizierte Aufklärungsbedarf ist schriftlich zu fixieren. Es findet eine ex ante-Kontrolle durch den Unabhängigen Kontrollrat statt.

Zu Absatz 3

Kooperationen nach § 31, sofern sie die Verarbeitung unselektierter Verkehrsdaten zum Gegenstand haben, bedürfen im dem benannten Fall der Anordnung durch die Präsidentin oder den Präsidenten des Bundesnachrichtendienstes oder eine durch sie oder ihn bestimmte Vertretung.

§ 34 (Eingriff in informationstechnische Systeme von Ausländern im Ausland)

Die Erhebung von Daten aus informationstechnischen Systemen von Ausländern im Ausland ist für die Aufgabenerfüllung des Bundesnachrichtendienstes unverzichtbar und erfolgt – unter Einhaltung des Verhältnismäßigkeitsgrundsatzes sowie strenger formeller Hürden – bereits aktuell. Eine Erweiterung des Tätigkeitsfeldes des Bundesnachrichtendienstes ist daher mit der Regelung in § 34 nicht verbunden. Da das Bundesverfassungsgericht in seinem Urteil zur strategischen Ausland-Fernmeldeaufklärung Maßnahmen der Ausland-Fernmeldeaufklärung gegenüber Ausländern im Ausland als Eingriffe in Artikel 10 GG bewertet hat und in der Folge dezidierte und detaillierte Befugnisnormen fordert, war auch die Rechtspraxis des Bundesnachrichtendienstes bei Eingriffen in informationstechnische Systeme von Ausländern im Ausland zu hinterfragen. Durch die Schaffung einer spezifischen Befugnisnorm für derartige Maßnahmen wird den zu Artikel 10 GG vom Bundesverfassungsgericht getroffenen Aussagen zur Reichweite des Grundrechtsschutzes bei Maßnahmen gegenüber Ausländern im Ausland Rechnung getragen, eine grundrechtskonforme Rechtsgrundlage für entsprechende Maßnahmen geschaffen und die Rechtssicherheit und Rechtsklarheit für entsprechende Maßnahmen des Bundesnachrichtendienstes gefördert.

Parallel zum technologischen Fortschritt im Bereich der Digitalisierung nehmen auch die Möglichkeiten der Verschlüsselung von Kommunikation signifikant zu. Heute stehen hoch komplexe, für den Bundesnachrichtendienst nicht lösbare Verschlüsselungsmethoden und -systeme jedermann zur Verfügung, so dass die Erhebung auftragsrelevanter Daten mit Mitteln der strategischen Ausland-Fernmeldeaufklärung in bestimmten Auftragsfeldern des Bundesnachrichtendienstes nur noch in stark reduziertem Maße möglich ist. Darüber hinaus besteht für den Bundesnachrichtendienst – im Gegensatz zu Inlandssachverhalten

– gegenüber Ausländern im Ausland keine Möglichkeit zur Verpflichtung von ausländischen Telekommunikationsanbietern zur Ausleitung relevanter Kommunikation.

Eingriffe in informationstechnische Systeme ermöglichen im Vergleich zu anderen nachrichtendienstlichen Mitteln die Erlangung zielgenauerer Informationen und leisten daher einen sehr wichtigen Beitrag im Rahmen der Versorgung der Bundesregierung mit besonders wichtigen Informationen zu außen- und sicherheitspolitischen Fragen sowie der Gefahrenfrüherkennung. Für die strategischen außen- und sicherheitspolitischen Entscheidungen der Bundesregierung sind diese Informationen von hoher Wichtigkeit, womit der Einsatz dieses Mittels einem legitimen Zweck dient. Auch können diese Art von Informationen regelmäßig nicht durch ein milderes Mittel gewonnen werden. Die Befugnis zu Eingriffen in informationstechnische Systeme von Ausländern im Ausland ist in der ausgestalteten Form auch im engeren Sinne verhältnismäßig. Die zusätzlichen Anforderungen (Absatz 2 bis 6) an den Einsatz des Mittels schränken den Anwendungsbereich erheblich ein und fokussieren diesen auf das zwingend erforderliche Maß im Rahmen der nachrichtendienstlichen Aufgabenzuweisung des Bundesnachrichtendienstes. Der bei diesen Eingriffen im Inland erforderliche Richtervorbehalt wird für diesen Fall der Auslandsaufklärung durch den Anordnungsvorbehalt nach § 37 in hinreichender Weise ersetzt. Die Regelung in § 34 soll dem Umstand Rechnung tragen, dass – je nach Maßnahme - nicht nur der sachliche Schutzbereich des Rechts auf informationelle Selbstbestimmung oder des Fernmeldegeheimnisses des Artikel 10 GG durch individuelle Aufklärungsmaßnahmen des Bundesnachrichtendienstes betroffen sein kann, sondern darüber hinaus in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nach Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG eingegriffen werden kann. Dieses Grundrecht wirkt im Verhältnis zum Fernmeldegeheimnis und dem Recht auf informationelle Selbstbestimmung subsidiär als Auffanggrundrecht zum Schließen von Schutzlücken.

Aufklärungsfelder, die sich durch die extensive Nutzung von Verschleierungs- und Verschlüsselungstechnologien bei der digitalen Kommunikation auszeichnen, sind zum Beispiel der Phänomenbereich des internationalen Terrorismus und Extremismus. Hier ist zu beobachten, dass relevante terroristische oder extremistische Gefährder bewusst auf die Nutzung von Medien ausweichen, von denen bekannt ist, dass deren Verschlüsselung nicht lösbar ist. Darüber hinaus beschränkt die Zunahme verschlüsselter Kommunikation die Aufklärungsfähigkeiten des Bundesnachrichtendienstes im Ausland auch in anderen Aufklärungsfeldern. So können beispielsweise auch im Bereich der politischen oder militärischen Aufklärung in Einzelfällen relevante Informationen nur über Eingriffe in informationstechnische Systeme im Ausland erlangt werden. Dabei wird im Regelfall nicht in persönliche IT-Endgeräte eingegriffen, die eine Vielzahl privater Informationen beinhalten können (z.B. Smartphone), sondern auf dienstlich genutzte informationstechnische Systeme oder informationstechnische Infrastruktur (Beispiel: Netzwerkelemente einer militärischen Einrichtung in einem Krisenstaat).

Die Befugnis des Bundesnachrichtendienstes zu Eingriffen in informationstechnische Systeme von Ausländern im Ausland ist vor diesem Hintergrund hinsichtlich der Systematik der Erhebungszwecke angelehnt an die Vorgaben des Bundesverfassungsgerichtes zur strategischen Ausland-Fernmeldeaufklärung (vgl. Absätze 2 und 3 der Norm). Die Befugnis zu Eingriffen in informationstechnische Systeme stellt zwar regelmäßig einen Eingriff in das von dem allgemeinen Persönlichkeitsrecht (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG) umfasste Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dar. Für derartige Eingriffe in dieses „IT-Grundrecht“ hat

das BVerfG bei Inlandssachverhalten im Falle der Gefahrenabwehr hohe Schranken gesetzt. Diese hohen Schranken können jedoch im Rahmen der nachrichtendienstlichen Auslandsaufklärung zur Unterrichtung der Bundesregierung oder der Früherkennung von aus dem Ausland ausgehenden Gefahren abgesenkt werden. Die Eingriffsschwellen im Falle der Auslandsaufklärung durch Eingriffe in informationstechnische Systeme können damit im Vergleich zu denen bei vergleichbaren Eingriffen im Inland abgesenkt sein.

Im Vergleich mit Maßnahmen der Ausland-Fernmeldeaufklärung ist aber aufgrund des mit dem Eingriff in informationstechnische Systeme von Ausländern im Ausland einhergehenden höheren Gewichts des Grundrechtseingriffs ein Mehr an Grundrechtsschutz erforderlich. Dem wird durch erhöhte formelle und materielle Hürden Rechnung getragen. Insbesondere sind die Schranken in Bezug auf die Erforderlichkeit des individuellen Eingriffs erhöht (vgl. Absatz 1 Satz 2).

Die Befugnis umfasst neben der laufenden Telekommunikation auch auf dem informationstechnischen Gerät gespeicherte Kommunikations- und sonstige Daten, da deren Auswertung in den oben genannten Szenarien gleichfalls für die Auftragserfüllung des Bundesnachrichtendienstes zwingend notwendig ist. Das wird am Beispiel eines in einem ausländischen militärischen IT-Netzwerk gespeicherten Dokuments deutlich. Das Beispiel verdeutlicht auch, dass der Bundesnachrichtendienst Eingriffe in informationstechnische Systeme regelmäßig nicht zur Erhebung persönlicher Daten individualisierter natürlicher Personen nutzt und diese auch nicht im Fokus stehen, sondern – analog zur Datenerhebung im Rahmen strategischer Aufklärungsmaßnahmen – Personen primär in ihrer beruflichen oder dienstlichen Funktion als Träger relevanter Informationen für die Aufklärung bestimmter Themen oder Regionen relevant sind. Die Person, die das IT-System nutzt, steht als solche regelmäßig nicht im Fokus der Aufklärung. Dem entsprechend sind auch private Daten der Person nicht Ziel des Eingriffs in das informationstechnische System. Soweit Eingriffe in informationstechnische Systeme im Ausnahmefall auf die Erhebung privater Daten von natürlichen Personen abzielen, sind diese in aller Regel dem terroristischen oder extremistischen Umfeld zuzuordnen. Als Beispiel seien hier auf privaten Endgeräten gespeicherte Kontaktlisten und Fotos eines Terroristen oder abgespeicherte extremistische Manifeste genannt.

Zu Absatz 1

Die Befugnis erlaubt Eingriffe in und Datenerhebung aus informationstechnischen Systemen von Ausländern im Ausland. Für die Auftragserfüllung des Bundesnachrichtendienstes ist die Erhebung von Daten aus informationstechnischen Systemen im Ausland unverzichtbar, denn für die Außen- und Sicherheitspolitik der Bundesrepublik bedeutsame Informationen können in bestimmten informationstechnischen Systemen typischerweise in besonders zuverlässiger, authentischer und konzentrierter Qualität gespeichert sein. In dieser Qualität können die Informationen durch Aufklärung mittels menschlicher Quellen nicht gewonnen werden. Die Datenerhebung umfasst die auf dem informationstechnischen System gespeicherten Kommunikations- und sonstigen Daten sowie die laufende Kommunikation.

Die Maßnahme wird dabei – im Gegensatz zur gezielten Datenerhebung im Rahmen strategischer Aufklärungsmaßnahmen - immer „individuell“ angeordnet, d.h. bestimmt oder bestimmbar in Richtung einer oder mehrerer natürlicher oder juristischer Personen oder einer Gruppierung natürlicher oder juristischer Personen im Ausland, die durch einen zugrundeliegenden Sachverhalt miteinander verbunden sind (z.B. eine einzelne Person von besonderem nachrichtendienstlichem Interesse, eine terroristische Organisation und ihre Mitglieder und Unterstützer, ein Unternehmen im Zusammenhang mit der Proliferation von

Massenvernichtungswaffen) oder – soweit vorstehende Personen oder Gruppierungen nicht benannt werden können, da sie nicht konkret bekannt sind – gegen ein informationstechnisches System im Ausland welches eindeutig benannt und identifiziert werden kann. Die Rechtmäßigkeit jeder Anordnung ist vor deren Vollzug durch den Unabhängigen Kontrollrat zu prüfen (vgl. § 37). Die individuelle Anordnung und die Prüfung auf Rechtmäßigkeit durch den Unabhängigen Kontrollrat vor Vollzug tragen dem mit dem Eingriff in informationstechnische Systeme einhergehenden großen Gewicht des Grundrechtseingriffs Rechnung.

Unter „technischen Mitteln“ im Sinne des Absatzes 1 sind informationstechnische nachrichtendienstliche Mittel zu verstehen, die dem heimlichen Aufklären von informationstechnisch erzeugten und verarbeiteten Daten auf einem Zielsystem bzw. in einem Zielbereich ohne oder gegen den Willen der Zielperson oder des Dateninhabers dienen oder eine Teilhabe an solchen Daten ermöglichen. Die zum Einsatz kommenden nachrichtendienstlichen Mittel können nicht abschließend dargestellt werden, da sie einer ständigen technischen Weiterentwicklung unterliegen. Die technischen Anforderungen an diese Mittel werden durch Absatz 4 normiert.

Absatz 1 Satz 2 sieht eine besondere Verhältnismäßigkeitsprüfung vor, bei der der besonderen Gewichtung des Grundrechtseingriffs Rechnung zu tragen ist. Danach darf der Eingriff nur durchgeführt werden, wenn die Erhebung der Daten erforderlich ist, um Daten von besonderer außen- und sicherheitspolitischer Bedeutung zu erheben und zu erwarten wäre, dass der Einsatz anderer nachrichtendienstlicher Mittel keinen oder nicht den gleichen Erfolg gewährleisten würde. Die Begrenzung des Einsatzes dieses Mittels auf Vorgänge von besonderer außen- und sicherheitspolitischer Bedeutung ist aufgrund des mit dem Eingriff in informationstechnische Systeme einhergehenden höheren Gewichts des Grundrechtseingriffs vorgesehen. Es handelt sich hierbei um eine Untermenge der im Auftragsprofil der Bundesregierung benannten Staaten und Themen, mit deren Aufklärung der Bundesnachrichtendienst beauftragt ist, die anhand aktueller politischer Entwicklungen variieren kann. Die Einhaltung dieses qualifizierten Maßstabs wird im Rahmen der Anordnung und der Rechtmäßigkeitsprüfung des Unabhängigen Kontrollrats geprüft.

Zu Absatz 2

Maßnahmen die der politischen Unterrichtung der Bundesregierung dienen, sind nur bei Vorliegen tatsächlicher Anhaltspunkte dafür zulässig, dass sich mit der Maßnahme Daten zu Themen von herausgehobener außen- und sicherheitspolitischer Bedeutung gewinnen lassen, die vom Bundeskanzleramt beauftragt wurden.

Zu Absatz 3

Der grundsätzlich möglichen schwereren Intensität derartiger Eingriffe in informationstechnische Systeme von ausländischen Personen im Ausland im Vergleich zu Eingriffen durch die Ausland-Fernmeldeaufklärung wird darüber hinaus durch eine Anhebung der Eingriffsschwellen Rechnung getragen. So ist die Erhebung von Daten mittels Eingriffs in informationstechnische Systeme von Ausländern im Ausland nur dann zulässig, wenn Tatsachen vorliegen, die den Verdacht rechtfertigen, dass durch sie entsprechende auftragsrelevante Erkenntnisse gewonnen werden können. Tatsächliche Anhaltspunkte sind nicht ausreichend. Darüber hinaus ist eine Datenerhebung nur dann zulässig, wenn durch sie Erkenntnisse von herausgehobener außen- und sicherheitspolitischer Bedeutung über die in § 19 Absatz 4 aufgeführten Gefahrenbereiche bzw. zum Schutz der dort genannten Rechtsgüter gewonnen werden können.

Zu Absatz 4

Absatz 4 schützt die Integrität des informationstechnischen Systems. So dürfen nur unbedingt notwendige Eingriffe erfolgen. Technische Veränderungen sind, soweit technisch möglich, automatisiert rückgängig zu machen. Der Bundesnachrichtendienst wird darüber hinaus verpflichtet, die eingesetzten technischen Mittel nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.

Zu Absatz 5

Soweit die individuelle Aufklärungsmaßnahme zum Zweck der Gefahrenfrüherkennung durchgeführt wird, darf sie sich nur gegen den in Absatz 5 genannten Personenkreis richten: Neben möglichen Gefahrverursachern darf sich die Maßnahme auch gegen Nachrichtenmittler richten, wobei auch die unbewusste oder nicht-willentliche Mitteilung entsprechender Nachrichten umfasst ist. Beispielsweise darf sich die Maßnahme gegen unbekannte Cyber-Angreifer richten, die einen Server infiltriert haben und diesen steuern. Die Maßnahme wird in diesem Fall durch einen Eingriff in den infiltrierten Server umgesetzt.

Die oben dargestellten Einschränkungen der möglichen Ziele der Maßnahme finden ausschließlich auf Maßnahmen mit dem Zweck der Gefahrenfrüherkennung Anwendung. Maßnahmen mit dem Zweck der politischen Unterrichtung der Bundesregierung oder einer Landesregierung sind somit unter Wahrung des Verhältnismäßigkeitsgrundsatzes somit auch gegen andere als die in Absatz 5 genannten Ziele zulässig.

Zu Absatz 6

Absatz 6 berücksichtigt die Tatsache, dass ein Eingriff in ein informationstechnisches System angesichts der vielfachen Sozialbezogenheit dort gespeicherter Daten andere Personen betreffen kann. Die Regelung beschränkt diese Drittbetroffenheit aber auf unvermeidbare und damit sachlich zwingend notwendige Fälle.

Die Drittbetroffenheit in diesem Sinne kann auch im Hinblick auf andere informationstechnische Systeme bestehen, wenn die Maßnahme nicht über einen direkten Eingriff in das relevante informationstechnische System umsetzbar ist, sondern ein technischer Vorschritt notwendig ist. Dies ist beispielsweise der Fall, wenn der Zugriff auf den Server eines extremistischen oder terroristischen Netzwerks erst durch ein Passwort erlangt werden kann, welches zuvor auf dem informationstechnischen System des Netzwerkadministrators erhoben werden muss. Eine Weiterverarbeitung derartiger Daten darf nur in dem zur Umsetzung der Maßnahme zwingend notwendigen Umfang erfolgen und unterliegt der vollumfänglichen Rechtskontrolle des Unabhängigen Kontrollrats.

Die individuelle Aufklärungsmaßnahme darf nur dann erfolgen, wenn der mit ihr verfolgte Zweck nicht erkennbar außer Verhältnis zum Nachteil für den oder die Betroffenen steht (Satz 2). Es wird ferner in Satz 3 auf die Regelungen zur Ausfilterung von Telekommunikationsverkehren von deutschen Staatsangehörigen, von inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen in § 19 Absatz 7 verwiesen, wobei anstelle der in § 19 Absatz 7 Satz 7 statuierten Pflicht zur Unterrichtung der G 10-Kommission bei Verstößen gegen die Pflicht zur unverzüglichen Löschung, die Unterrichtung des Unabhängigen Kontrollrats tritt. Dieser ist auch für Entscheidungen nach § 55 Absatz 2 zuständig.

Zu Absatz 7

Absatz 7 regelt das Verfahren zur Prüfung der erhobenen Daten auf Erforderlichkeit. Für diese Prüfung sieht Absatz 7 die Möglichkeit vor, mit Zustimmung des Unabhängigen Kontrollrates im Ausnahmefall eine längere Prüfdauer festzulegen. Daten, für die die Prüfung ergibt, dass sie für die in Absatz 1 genannten Zwecke nicht erforderlich sind,

werden unter juristischer Aufsicht unverzüglich gelöscht. Die Löschung ist zu protokollieren, die Protokolldaten unterliegen einer strengen Zweckbindung.

Zu Absatz 8

Absatz 8 regelt die Kennzeichnung der erhobenen Daten unmittelbar nach deren Erhebung. Auf die entsprechenden Erläuterungen zu § 19 Absatz 10 wird verwiesen.

Zu Absatz 9

Absatz 9 ermöglicht als Spezialfall des Absatz 6 längere Zeiträume für die Prüfung der Erforderlichkeit der erhobenen Daten aus informationstechnischen Systemen, die sich im Besitz des Bundesnachrichtendienstes befinden (Asservate), bzw. für Abbilder der darauf befindlichen Daten, die in einer Vielzahl von Fällen im unlesbaren Rohformat gespeichert werden (sogenannte „images“). Zum Auslesen und späteren Auswerten nutzt der Bundesnachrichtendienst kommerziell verfügbare Software-Produkte. Änderungen an diesen Software-Produkten sind aus technischen Gründen nicht möglich. Eine Löschung von mangels nachrichtendienstlicher Relevanz für die Aufgabenerfüllung nicht erforderlichen Inhalten ist auf dem generierten image technisch nicht möglich, ohne es als solches zu zerstören. Daher wird hier der Erforderlichkeitsprüfung ein größerer zeitlicher Rahmen von drei Jahren ab Lesbarmachung der Daten eingeräumt. In Einzelfällen kann der Zeitraum nach Maßgabe des Unabhängigen Kontrollrates auch verlängert werden.

§ 35 (Schutz von Vertraulichkeitsbeziehungen)

Mit der Regelung wird analog zur Datenerhebung im Rahmen strategischer Aufklärungsmaßnahmen (vgl. § 21) der besonderen Schutzbedürftigkeit von Vertraulichkeitsbeziehungen insbesondere Journalistinnen und Journalisten, Rechtsanwältinnen und Rechtsanwälten sowie Geistlichen Rechnung getragen werden. Die Ausführungen zu § 21 gelten auch hier.

§ 36 (Kernbereichsschutz)

Auch im Rahmen von individuellen Aufklärungsmaßnahmen ist dem Schutz des Kernbereichs privater Lebensgestaltung Rechnung zu tragen. § 36 sieht – analog zu § 22 bei strategischen Aufklärungsmaßnahmen – zum Kernbereichsschutz im Bereich der Fernmeldeaufklärung ein zweistufiges Schutzkonzept vor, um den Betroffenen vor Eingriffen in den absolut geschützten Kernbereich privater Lebensgestaltung zu bewahren. Die zu § 22 getroffenen Aussagen gelten auch hier.

§ 37 (Anordnung)

Zu Absatz 1

Individuelle Aufklärungsmaßnahmen sind durch die Präsidentin oder den Präsidenten des Bundesnachrichtendienstes oder durch eine durch sie oder ihn bestimmte Vertretung anzuordnen. Vor Vollzug der Anordnung wird deren Rechtmäßigkeit durch den Unabhängigen Kontrollrat geprüft. Die Möglichkeit des Vollzugs der Anordnung nach vorläufiger Bestätigung der Rechtmäßigkeit durch ein Mitglied des Unabhängigen Kontrollrats ist vorgesehen, wenn die Gefahr besteht, dass das Ziel der Maßnahme durch die Verzögerung aufgrund des Prüferfahrens ansonsten vereitelt oder wesentlich erschwert wird. Sofern eine Anordnung nach vorläufiger Bestätigung der Rechtmäßigkeit durch ein Mitglied des Unabhängigen Kontrollrats vollzogen wurde und im Anschluss durch den Unabhängigen Kontrollrat für rechtswidrig erklärt wird, sind die aufgrund der Anordnung bereits erhobenen personenbezogenen Daten unverzüglich zu löschen.

Zu Absatz 2

Absatz 2 enthält Angaben zu Form und Inhalt der Anordnung nach Absatz 1.

Zu Absatz 3

Absatz 3 enthält eine Befristungsregelung für Anordnung nach Absatz 1. Verlängerungen der Anordnung sind – auch mehrfach – zulässig, wenn deren materielle Voraussetzungen weiterhin vorliegen.

Zu Absatz 4

Absatz 4 statuiert Unterrichtungspflichten des Bundesnachrichtendienstes gegenüber dem Bundeskanzleramt. Das Bundeskanzleramt unterrichtet das parlamentarische Kontrollgremium jährlich über die Anzahl der getroffenen Anordnungen nach Absatz 1.

§ 38 (Übermittlung von personenbezogenen Daten aus individuellen Aufklärungsmaßnahmen an inländische öffentliche Stellen und andere inländische Stellen)

§ 38 dient als spezielle und damit abschließende Übermittlungsnorm für personenbezogene Daten, die nach § 34 erhoben wurden und an inländische Stellen übermittelt werden. Der mit der Erhebung der Daten teilweise einhergehende und durch die Übermittlung perpetuierte Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nach Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG erfordert auch gegenüber den bereits erhöhten Schwellen der §§ 29 ff. ein eigenes Übermittlungsregime, das der Eingriffsschwere vor dem Hintergrund des Verhältnismäßigkeitsgrundsatzes Rechnung trägt.

Zu Absatz 1

Die Regelung in Absatz 1 findet ihre Entsprechung in § 29 Absatz 1. Die dortigen Ausführungen gelten entsprechend.

Zu Absatz 2

Die Regelung in Absatz 2 findet ihre Entsprechung in § 29 Absatz 2. Die dortigen Ausführungen gelten entsprechend.

Zu Absatz 3

Der Absatz 3 ist in seinem Aufbau weitgehend an § 29 Absatz 3 angelehnt, die Übermittlungsschwelle ist erhöht („Tatsachen, die die Annahme rechtfertigen“ statt „tatsächliche Anhaltspunkte“). Diese Differenzierung entspricht den Vorgaben des Bundesverfassungsgerichts bezogen auf den Schutz des Artikel 10 Absatz 1 GG und wird hier auch auf die Übermittlungssystematik im Hinblick auf personenbezogene Daten aus einem möglichen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nach Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG übertragen.

Zu Absatz 4

Der Absatz 4 ist in seinem Aufbau weitgehend an § 29 Absatz 4 angelehnt. Die Übermittlungsschwelle ist jedoch in dem in Absatz 3 ausgeführten Sinne erhöht.

Zu Absatz 5

Absatz 5 regelt die Datenübermittlung an die Bundeswehr und ist in seinem Aufbau weitgehend an § 29 Absatz 5 angelehnt. Auf die dortigen Ausführungen wird verwiesen.

Zu Absatz 6

Absatz 6 erklärt für Übermittlungen von personenbezogenen Daten an andere inländische Stellen § 29 Absatz 6 für entsprechend anwendbar. Die dortigen Ausführungen gelten entsprechend.

Zu Absatz 7

Eine Übermittlung der nach Absatz 1 erhobenen und ausschließlich mit dem Zweck der politischen Unterrichtung der Bundesregierung gekennzeichneten personenbezogenen Daten an inländische öffentliche Stellen ist über Absatz 1 und 2 hinaus zum Schutz elementarer Rechtsgüter zulässig. Bei Gefahr für Leib, Leben oder Freiheit einer Person ist eine Übermittlung an andere inländische Stellen zulässig.

Zu Absatz 8

Absatz 8 erklärt für Übermittlungen nach Absatz 1 bis 7 § 29 Absatz 8 bis 16 für entsprechend anwendbar. Die dortigen Ausführungen gelten entsprechend.

§ 39 (Übermittlung von personenbezogenen Daten aus individuellen Aufklärungsmaßnahmen an ausländische öffentliche Stellen, über- und zwischenstaatliche Stellen sowie an andere ausländische Stellen)

Zu Absatz 1

Die Regelung in Absatz 1 findet ihre Entsprechung in § 30 Absatz 1. Die dortigen Ausführungen gelten entsprechend.

Zu Absatz 2

Absatz 2 entspricht weitgehend § 30 Absatz 2. Die dortigen Ausführungen gelten entsprechend.

Zu Absatz 3

Absatz 3 entspricht weitgehend § 30 Absatz 3. Insoweit wird auf die dortigen Ausführungen verwiesen. Vor dem Hintergrund der grundrechtsintensiven Erlangung der personenbezogenen Daten, die in das Ausland zu Folgemaßnahmen mit unmittelbarer Außenwirkung für den Betroffenen übermittelt werden, sieht Satz 2 eine zusätzliche formelle Hürde vor: Die im Rahmen des Satz 1 anzustellende Erforderlichkeitsprüfung hat unter Aufsicht eines Bediensteten des Bundesnachrichtendienstes zu erfolgen, der die Befähigung zum Richteramt hat. Hierdurch soll ein entsprechendes juristisches Niveau im Rahmen der zu treffenden Übermittlungsentscheidung gesichert werden.

Zu Absatz 4

Eine Übermittlung der ausschließlich mit dem Zweck der politischen Unterrichtung der Bundesregierung gekennzeichneten personenbezogenen Daten ist über Absatz 1 hinaus zum Schutz elementarer Rechtsgüter zulässig. Auf die Ausführungen zum gleichlautenden § 30 Absatz 5 wird verwiesen

Zu Absatz 5

Absatz 5 erklärt für Übermittlungen an andere ausländische Stellen die Regelungen in § 30 Absatz 4 und Absatz 5 Satz 2 für entsprechend anwendbar. Die dortigen Ausführungen gelten entsprechend.

Zu Absatz 6

Absatz 6 erklärt für Übermittlungen nach den Absätzen 1 bis 5 den § 30 Absatz 6 bis 9 für entsprechend anwendbar.

Unterabschnitt 5 (Unabhängige Rechtskontrolle)

Wesentliches Strukturmerkmal des demokratischen Rechtsstaats und der hiermit einhergehenden Bindung der Exekutive an Recht und Gesetz ist die Kontrolle behördlichen Handelns. Kontrolle dient der Legitimation exekutiven Handelns. Kontrolle findet dabei auf mehreren Ebenen statt: Neben behördeninternen Kontrollinstrumenten, z. B. in Anordnungs- und Genehmigungsverfahren besteht innerhalb der Exekutive die Fach- und Dienstaufsicht mit einem weit gefassten Instrumentarium. Daneben findet im Bereich der Nachrichtendienste des Bundes spezifische Kontrolle durch das Parlamentarische Kontrollgremium, G 10-Kommission, das Vertrauensgremium, die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und den Bundesrechnungshof statt. Das Gesamtsystem der Kontrolle über die Nachrichtendienste des Bundes ist in den letzten Jahren zum Teil erheblich ausgebaut worden.

Im Falle der Nachrichtendienste, deren Arbeit wegen der verdeckten Sammlung von Informationen und des Einsatzes nachrichtendienstlicher Mittel in die Grundrechte der Betroffenen eingreifen kann, kommt der Kontrolle eine besonders wichtige, weil vertrauensstiftende Rolle zu. Vertrauen in die Lauterkeit und Gesetzmäßigkeit der meist klandestinen Tätigkeit der Dienste kann aber nur entstehen und gefestigt werden, wenn die vorgesehenen Kontrollinstrumente effektiv sind und die Kontrollinstanz mit ausreichenden Kompetenzen ausgestattet ist (BT-Drs. 16/12411, Seite 7).

Dabei ist zu berücksichtigen, dass die für die Arbeit eines Nachrichtendienstes unerlässliche Geheimhaltung im parlamentarisch-politischen Umfeld faktischen Grenzen unterliegt. (BVerfG, a.a.O., Randnummer 298) Die Einrichtung eines neuen Organs zur Kontrolle der technischen Aufklärung des Bundesnachrichtendienstes trägt beiden Gesichtspunkten Rechnung: Über die Wahl der Mitglieder durch sowie umfassende Berichtspflichten an das Parlament in Gestalt des Parlamentarischen Kontrollgremiums findet eine demokratische Legitimation statt. Die parlamentarische – politische – Kontrolle wird gewährleistet. Ergänzt wird diese Anbindung an das Parlament durch die festgeschriebene Möglichkeit der Berichtslegung auch an den Deutschen Bundestag. Die spezifischen Bedingungen eines Nachrichtendienstes werden berücksichtigt in Gestalt einer umfassenden Rechtskontrolle in der Sphäre der Exekutive. Durch die Zuordnung zur Exekutive wird eine unabhängige und effektive Kontrolle des Bundesnachrichtendienstes, wie vom Bundesverfassungsgericht gefordert, ermöglicht, die an der sogenannten Third-Party-Rule nicht Halt macht.

§ 40 (Ausübung der unabhängigen Rechtskontrolle)

Zu Absatz 1

Die verfassungsrechtlichen Anforderungen an die Ausgestaltung einer objektivrechtlichen Kontrolle sind in Bezug auf die technische Aufklärung besonders hoch. Mit der Kontrolle wird ein Ausgleich dafür geschaffen, dass hergebrachte rechtsstaatliche Sicherungen nicht bestehen. Die Kontrolle erfüllt mithin zwei Funktionen: sie gleicht das Rechtsschutzdefizit aus, das durch die geringeren individuellen Rechtsschutzmöglichkeiten besteht. Da die technische Aufklärung wegen ihrer Geheimhaltungsbedürftigkeit kaum Auskunfts- und Benachrichtigungspflichten gebietet und deshalb der individuelle Rechtsschutz zurückgenommen ist, wird dies mit der objektivrechtlichen Kontrolle durch den Unabhängigen Kontrollrat kompensiert. Diese Kontrolle schafft weiterhin einen Ausgleich für die im Wesentlichen nur finale Anleitung der Aufklärungsbefugnisse, eine verfahrensmäßige Strukturierung der Handhabung dieser Befugnisse abzusichern. Die objektivrechtliche Kontrolle gewährleistet, dass die Befugnisse des

Bundesnachrichtendienstes verfahrensmäßig rationalisierend auf die gesetzlichen Ziele hin ausgerichtet werden (BVerfG a.a.O., Randnummer 273).

Zu Absatz 2

Die Regelung stellt sicher, dass es zwei verschiedene Arten der Kontrolle (BVerfG, a.a.O., Randnummer 274) bei institutionell klarer Strukturierung innerhalb des einheitlichen Unabhängigen Kontrollrates gibt. Die objektivrechtliche Kontrolltätigkeit ist auf zwei Kontrollorgane aufgeteilt: zum einen das gerichtsähnliche Kontrollorgan mit den sich aus § 42 ergebenden Katalogzuständigkeiten sowie dem Recht aus § 50 Absatz 2 Satz 2 zur Erteilung einzelfallbezogener Prüfaufträge an das administrative Kontrollorgan und zum anderen das administrative Kontrollorgan mit den in § 50 geregelten Zuständigkeiten. Im Zusammenwirken beider Kontrollorgane unter einem Dach werden schnittstellenfrei Kommunikationsflüsse sichergestellt und zwischenbehördliche Abstimmungsprozesse vermieden. Dies trägt zum einen einer effektiven und ganzheitlichen Kontrolle Rechnung. Zum zweiten steht dem Kontrollierten ein einheitliches Organ gegenüber, welches in den hoch sensiblen Bereich der Informationen ausländischer Nachrichtendienste Einsicht nehmen kann. Bereits um die Möglichkeit der Kooperationen weiterhin zu ermöglichen, ist ein solches einheitliches Kontrollorgan essenziell. Denn ausländische Nachrichtendienste werden von Kooperationen Abstand nehmen, wenn ihre Informationen an unterschiedlichen Stellen der Kontrollzuständigkeit unterliegen.

Gerichtet ist die Kontrolle, ob gerichtsähnlich oder administrativ, auf die Prüfung der objektiven Rechtmäßigkeit. Die Entscheidung über die fachlich zweckmäßige Ausübung der Befugnisse im Rahmen der rechtlichen Regelungen bleibt hiervon unberührt (BVerfG, a.a.O., Randnummer 279) und unterliegt keiner Kontrolle durch den Unabhängigen Kontrollrat. Diese Struktur trägt dem Grundsatz des Schutzes des Kernbereichs exekutiver Eigenverantwortung (hierzu m. w. N. BVerfG, 2 BvE 2/15 - Randnummer 119) Rechnung.

§ 41 (Unabhängiger Kontrollrat)

Der Unabhängige Kontrollrat zur Rechtskontrolle der technischen Aufklärung des Bundesnachrichtendienstes (Unabhängiger Kontrollrat) kontrolliert die Rechtmäßigkeit der technischen Aufklärung und damit verbundener Übermittlungen und Kooperationen mit ausländischen Nachrichtendiensten des Bundesnachrichtendienstes. Er stellt eine unabhängige, objektivrechtliche Rechtskontrolle sicher, welche den Prozess der technischen Aufklärung kontinuierlich und als Ganzes in den Blick nimmt. Diese Kontrolle ist auf die Wahrung der Grundrechte der von der technischen Aufklärung Betroffenen ausgerichtet und gilt der Sicherung und praktischen Effektivierung der rechtlichen Grenzen der Aufklärungstätigkeit des Bundesnachrichtendienstes (BVerfG, a.a.O., Randnummer 272). Mit dem Unabhängigen Kontrollrat wird ein einheitliches Kontrollorgan mit institutionell klaren Strukturen (BVerfG, a.a.O., Randnummer 282) geschaffen, welches auf eine wirksame und unabhängige Erfüllung seiner Aufgaben ausgerichtet ist (BVerfG, a.a.O., Randnummer 283). Die beiden Säulen einer umfassenden Kontrolle (§ 40 Absatz 2) der technischen Aufklärung von Ausländern im Ausland durch den Bundesnachrichtendienst gewährleisten die effektive Beachtung des Verhältnismäßigkeitsgrundsatzes in diesem Bereich der Informationsgewinnung durch den Bundesnachrichtendienst. Der Verhältnismäßigkeitsgrundsatz stellt für Überwachungsmaßnahmen Anforderungen an Transparenz, individuellen Rechtsschutz und Kontrolle (vgl. m. w. N. BVerfGE 141, 220, [282 ff.]). In Bezug auf Transparenz und individuellen Rechtsschutz sind diese für die technische Auslandsaufklärung allerdings zurückgenommen. Im Ausgleich hierfür sind dem Verhältnismäßigkeitsgrundsatz besondere Anforderungen an eine unabhängige objektivrechtliche Kontrolle zu entnehmen (vgl. BVerfGE 133, 277, [369]; 141, 220, [284 ff.]). Eingerichtet wird daher eine mit abschließenden Entscheidungsbefugnissen verbundene

gerichtsähnliche Kontrolle durch das gerichtsähnliche Kontrollorgan in Bezug auf die wesentlichen Verfahrensschritte der strategischen Fernmeldeaufklärung. Weiter prüft das administrative Kontrollorgan, auch eigeninitiativ stichprobenmäßig, den gesamten Prozess der Aufklärung auf seine Rechtmäßigkeit hin. Durch die einheitliche Behördenstruktur ist zwischen beiden Säulen ein offener und unmittelbarer Austausch gewährleistet, um dem Gebot einer wirksamen und kohärenten Kontrolle nachzukommen (BVerfGE, a.a.O., Randnummer 297).

Mit dem Unabhängigen Kontrollrat wird das im Jahr 2016 ins Leben gerufene Unabhängige Gremium fortentwickelt. Aus drei Mitgliedern und drei Stellvertretern, die im Nebenamt tätig sind, wird ein gerichtsähnliches Kontrollorgan des Unabhängigen Kontrollrates bestehend aus drei Spruchkörpern mit Mitgliedern im Hauptamt.

Zu Absatz 1

Der Unabhängige Kontrollrat ist eine oberste Bundesbehörde. Die Ausgestaltung als oberste Bundesbehörde trägt den vom Bundesverfassungsgericht geforderten Merkmalen für eine Kontrolle umfassend Rechnung. Sie stellt die Unabhängigkeit der Tätigkeit des Kontrollorgans sicher. Eine auch nur mittelbare Einflussnahme durch eine übergeordnete Behörde wird so ausgeschlossen. Weiterhin trägt diese Behördenstruktur den besonderen Anforderungen an eine Kontrolle der technischen Aufklärung des Bundesnachrichtendienstes Rechnung.

Mit der Ausgestaltung als oberste Bundesbehörde wird die Kontrolle des Bundesnachrichtendienstes in Bezug auf die technische Aufklärung (neben der dienstinternen und der Fach- und Dienstaufsicht durch das Bundeskanzleramt) an die Exekutive angebunden, so dass dafür Sorge getragen ist, dass die Kontrolle nicht durch die sogenannte Third Party Rule behindert wird (BVerfG, a.a.O. Leitsatz 8).

Die Anbindung an die Exekutive muss aber, bereits zur Wahrung ihrer Unabhängigkeit, von einer, wenn auch nur faktischen, Nachordnung Abstand nehmen. Zugleich hat die objektivrechtliche Kontrolle in einem gewissen Abstand zu den Aufgaben der klassischen, ministeriellen Exekutive zu stehen. Dies wird durch die Ausgestaltung als oberste Bundesbehörde in eindeutiger Art und Weise umgesetzt. Durch die Schaffung einer neuen Behörde gegenüber der Angliederung an eine bereits bestehende Behörde übt der Gesetzgeber seinen Gestaltungsspielraum aus (BVerfG, aaO, Randnummer 282). Gleichzeitig wird so in unzweifelhafter Weise gewährleistet, dass weitere Zwecke, denen bereits bestehende Behörden zwangsläufig bereits unterliegen, nicht mit der gewünschten Unabhängigkeit der Kontrolle konfligieren können.

Zu Absatz 2

Die oberste Bundesbehörde Unabhängiger Kontrollrat wird von einer Präsidentin oder einem Präsidenten geleitet. Ihr oder ihm untersteht der Unabhängige Kontrollrat bestehend aus dem gerichtsähnlichen und dem administrativen Kontrollorgan insgesamt. Die Präsidentin oder der Präsident leitet die Verwaltung des Unabhängigen Kontrollrates und übt entsprechend die Dienstaufsicht aus.

Zu Absatz 3

Es handelt sich um eine klarstellende Regelung, da mit der Ausgestaltung des unabhängigen Kontrollrates als oberste Bundesbehörde dessen Unabhängigkeit einhergeht. Dabei bedeutet „unabhängig“, dass es weder eine rechtliche oder Abhängigkeit geben darf, noch, dass wirtschaftlicher, politischer oder sonstiger Druck ausgeübt wird (Brand, in: Bruck/Möller, VVG, 9. Aufl. 2012, § 214 Schlichtungsstelle, Randnummer 11). „Nicht weisungsabhängig“ bedeutet, dass es bei der Ausübung der ihm gesetzlich zugewiesenen Tätigkeit faktisch keinen Beschränkungen und Einflussnahmen von dritter Seite unterworfen ist (Brand, a. a. O.) Der Unabhängige Kontrollrat ist zugleich zur

Unabhängigkeit verpflichtet und darf nicht an anderer Stelle um Weisung ersuchen. Er ist der Exekutive zuzuordnen, sodass die Kontrolltätigkeit nicht an der Anwendung der sogenannten Third Party-Rule zum Halten kommt.

Zu Absatz 4

Der Unabhängige Kontrollrat unterliegt der Haushalts- und Wirtschaftsprüfung durch den Bundesrechnungshof, soweit hierdurch seine Unabhängigkeit nicht beeinträchtigt wird.

Zu Absatz 5

Der Unabhängige Kontrollrat gibt sich unter Berücksichtigung des Geheimschutzes eine Geschäftsordnung und eine Verfahrensordnung. Diese stehen grundsätzlich unter keinem Zustimmungsvorbehalt durch eine weitere Stelle, da hierdurch die Unabhängigkeit des Kontrollrates beeinträchtigt werden könnte. Gleichwohl ist es im Sinne einer transparenten Zusammenarbeit angezeigt, die Position des Bundeskanzleramtes als der Fach- und Dienstaufsicht des Bundesnachrichtendienstes einzuholen. Auf diese Weise kann ein Gleichlauf z.B. sicherheitlicher Standards erreicht werden. Diese weisen beim Bundesnachrichtendienst zum Teil Besonderheiten auf, was Regelungen zur Fernmeldeaufklärung angeht oder auch die Anerkennung von Geheimhaltungsgraden ausländischer Nachrichtendienste. Insoweit wird der Unabhängige Kontrollrat das Bundeskanzleramt vor Beschluss über eine Geschäftsordnung anhören. Die Beschlüsse über eine Geschäftsordnung und eine Verfahrensordnung fassen die Mitglieder des gerichtsähnlichen Kontrollorgans mit der Mehrheit der Stimmen.

Ist die Geschäftsordnung beschlossen, wird das Parlamentarische Kontrollgremium durch den Unabhängigen Kontrollrat hierüber unterrichtet.

Die Verfahrensordnung des Unabhängigen Kontrollrates regelt die Einzelheiten im Verfahrensablauf der Kontrolltätigkeit des Unabhängigen Kontrollrates gegenüber dem Bundesnachrichtendienst. Sowohl die grundsätzliche Ausgestaltung als auch die Detailtiefe der Regelungsmaterie obliegt der unabhängigen Entscheidung des Kontrollrates.

Zu Absatz 6

Die Sitze der Behörde in Berlin und Pullach spiegeln die zu kontrollierende Stelle und berücksichtigen die mit der Handhabung von Verschlussachen verbundenen Erschwernisse bei Verwaltungsabläufen. Die Einrichtung von (auch temporären) Außenstellen bleibt unbenommen.

§ 42 (Zuständigkeit der gerichtsähnlichen Rechtskontrolle)

Die Zuständigkeit des gerichtsähnlichen Kontrollorgans bestimmt sich anhand des gesetzlichen Zuständigkeitskatalogs. Dieser stellt eine gerichtsähnliche Rechtskontrolle der wesentlichen Verfahrensschritte der technischen Aufklärung sicher und versieht diese mit einer abschließenden Entscheidungsbefugnis des gerichtsähnlichen Kontrollorgans.

Zu Absatz 1

Absatz 1 regelt die Kontrolle vor Vollzug.

Nummer 1

Ähnlich dem Richtervorbehalt prüft das gerichtsähnliche Kontrollorgan die Rechtmäßigkeit jeder strategischen Aufklärungsmaßnahme vor deren Vollzug (BVerfG, a.a.O., Randnummer 179 bis 181). Diese objektivrechtliche ex-ante Kontrolle steht am Anfang jedweder Tätigkeit des Bundesnachrichtendienstes bei der technischen Aufklärung und spannt so einen Schirm auf über alle seine aus ihr abgeleiteten Aktivitäten.

Nummer 2

Das gerichtsähnliche Kontrollorgan prüft unterhalb der Ebene der strategischen Aufklärungsmaßnahme die Rechtmäßigkeit der Anordnung von Zielen nach § 23 Absatz 5 vor deren Vollzug, Dies umfasst besonders schützenswerte Personen der nachfolgenden drei Fallgruppen:

- Anordnungen zur gezielten Datenerhebung von Einrichtungen der Europäischen Union oder von öffentliche Stellen der Mitgliedstaaten der Europäischen Union unter den Voraussetzungen des § 20 Absatz 1.
- Anordnungen zur gezielten Datenerhebung zu möglichen Gefahrverursachern unter den Voraussetzungen des § 20 Absatz 2. Die Aufklärung dieser Personen hat eine besondere Intensität, da eine gesteigerte Wahrscheinlichkeit dafür vorliegt, dass es für diese Personen begründet durch die Aufklärung zu belastenden Folgen kommt (vgl. BVerfG, a.a.O., Randnummer 188). Die Prüfung durch das gerichtsähnliche Kontrollorgan ist darauf gerichtet festzustellen, ob die Aufklärung der Person zur Verfolgung des Aufklärungszwecks den Verhältnismäßigkeitsanforderungen genügt. Diese Prüfung stellt mithin einen besonderen Schutzmechanismus für die aufzuklärenden Personen dar.
- Anordnungen zur gezielten Datenerhebung aus Vertraulichkeitsbeziehungen gemäß § 21 Absatz 2 (vgl. BVerfG, a.a.O., Randnummer 194).

Sämtliche weiteren gezielten Datenerhebungen, die nicht der hier statuierten ex-ante-Kontrolle unterworfen sind, unterliegen der Rechtmäßigkeitskontrolle des administrativen Kontrollorgans ex post. Das administrative Kontrollorgan darf mithin jederzeit sämtliche vom Bundesnachrichtendienst genutzte Suchbegriffe – ohne Einschränkung durch die sogenannte Third-Party-Rule – einsehen und prüfen.

Nummer 3

Bei Kooperationen mit ausländischen Nachrichtendiensten, die die automatisierte Übermittlung von unselektierten personenbezogenen Verkehrsdaten zum Gegenstand hat, bedarf es eines qualifizierten Aufklärungsbedarfs. Ob die Festlegung dieses qualifizierten Aufklärungsbedarfs rechtmäßig getroffen wurde, prüft das gerichtsähnliche Kontrollorgan (BVerfG, a.a.O., Randnummer 263). Die Festlegung hierzu erfolgt mittels Zuordnung zu einer konkreten Aufklärungsmaßnahme. Dies kann bereits bei Anordnung der Aufklärungsmaßnahme geschehen, ist aber auch bei bereits bestehenden Anordnungen von Aufklärungsmaßnahmen möglich. Maßgeblich ist insoweit die schriftlich zu erfolgende Zuordnung (vgl. § 33 Absatz 2).

Nummer 4

Das gerichtsähnliche Kontrollorgan entscheidet über die Verwertbarkeit erhobener Daten, zu denen Zweifel bestehen, ob sie dem Kernbereich privater Lebensgestaltung zuzuordnen sind (vgl. BVerfG, a.a.O., Randnummer 207).

Nummer 5

Das gerichtsähnliche Kontrollorgan prüft die Rechtmäßigkeit sämtlicher Datenübermittlungen zu Vertraulichkeitsbeziehungen.

Zu Absatz 2

Absatz 2 regelt die Kontrolle nach Vollzug.

Nummer 1

Stellt der Bundesnachrichtendienst erst bei der Verarbeitung von Daten fest, dass diese aus der Kommunikation innerhalb einer Vertraulichkeitsbeziehung nach § 21 Absatz 1 stammen, so dürfen diese nur bei Vorliegen der materiellen Voraussetzungen des § 21

Absatz 2 verwendet werden. Eine Anordnung als formelle Voraussetzung des Absatzes 2 kann denklöglich in diesen Fällen nicht vorliegen, da zum Zeitpunkt der Datenerhebung nicht bekannt war, dass es sich um eine Vertraulichkeitsbeziehung handelt. Die auf dieser Basis verwendeten Daten sind dem gerichtsähnlichen Kontrollorgan unverzüglich zur Prüfung vorzulegen (BVerfG, a.a.O., Randnummern 195, 278).

Nummer 2

Werden Daten ausschließlich zum Zweck der Information der Bundesregierung erhoben, so ist deren Übermittlung an ausländische Stellen grundsätzlich unzulässig. Eine Übermittlung ist jedoch zulässig, wenn tatsächliche Anhaltspunkte dafür bestehen, diese erforderlich ist zur Verhinderung einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person, für lebenswichtige Güter der Allgemeinheit oder für 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. Die auf diese Weise mit einer Zweckänderung verbundene Übermittlung überprüft das gerichtsähnliche Kontrollorgan (BVerfG, a.a.O., Randnummer 228, 174).

Nummer 3

Das gerichtsähnliche Kontrollorgan prüft die Dienstvorschrift oder die Dienstvorschriften des Bundesnachrichtendienstes, soweit diese Regelungen zur Auswertung von Daten enthalten (BVerfG, a.a.O., Randnummer 192).

Nummer 4

Dem gerichtsähnlichen Kontrollorgan kommt die abschließende Entscheidungsbefugnis über Beanstandungen des administrativen Kontrollorgans zu. Begegnen dem administrativen Kontrollorgan grundlegende Rechtsfragen (BVerfG, a.a.O., Randnummer 276), so ist über die einheitliche Behördenstruktur des Unabhängigen Kontrollrates sichergestellt, dass diese, unabhängig von dem formalisierten Beanstandungsrecht, dem gerichtsähnlichen Kontrollorgan zur Kenntnis gebracht werden können.

Zu Absatz 3

Das gerichtsähnliche Kontrollorgan prüft die Anordnung von allen individuellen Aufklärungsmaßnahmen nach § 34 vor deren Vollzug.

Zu Absatz 4

Absatz 4 regelt die Kontrolle nach Vollzug.

Nummer 1

Stellt der Bundesnachrichtendienst erst bei der Verarbeitung von Daten fest, dass diese aus einer Vertraulichkeitsbeziehung nach § 21 Absatz 1 stammen, so dürfen diese nur bei Vorliegen der materiellen Voraussetzungen des § 35 Absatz 2 verwendet werden. Die auf dieser Basis verwendeten Daten sind dem gerichtsähnlichen Kontrollorgan unverzüglich zur Prüfung vorzulegen.

Nummer 2

Werden Daten ausschließlich zum Zweck der Information der Bundesregierung erhoben, so ist deren Übermittlung an ausländische Stellen grundsätzlich unzulässig. Eine Übermittlung ist jedoch zulässig, wenn tatsächliche Anhaltspunkte dafür bestehen, diese erforderlich ist zur Verhinderung einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person, für lebenswichtige Güter der Allgemeinheit oder für 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. Die auf diese Weise mit einer Zweckänderung verbundene Übermittlung überprüft das gerichtsähnliche Kontrollorgan.

Nummer 3

Dem gerichtsähnlichen Kontrollorgan kommt die abschließende Entscheidungsbefugnis über Beanstandungen des administrativen Kontrollorgans zu. Begegnen dem administrativen Kontrollorgan grundlegende Rechtsfragen, so ist über die einheitliche Behördenstruktur des Unabhängigen Kontrollrates sichergestellt, dass diese, unabhängig von dem formalisierten Beanstandungsrecht, dem gerichtsähnlichen Kontrollorgan zur Kenntnis gebracht werden können.

§ 43 (Besetzung des gerichtsähnlichen Kontrollorgans; Wahl der Mitglieder)

Zu Absatz 1

Das gerichtsähnliche Kontrollorgan besteht aus sechs Mitgliedern.

Nummer 1

Im gerichtsähnlichen Kontrollorgan kommt stets der richterlichen Perspektive ein maßgebliches Gewicht zu und diese ist für eine maßgebliche Zahl der Mitglieder (BVerfGE, a.a.O., Randnummer 286) durch langjährige richterliche Erfahrung am Bundesgerichtshof belegt. Ergänzend kann auch die richterliche Erfahrung in Ansatz gebracht werden, die vor der Wahl zur Richterin oder zum Richter am Bundesgerichtshof gesammelt wurde. In der Regel sollten die Mitglieder mindestens zwanzig Jahre richterlicher Erfahrung mitbringen.

Nummer 2

Neben den Richterinnen und Richtern am Bundesgerichtshof können auch Bundesanwältinnen und Bundesanwälte beim Bundesgerichtshof Mitglied der gerichtsähnlichen Rechtskontrolle werden. Die Beteiligung staatsanwaltlicher Mitglieder in der Kontrolle ermöglicht eine auch ermittelnde Sichtweise, freilich unter dem Blickwinkel nachrichtendienstlicher Tätigkeit. Diese Kombination an Expertise hat sich bereits in der Tätigkeit des Unabhängigen Gremiums etabliert und bewährt, so dass hieran grundsätzlich festgehalten wird. Auch die Bundesanwältinnen und Bundesanwälte sollten als staatsanwaltschaftliche Mitglieder des Unabhängigen Kontrollrates über eine vergleichbar langjährige justizielle Vorerfahrung verfügen wie die richterlichen Mitglieder. Da die Ernennung zur Bundesanwältin oder Bundesanwalt beim Bundesgerichtshof bereits eine entsprechend langjährige staatsanwaltliche Erfahrung voraussetzt, ist eine ausdrückliche langjährige Erfahrung in dem Amt als Bundesanwältin oder Bundesanwalt beim Bundesgerichtshof anders als bei den Richterinnen oder Richtern am Bundesgerichtshof nicht erforderlich.

Zu Absatz 2

Zum Schutz von Sicherheitsbelangen haben sich alle Mitglieder des gerichtsähnlichen Kontrollorgans einer erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlungen zu unterziehen. Der Unabhängige Kontrollrat wird oberste Dienstbehörde im Sinne von § 3 Absatz 1 des Bundesbeamtengesetzes (BBG) sein. Dies folgt aus § 40 Absatz 1 BNDG (neu) in Verbindung mit § 3 Absatz 1 BBG.

Zu Absatz 3

Das Parlamentarische Kontrollgremium wählt die Mitglieder des gerichtsähnlichen Kontrollorgans mit jeweils einfacher Mehrheit. Das Vorschlagsrecht liegt bei der Präsidentin

oder dem Präsidenten des Bundesgerichtshofes für die richterlichen Mitglieder und die Generalbundesanwältin oder dem Generalbundesanwalt für die staatsanwaltlichen Mitglieder. Die Bundesregierung wird über die Vorschläge vor der Wahl in Kenntnis gesetzt. Über die Wahl erfährt das Gesamtorgan seine parlamentarische Legitimation, da die Wahl unter Berücksichtigung der verschiedenen im Parlament vertretenen politischen Richtungen erfolgt. Gleiches gilt hinsichtlich der einzelnen Personen in Bezug auf ihre persönliche Legitimation zur Ausübung der ihnen gesetzlich übertragenen Tätigkeiten. Zugleich trägt die Wahl durch das Parlamentarische Kontrollgremium der Staatsschutzklausel aus Artikel 10 Absatz 2 Satz 2 Grundgesetz Rechnung. Beim Unabhängigen Kontrollrat handelt es sich um ein vom Parlament bestelltes Organ oder Hilfsorgan nach Artikel 10 Absatz 2 Grundgesetz. Es erfolgt eine Entbindung von der grundrechtsfundierten Unterrichtungspflicht (Dreier/Hermes Randnummer 59; Funke/Lüdemann JuS 2008, 780 [784]) gegenüber den Betroffenen von Eingriffen in Artikel 10 Absatz 1 Grundgesetz, da Beschränkung des Artikel 10 Grundgesetz dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes dienen. An die Stelle des Rechtswegs tritt die objektive Rechtskontrolle durch den Unabhängigen Kontrollrat. Naturgemäß gebietet die technische Aufklärung von Ausländern im Ausland wegen ihrer Geheimhaltungsbedürftigkeit nur sehr begrenzte Auskunfts- und Benachrichtigungspflichten (BVerfG, a.a.O., Randnummer 273), wodurch individueller Rechtsschutz schwer zu erlangen ist. Dieses grundrechtliche Defizit kompensiert die umfassende, unabhängige Rechtskontrolle durch den Unabhängigen Kontrollrat.

§ 44 (Rechtsstellung und Ernennung der Mitglieder des gerichtsähnlichen Kontrollorgans)

Zu Absatz 1

Dieses Gesetz begründet für die Mitglieder des Unabhängigen Kontrollrates ein Beamtenverhältnis auf Zeit. Bei Berücksichtigung der hohen Vorgaben, die das Bundesverfassungsgericht an Status und Qualifikation der Mitglieder der gerichtsähnlichen Kontrolle macht, und da nur ein herausgehobener und eng begrenzter Kreis von Personen als Mitglied des gerichtsähnlichen Kontrollorgans in Frage kommt, ist das Beamtenverhältnis auf Zeit das geeignete dienstrechtliche Instrument, um den Bedarfen der entsendenden sowie der aufnehmenden Stellen einerseits und der Mitglieder andererseits zu entsprechen. Das Beamtenverhältnis auf Zeit überlagert für die Dauer der Amtszeit das weitere Dienstverhältnis als Richterin oder Richter oder Beamtin oder Beamten auf Lebenszeit. Dieses ruht. Die Regelungen zum Beamtenverhältnis auf Zeit werden in Anlehnung an die entsprechende Ausgestaltung in dem Gesetz über den Bundesrechnungshof getroffen. Auch hier gelten hohen Anforderungen für die Unabhängigkeit der Dienstausbübung. Auf die Regelungen des Beamtenrechts wird verwiesen, soweit nicht Verweise auf Regelungen im Deutschen Richtergesetz abweichendes vorsehen. Die richtergleiche Unabhängigkeit (BVerfG, a.a.O., Randnummer 282) der Mitglieder des Unabhängigen Kontrollrates, die auch für die Mitglieder, die Bundesanwältin oder Bundesanwalt beim Bundesgerichtshof gilt, wird über Satz 2 herausgestellt.

Zu Absatz 2 und 3

Die Ernennung durch die Bundespräsidentin oder den Bundespräsidenten hebt die besondere Stellung der Mitglieder des gerichtsähnlichen Kontrollorgans hervor. Das Abnehmen des Amtseides durch die Präsidentin oder den Präsidenten des Deutschen Bundestages betont die Unabhängigkeit des Kontrollrates und ist sachgerecht, da es sich

bei dem Unabhängigen Kontrollrat um ein vom Parlament bestelltes Hilfsorgan nach Artikel 10 Absatz 2 Satz 2 Grundgesetz handelt.

Zu Absatz 4

Während die Präsidentin oder der Präsident sowie die Vizepräsidentin oder der Vizepräsident am Unabhängigen Kontrollrat diese Amtsbezeichnungen führen, führen die übrigen Mitglieder des gerichtsähnlichen Kontrollorgans die Amtsbezeichnung „Kontrollbeauftragte beim Unabhängigen Kontrollrat“ oder „Kontrollbeauftragter beim Unabhängigen Kontrollrat“.

§ 45 (Amtszeit der Mitglieder des gerichtsähnlichen Kontrollorgans)

Zu Absatz 1

Die Amtszeit soll zwölf Jahre betragen. Die Dauer der Amtszeit ist gewählt worden, da zur Wahrung der Unabhängigkeit eine Wiederwahl unzulässig ist. Die Unabhängigkeit der Mitglieder darf nicht durch eine Wiederwahlverpflichtung konterkariert werden. Eine zwölfjährige Amtszeit ermöglicht eine aufgrund der herausfordernden Prüfungsmaterie erforderliche, umfassende Einarbeitung und sodann eine die Kontinuität wahrende Fortentwicklung der Kontrolltätigkeit. Den Mitgliedern des gerichtähnlichen Kontrollorgans wird eine konkrete berufliche Perspektive eröffnet.

Zu Absatz 2

Das Beamtenverhältnis auf Zeit der Mitglieder des gerichtsähnlichen Kontrollorgans beginnt mit der Aushändigung der Ernennungsurkunde, wenn nicht in der Urkunde ein späterer Tag bestimmt ist. Auch eine Wirkungsurkunde ist zugelassen.

Zu Absatz 3

Da die Mitglieder des gerichtsähnlichen Kontrollorgans ihre Tätigkeit im Hauptamt ausüben sollen und ein Nebeneinanderbestehen von verschiedenen aktiven Dienstverhältnissen nicht möglich und nicht gewollt ist, scheiden die Betroffenen aus ihrem bisherigen Richteramt aus und deren Rechte und Pflichten aus ihren Dienstverhältnissen ruhen kraft Gesetz mit Ernennung ins Beamtenverhältnis auf Zeit im Unabhängigen Kontrollrat. Satz 2 legt fest, dass grundlegende dienstliche Verpflichtungen wie die Verschwiegenheitspflicht und das Verbot der Annahme von Belohnungen, Geschenken und sonstigen Vorteilen fortbestehen.

Zu Absatz 4

Aufgrund der hohen Anforderungen an die Qualifikationen derjenigen Personen, die zum Mitglied der gerichtsähnlichen Kontrolle gewählt werden und in Anbetracht der Länge der Amtszeit dürfte es sich bei diesen Personen um solche handeln, die aus dem Beamtenverhältnis auf Zeit in den Ruhestand gehen. Anders als im Beamtenrecht ist im Dienstrecht der Richter eine richterliche Tätigkeit nach Erreichen der Regelaltersgrenze aufgrund von § 48 Abs. 2 des deutschen Richtergesetzes nicht möglich. Das Beamtenverhältnis auf Zeit hingegen endet nach zwölf Jahren oder spätestens mit Vollendung des 70. Lebensjahres. Mithin kann diese Tätigkeit auch ausgeübt werden. Wenn eine Richterin oder ein Richter auf Lebenszeit in selbiger Funktion bereits in den Ruhestand getreten ist.

Der Satz folgt der Regelung in § 70 Absatz 2 des Deutschen Richtergesetzes für die wohl wenig praxisrelevanten Fälle, dass das Beamtenverhältnis auf Zeit vor Erreichen der Regelaltersgrenze endet.

Zu Absatz 5

Die Regelung sichert die Kontinuität in der Führung der Amtsgeschäfte bis zur Ernennung einer Nachfolgerin oder eines Nachfolgers.

§ 46 (Besoldung der Mitglieder des gerichtsähnlichen Kontrollorgans)

Zu Absatz 1

Es werden Beginn und Ende des Anspruchs sowie die Höhe der Besoldung durch Angabe der Besoldungsgruppe – B 7 – bestimmt.

Zu Absatz 2

Die Präsidentin oder der Präsident des Unabhängigen Kontrollrates erhält Besoldung aus der Besoldungsgruppe B 9.

§ 47 (Weitere Rechte und Pflichten der Mitglieder des gerichtsähnlichen Kontrollorgans)

Zu Absätze 1 und 2

Für die vom Parlamentarischen Kontrollgremium gewählten Personen gelten die Vorschriften für die Richter an den obersten Gerichtshöfen des Bundes über Unabhängigkeit und Disziplinarmaßnahmen entsprechend. Sie richten ihre Handlungen danach aus, ob diese mit ihrem Amt vereinbar sind. Deren richtergleiche Unabhängigkeit ist besonders zu schützen. Diesem Umstand wird über einen Verweis auf § 4 DRiG Rechnung getragen. In entsprechender Anwendung sind hier die für mit Beamtenverhältnis auf Zeit unvereinbaren Aufgaben aufgeführt. Auch im Rahmen zulässiger Aufgaben ist den Mitgliedern des gerichtsähnlichen Kontrollorgans eine besondere Sensibilität im Hinblick auf Geheimschutzbelange abzuverlangen.

§ 48 (Leitung des Unabhängigen Kontrollrates)

Die Vorschrift regelt die Bestimmung der Leitung des Unabhängigen Kontrollrates durch das Parlamentarische Kontrollgremium. Darüber hinaus werden die Amtsbezeichnungen für die Präsidentin oder den Präsidenten des gerichtsähnlichen Kontrollorgans sowie für die Vizepräsidentin oder Vizepräsidenten des gerichtsähnlichen Kontrollorgans geregelt.

§ 49 (Spruchkörper des gerichtsähnlichen Kontrollorgans; Beschlussfassung)

Das gerichtsähnliche Kontrollorgan besteht aus drei Spruchkörpern; dem Senat sowie zwei Kammern.

Zu Absatz 1

Alle Mitglieder des gerichtsähnlichen Kontrollorgans bilden den Senat des gerichtsähnlichen Kontrollorgans. Vorsitz im Senat führt die Präsidentin oder der Präsident oder, sollte sie oder er nicht im Senat vertreten sein, die Vizepräsidentin oder der Vizepräsident.

Zu Absatz 2

Der Senat beruft zwei Kammern. Jede Kammer besteht aus drei Mitgliedern. Die Mitglieder einer Kammer bestimmen ein richterliches Mitglied als Vorsitzende oder Vorsitzenden. Die Kammer soll nicht länger als zwei Jahre in gleicher Besetzung bestehen. Die weitere Ausgestaltung, z.B. zu den Kammerzuständigkeiten, obliegt der Selbstorganisation des gerichtsähnlichen Kontrollorgans und kann in der Geschäftsordnung des Unabhängigen Kontrollrates verankert werden.

Zu Absatz 3

In allen Spruchkörpern (Senat und Kammern) wird gewährleistet, dass die Mehrzahl der Sitze mit Richterinnen oder Richtern besetzt ist und somit der richterlichen Perspektive, belegt durch langjährige richterliche Erfahrung, ein maßgebliches Gewicht zukommt (BVerfG, a. a. O, Randnummer 286).

Zu Absatz 4

Ein Spruchkörper ist beschlussfähig, wenn die Mehrheit seiner Mitglieder anwesend ist. Damit der richterlichen Perspektive, belegt durch langjährige richterliche Erfahrung, ein maßgebliches Gewicht zukommt (BVerfG, a. a. O, Randnummer 286), ist die Beschlussfähigkeit zusätzlich an die Voraussetzung geknüpft, dass die Richterinnen oder Richter am Bundesgerichtshof mehrheitlich im Spruchkörper vertreten sein müssen. Die Beschlussfassung in den jeweiligen Spruchkörpern des gerichtsähnlichen Kontrollorgans erfolgt sodann mit einfacher Stimmenmehrheit. Bei Stimmengleichheit entscheidet die Stimme der oder des Vorsitzenden. Ist die oder der Vorsitzende verhindert, entscheidet bei Stimmengleichheit die Stimme des richterlichen Mitglieds.

§ 50 (Aufbau und Organisation des administrativen Kontrollorgans)

Dem administrativen Kontrollorgan steht eine Leiterin oder ein Leiter mit der Befähigung zum Richteramt vor. Sie oder er steht in einem Beamtenverhältnis zum Bund und erhält Besoldung in Höhe der Besoldungsgruppe B 4.

§ 51 (Zuständigkeit des administrativen Kontrollorgans)

Der administrative Kontrollkörper ist so auszugestalten, dass dieser eigeninitiativ stichprobenmäßig den gesamten Prozess der technischen Aufklärung von Ausländern im Ausland auf seine Rechtmäßigkeit prüft. Dies umfasst sowohl Einzelentscheidungen und Verfahrensabläufe als auch die Gestaltung der Datenverarbeitung und der Filterprozesse sowie der hierfür verwendeten technischen Hilfsmittel (BVerfG, a.a.O., Randnummer 276). Um die Unabhängigkeit des Kontrollrates sicherzustellen, bleiben Organisation und Arbeitsweise dem Kontrollrat selbst überlassen.

Zu Absatz 1

An die Kontrollzuständigkeiten des gerichtsähnlichen Kontrollorgans fügt sich die Kontrollzuständigkeit des administrativen Kontrollorgans nahtlos an. Beide Säulen der Kontrolle – gerichtsähnlich und administrativ - sind so miteinander verzahnt, dass eine lückenlose Kontrolle der technischen Aufklärung von Ausländern im Ausland durch den Bundesnachrichtendienst möglich wird. Dabei bleibt es dem gerichtsähnlichen Kontrollorgan unbenommen, auf die Expertise des administrativen Kontrollorgans zuzugreifen, um z.B. seine Entscheidungen vorzubereiten. Die konkrete Ausgestaltung der Behördenstruktur bleibt dem Unabhängigen Kontrollrat insoweit selbst überlassen. Soweit im Verfahrensgang der technischen Aufklärung von Ausländern im Ausland eine Zuständigkeit der gerichtsähnlichen Kontrolle nicht gegeben ist, ist die Zuständigkeit des administrativen Kontrollorgans eröffnet. Der gesamte Prozess der technischen Aufklärung wird durch diese komplementäre Zuständigkeitsverteilung potentiell umfassend der Kontrolle durch den Unabhängigen Kontrollrat unterworfen (BVerfG, a.a.O., Randnummer 279). Dem administrativen Kontrollorgan kommt primär eine Beobachterrolle zu; sie begleitet und beurteilt die Prozesse des Bundesnachrichtendienstes und unterzieht diese einer objektiven Rechtmäßigkeitsprüfung. Unberührt hiervon bleibt die Entscheidung über die fachlich zweckmäßige Ausübung der Befugnisse des Bundesnachrichtendienstes im Rahmen der rechtlichen Regelungen.

Zu Absatz 2

Das gerichtsähnliche Kontrollorgan bestimmt die Aufgaben des administrativen Kontrollorgans auf Vorschlag der Leiterin oder des Leiters. Dessen ungeachtet kann das gerichtsähnliche Kontrollorgan das administrative Kontrollorgan mit einzelfallbezogenen Prüfaufträgen beauftragen. Maßgeblich bei der Bestimmung von Aufgaben und Prüfaufträgen ist, dass die technische Aufklärung nach diesem Gesetz insgesamt der objektivrechtlichen Kontrolle unterliegt.

Zu Absatz 3

Dem administrativen Kontrollorgan kommt im Rahmen seiner Prüfständigkeit keine abschließende Entscheidungsbefugnis zu. Stellt es einen rechtswidrigen Zustand fest, kann es dies beanstanden. Die abschließende Entscheidung obliegt dem gerichtsähnlichen Kontrollorgan. Die nähere Ausgestaltung des Beanstandungsverfahrens regelt § 52.

§ 52 (Beanstandungen)

Zu Absatz 1

Stellt das administrative Kontrollorgan einen seiner Überzeugung nach rechtswidrigen Zustand fest, so kann es diesen gegenüber dem Bundesnachrichtendienst beanstanden. Dies kommt infrage, soweit bei der Tätigkeit des administrativen Kontrollorgans strukturelle Probleme erkennbar werden oder anders nicht auszuräumende Differenzen mit dem Bundesnachrichtendienst entstehen (BVerfG, a.a.O., Randnummer 297). Zuvor hat es den Bundesnachrichtendienst anzuhören. Die Entscheidung über die Ausübung des Beanstandungsrechts im Allgemeinen sowie der einzelnen Beanstandungsschritte bis zur Vorlage der Beanstandung zur abschließenden Entscheidung beim gerichtsähnlichen Kontrollorgan trifft das administrative Kontrollorgan nach pflichtgemäßem Ermessen. So kann es von Beanstandungen oder den weiteren Beanstufungsstufen absehen, wenn deren Abhilfe absehbar bevorsteht.

Zu Absatz 2

Hält das administrative Kontrollorgan nach Anhörung des Bundesnachrichtendienstes an der Beanstandung fest, so kann es diese dem Bundeskanzleramt vorlegen. Das Bundeskanzleramt nimmt zur Beanstandung Stellung.

Zu Absatz 3

Hält das administrative Kontrollorgan auch nach Stellungnahme des Bundeskanzleramtes an der Beanstandung fest, so kann es diese dem gerichtsähnlichen Kontrollorgan zur abschließenden Entscheidung vorlegen.

Zu Absatz 4

Das gerichtsähnliche Kontrollorgan hört das Bundeskanzleramt vor seiner Entscheidung zur Sache an. Die Entscheidung des gerichtsähnlichen Kontrollorgans ist für das Bundeskanzleramt und den Bundesnachrichtendienst bindend und in angemessener Frist umzusetzen.

Beanstandungen richtet sie zunächst unter Fristsetzung zur Abhilfe an den Bundesnachrichtendienst und, wenn aus ihrer Sicht der Beanstandung nicht abgeholfen wurde, an das Bundeskanzleramt. Sie sieht von einer Beanstandung ab, wenn dem Mangel abgeholfen wurde oder dieser als unerheblich angesehen werden kann.

§ 53 (Mitarbeiterinnen und Mitarbeiter des Unabhängigen Kontrollrates)

Ebenso wie die Mitglieder des gerichtsähnlichen Kontrollorgans müssen sich alle anderen im Unabhängigen Kontrollrat tätigen Personen der erweiterten Sicherheitsüberprüfung mit

Sicherheitsermittlung unterziehen. Die Mitarbeiterinnen und Mitarbeiter müssen deutsche Staatsangehörige sein.

§ 54 (Geheimhaltung; Aussagegenehmigung)

Zu Absatz 1

Der Unabhängige Kontrollrat ist bei seiner Tätigkeit umfassend dem Geheimschutz verpflichtet. Ausnahmslos alle Beratungen des Unabhängigen Kontrollrates sind geheim.

Zu Absatz 2

Über die aktive Tätigkeit im Unabhängigen Kontrollrat hinaus sind alle Mitglieder und Mitarbeiterinnen und Mitarbeiter zeitlebens zur Geheimhaltung über diejenigen Dinge verpflichtet, die sie bei oder bei Gelegenheit der Tätigkeit zur Kenntnis genommen haben.

Zu Absatz 3

Zuständige Stelle für die Erteilung einer Aussagegenehmigung für Mitglieder und Mitarbeiterinnen und Mitarbeiter ist die Präsidentin oder der Präsident des Unabhängigen Gremiums. Sie oder ihn selbst betreffend entscheidet die Präsidentin oder der Präsident selbst nach pflichtgemäßem Ermessen. In bestimmten herausgehobenen Fällen ist eine Aussagegenehmigung zu versagen. Insoweit enthält die Regelung entsprechende Versagungsgründe, insbesondere das Wohl des Bundes oder eines Landes.

§ 55 (Unterrichtung durch den Unabhängigen Kontrollrat)

Zu Absatz 1

Die Norm regelt die Berichtspflichten des Unabhängigen Kontrollrates gegenüber dem Parlamentarischen Kontrollgremium. Zwischen den Unterrichtungen dürfen nicht mehr als sechs Monate liegen. Dies entspricht der etablierten Berichtspflicht des Unabhängigen Gremiums.

Das Parlamentarische Kontrollgremium ist in der Kontrolllandschaft das zentrale Organ der politischen Kontrolle, in dem die Informationen zusammenlaufen. In Bezug auf den Unabhängigen Kontrollrat wird – neben der herausgehobenen Stellung bei der Wahl der Mitglieder des Unabhängigen Kontrollrates diese zentrale Aufgabe des Parlamentarischen Kontrollgremiums ermöglicht und sichergestellt.

Zu Absatz 2

Die Rahmenbedingungen der Unterrichtung des Parlamentarischen Kontrollgremiums sind in entsprechender Weise gleichlaufend mit den Bedingungen der Kontrolle nach dem Kontrollgremiumgesetz (PKGrG) ausgestaltet, dort insbesondere § 6 PKGrG. Der Geheimschutz ist zudem zu wahren.

Der Unabhängige Kontrollrat hört das Bundeskanzleramt zu seinem vorgesehenen Bericht an. Sollte das Bundeskanzleramt der Auffassung sein, dass sich im Bericht Inhalte befinden, die nicht der alleinigen Verfügungsbefugnis des Bundesnachrichtendienstes unterliegen, so informiert das Bundeskanzleramt den Unabhängigen Kontrollrat hierüber. Auf Verlangen des Unabhängigen Kontrollrates ergreift das Bundeskanzleramt geeignete Maßnahmen, um das Parlamentarische Kontrollgremium über diese Informationen und Gegenstände unterrichten zu dürfen. Diese Regelung trägt dem Umstand Rechnung, dass die Kontrolle des Unabhängigen Kontrollrates an der für die nachrichtendienstlichen Zusammenarbeit essenzielle Third Party Rule nicht halt macht. Dort, wo Informationen die Sphäre der Kontrolltätigkeit des Unabhängigen Kontrollrates verlassen, namentlich bei dessen Berichtslegung, greift die Regelung der Third Party Rule vollumfänglich. Dies ist zum Schutz der nachdienstlichen Kooperationen von herausgehobener Bedeutung.

Zu Absatz 3

Es steht im Ermessen des Unabhängigen Kontrollrates, dem Deutschen Bundestag als Ganzes in allgemeiner Art und Weise und unter besonderer Beachtung des Geheimschutzes über Beanstandungen zu informieren. Das Bundeskanzleramt kann diesem Bericht eine eigene Stellungnahme beifügen.

§ 56 (Pflicht des Bundesnachrichtendienstes zur Unterstützung; Amtshilfe)

Zu Absatz 1

Der Bundesnachrichtendienst ist verpflichtet, den Unabhängigen Kontrollrat bei der Durchführung seiner gesetzlichen Kontrollbefugnisse zu unterstützen. BVerfGE a.a.O. Randnummer 290.

Zu Absatz 2

In Konkretisierung der Unterstützungspflicht nach Absatz 1 legt Absatz 2 Unterstützungsmaßnahmen des Bundesnachrichtendienstes bei der Kontrolle durch den Unabhängigen Kontrollrat fest, BVerfGE a.a.O. Randnummer 290. Der Bundesnachrichtendienst ist verpflichtet, dem Unabhängigen Kontrollrat im Rahmen seiner Kontrollbefugnis die Informationen und Daten zur Verfügung zu stellen, die dieser für die Durchführung der Kontrolle benötigt. Er geht damit materiell weiter als ein bloßes Akteneinsichtsrecht zur Verwirklichung einer wirksamen Kontrolle. In besonderen Fällen kann auch eine Vorlage des Originals notwendig werden, wenn auch im Regelfall eine Kopie ausreichen wird. Dienstlich entstandene private Notizen unterfallen nicht der Vorlagepflicht, wohl aber Akteninhalte, auch wenn diese etwa von einem ausländischen Nachrichtendienst stammen. Das Bundesverfassungsgericht hat festgestellt, dass die „Third Party Rule“ im Verhältnis zum Unabhängigen Kontrollrat kein Hinderungsgrund für eine wirksame Rechtskontrolle sein dürfe (BVerfGE a.a.O. Randnummern 292, 294, 295). Die „Third Party Rule“ ist eine auf Vereinbarungen mit Partnerdiensten beruhende allgemein anerkannte Verhaltensregel unter den Nachrichtendiensten, nach der Informationen von ausländischen Diensten nach Maßgabe in formeller Absprachen nicht ohne deren Zustimmung an Dritte weitergeben werden dürfen (BVerfGE, a.a.O., Randnummer 293, in ebensolchem Sinne BVerfGE 2 BvE 2/15, Randnummer 162). Auf diese Regel kann sich auch die Bundesregierung berufen, sofern sie entsprechende Zusagen gegeben hat, auf deren Grundlage Informationen von dem ausländischen Dienst übermittelt wurden und hieran anschließend eine Übermittlung an „Dritte“ in Frage steht (BVerfGE, a.a.O., Randnummer 293) Die „Third Party Rule“ ist insoweit eine auf eine rechtlich nicht verbindliche, aber auf Vereinbarung mit anderen Diensten beruhende und damit flexible Verwaltungspraktik, auf deren praktische Bedeutung die Bundesregierung Einfluss hat (BVerfGE, a.a.O., Randnummer 294 m.w.N.). Dieses Hindernis zur Einsichtnahme in Informationen, die von einem anderen Dienst übermittelt wurden, darf der verfassungsrechtlich gebotenen umfassenden Rechtskontrolle des Bundesnachrichtendienstes durch eine strikt auf Geheimhaltung ausgerichtete und verpflichtete unabhängige Instanz wie den Unabhängigen Kontrollrat, der nicht in das Parlament und dessen politische Kommunikationszusammenhänge eingebunden ist, nicht entgegengehalten werden (BVerfGE, a.a.O., Randnummer 294). Die Bundesregierung und der Bundesnachrichtendienst bleiben an gegebene Zusagen gebunden. Der Unabhängige Kontrollrat darf mit Blick auf die von anderen Diensten übermittelten Informationen aufgrund seiner vom Bundesverfassungsgericht geforderten strikt auf Geheimhaltung ausgerichteten Ausgestaltung jedoch nicht als „Dritter“ im Sinne der „Third Party Rule“ angesehen werden. Es ist so zu gewährleisten, dass sich sowohl die verfassungsrechtlich gebotene Kontrolltätigkeit ungehindert von der „Third Party Rule“ auch auf den Umgang des

Bundesnachrichtendienstes mit von ausländischen Diensten stammenden Informationen erstreckt, als auch die für die Wahrung der außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland besonders bedeutende Zusammenarbeit des Bundesnachrichtendienstes mit anderen Nachrichtendiensten weitergeführt werden kann (BVerfGE, a.a.O., Randnummer 295).

Die Unterstützungspflicht besteht im Umfang des gesetzlich festgelegten Kontrollrahmens des Unabhängigen Kontrollrates zur Rechtskontrolle der Technischen Aufklärung des Bundesnachrichtendienstes in persönlicher, sachlicher und zeitlicher Hinsicht, nicht darüber hinaus. In Bezug auf die einzeln aufgelisteten Kategorien erstreckt sich die Vorlagepflicht auf bereits vorhandene Informationen und Daten.

Zu Absatz 3

Die Kontrollbefugnis beinhaltet ein Zutrittsrecht zu allen Dienststellen sowie Zugang zu informationstechnischen Systemen der Technischen Aufklärung, BVerfGE a.a.O. Randnummer 290. Dabei ist der Begriff der Dienststelle in entsprechendem Sinne zu § 5 Abs. 1 S. 2 PKGrG für den Bundesnachrichtendienst zu verstehen. Das Zugangsrecht besteht soweit die Kontrolle des Unabhängigen Kontrollrates reicht und der Zugang für die Ausübung der Kontrolle erforderlich ist, nicht aber darüber hinaus. Das Zutrittsrecht ist akzessorisch zu Absatz 2 zu sehen und kann daher nicht weiter reichen als die dort festgelegten Befugnisse. Zudem muss es sich um Dienststellen und informationstechnische Systeme handeln, für die der Bundesnachrichtendienst allein Verfügungsberechtigt ist. Eine solche Verfügungsbefugnis liegt vor, wenn einzig der Bundesnachrichtendienst Zugriff auf das Zugangssystem hat und das Verfügungsrecht nicht durch einen Dritten eingeschränkt ist. Vom Bundesnachrichtendienst verarbeitete Daten, die ausschließlich in IT-Systemen gespeichert sind, welche ihrerseits nicht der alleinigen Verfügungsbefugnis des Bundesnachrichtendienstes unterliegen, sind dennoch – auch in Umsetzung der Maßgabe, dass die „Third Party Rule“ kein Kontrollhindernis mit Blick auf den Umgang des Bundesnachrichtendienstes mit von ausländischen Diensten stammenden Informationen sein darf – vollumfänglich kontrollierbar: Diese werden für Kontrollzwecke durch den Bundesnachrichtendienst in eigene IT-Systeme des Bundesnachrichtendienstes kopiert und können dort eingesehen und geprüft werden.

Die Fernmeldeaufklärung konkret dient dem überragenden öffentlichen Interesse an einer wirksamen Auslandsaufklärung und den hierdurch geschützten Verfassungsgütern von hohem Rang wie der Bewahrung demokratischer Selbstbestimmung und dem Schutz der verfassungsrechtlichen Ordnung im Sinne eines gesamtstaatlichen Interesses, das über das Interesse an der Gewährleistung der inneren Sicherheit als solcher deutlich hinausgeht (BVerfGE a.a.O. Randnummer 161f.). In diesem Zusammenhang ist eine entsprechende Ausnahmesituation, die nur eine Unterrichtung eines sehr engen Personenkreises ermöglicht nicht gänzlich auszuschließen. In einem solchen Fall wird das Bundeskanzleramt die Entscheidung gegenüber dem Unabhängigen Kontrollrat begründen müssen und gemeinsam nach einer angemessenen Unterrichtungsmöglichkeit suchen, die trotz der Ausnahmesituation die erforderliche Rechtskontrolle ermöglicht.

Zu Absatz 4

Im Rahmen der Kontrolle kann der Unabhängige Kontrollrat aktuell dort beschäftigte Angehörige des Bundesnachrichtendienstes befragen oder von ihnen schriftliche Auskünfte einholen. Es besteht die Pflicht zur vollständigen und wahrheitsgemäßen Auskunft. Diese Pflicht ist von einer Zeugenvernehmung im Sinne eines Strafverfahrens oder im Kontext eines Untersuchungsausschusses zu unterscheiden, an die spezifische Sanktionen geknüpft sind, §§ 48 ff. StPO, 20ff. PUAG.

Zu Absatz 5

Die Unterstützungsleistungen hat der Bundesnachrichtendienst unverzüglich, das heißt ohne schuldhaftes Zögern, zu erbringen.

§ 57 (Personal- und Sachausstattung; Personalverwaltung)

Zu Absatz 1

Die Regelung stellt sicher, dass dem Unabhängigen Kontrollrat hinreichendes Personal und hinreichende Mittel zu Verfügung stehen (BVerfG, a.a.O, Randnummer 288). Als oberste Bundesbehörde erhält der Unabhängige Kontrollrat ein eigenes Budget (BVerfG, a.a.O., Randnummer 281). Der Selbstorganisation des Kontrollrates obliegt der Personal- und Mitteleinsatz in einer Weise, die es ermöglicht, den ihm zu übertragenden Kontrollaufgaben mit Sorgfalt nachzukommen. Über die grundsätzliche Organisationsstruktur bestehend aus gerichtsähnlichem und administrativem Kontrollorgan unter einem Dach hinaus würde jede weitere organisationsrechtliche Vorgabe die Unabhängigkeit des Kontrollrates in Frage stellen. Der Unabhängige Kontrollrat verfügt schließlich über die Personalhoheit der bei ihm tätigen Bundesbeamtinnen und Bundesbeamten oder Richterinnen und Richter.

Zu Absatz 2

Die Regelung ermöglicht dem Unabhängigen Kontrollrat die grundsätzlich in eigener organisatorischer Verantwortung zu bewältigenden Aufgaben der Personalverwaltung und Personalwirtschaft auf das Bundeskanzleramt auszulagern. Dies soll eine organisationsrechtliche Entlastung der zukünftig kleinsten obersten Bundesbehörde ermöglichen. Personenbezogene Daten der Beschäftigten dürfen an das Bundeskanzleramt übermittelt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist.

§ 58 (Zusammenarbeit mit dem Parlamentarischen Kontrollgremium, der G 10-Kommission und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit)

Zu Absatz 1

Die Regelung stellt klar, dass auch ein regelmäßiger Austausch mit dem Parlamentarischen Kontrollgremium, der G10-Kommission und dem Beauftragten für den Datenschutz und die Informationsfreiheit über allgemeine Angelegenheiten der jeweiligen Kontrolltätigkeit möglich ist. Dieser Austausch kann dabei immer nur unter Wahrung der jeweils geltenden Geheimhaltungsvorschriften und nur im Rahmen der jeweiligen Kontrollzuständigkeiten erfolgen. Bei dem Parlamentarischen Kontrollgremium ist zu beachten, dass dieses sehr umfassende Kontrollzuständigkeiten besitzt. Entsprechend der Vorgaben des Bundesverfassungsgerichts weist die parlamentarische Kontrolle jedoch einen anderen Charakter auf, als eine Kontrolle, die alleine auf die Beachtung des objektiven Rechts ausgerichtet ist und deren Geheimhaltung keinerlei Grenzen unterliegt (BVerfGE, a.a.O., Randnummer 298). Der Informationsfluss in den parlamentarischen Raum und damit auch zum Parlamentarischen Kontrollgremium kann deswegen aus Geheimhaltungsgründen grundsätzlich begrenzt sein (BVerfGE, a.a.O., Randnummer 298).

Zu Absatz 2

Die Kontrollbefugnisse der politischen Kontrolle durch das Parlamentarische Kontrollgremium bleiben von der Kontrolle des Unabhängigen Kontrollrates unberührt. Beim Parlamentarischen Kontrollgremium handelt es sich um ein mit eigenen Rechten ausgestattetes Hilfsorgan des Bundestages (BT-Drs. 16/ 12412, Seite 4). Es ist unter Wahrung des Geheimschutzes mit der politischen Kontrolle der Nachrichtendienste betraut

und erfüllt hier eine zentrale, integrative Aufgabe in der nachrichtendienstlichen Kontrolllandschaft. Die Regelung stellt zudem klar, dass auch die Befugnisse der G10-Kommission sowie des Bundebeauftragten für den Datenschutz und die Informationsfreiheit zur Kontrolle der Tätigkeit des Bundesnachrichtendienstes durch die Tätigkeit des Unabhängigen Kontrollrates unberührt bleiben.

Unterabschnitt 6 (Mitteilungen, Evaluierung und Dienstvorschriften)

Die Überschrift zum Unterabschnitt wurde neu eingefügt.

§ 59 (Mitteilung an Betroffene und Benachrichtigungspflichten)

Diese Norm entspricht dem Erfordernis der Gewährleistung von Transparenz bei der Datenverarbeitung.

Zu Absatz 1

Auch wenn das BVerfG in seinem Urteil klarstellt, dass eine Transparenzpflicht auch für Nachrichtendienste besteht, erkennt es gleichzeitig an, dass die Geheimhaltung ein unverzichtbares Element einer funktionierenden Auslandsaufklärung darstellt (BVerfG, a.a.O., Randnummer 266). Das Gericht führt aus, dass für Aktivitäten des Bundesnachrichtendienstes, die unmittelbar in das Ausland hineinwirken oder dort vorgenommen werden, ein elementares Interesse daran besteht, dass diese insgesamt unbemerkt bleiben, damit der Bundesnachrichtendienst seine Aufgaben dauerhaft wahrnehmen kann. Zudem könnte eine solche Benachrichtigung im Einzelfall sogar negative Auswirkungen für den Betroffenen haben, da er so der Aufmerksamkeit und dem Misstrauen der eigenen Behörden oder gegebenenfalls Dritter ausgesetzt wird. (BVerfG, a.a.O., Randnummer 269). Absatz 1 stellt daher klar, dass bei einer Datenerhebung von sich im Ausland befindlichen Ausländern keine Mitteilung an die betroffenen Personen ergeht.

Zu Absatz 2

Das BVerfG hat in seinem Urteil klargestellt, dass es bei strategischen Aufklärungsmaßnahmen gegenüber Personen im Inland differenzierter Regelungen bedarf, die eine Benachrichtigung weitestgehend sicherstellen (BVerfG, a.a.O., Randnummer 268). Dies ist dann von Bedeutung, wenn trotz der vorhandenen Filtermechanismen des § 19 Absatz 7 dennoch Kommunikation unter Beteiligung von Inländern oder Deutschen erst im Rahmen einer manuellen Auswertung erkannt und aufgrund der Ausnahmeregelungen des § 19 Absatz 7 Satz 6 nicht unverzüglich gelöscht wird. Die betroffene Person ist dann zu informieren.

Diese Mitteilung an den Betroffenen stellt in rechtlicher Hinsicht den Regelfall dar. Nur wenn durch eine Mitteilung der Zweck der Maßnahme gefährdet würde oder ein überwiegender Nachteil für das Wohl des Bundes oder eines Landes absehbar ist, darf sie ausnahmsweise zurückgestellt werden. Die weiteren Regularien zur Einbindung und Zustimmung der G 10-Kommission für eine weitere Zurückstellung der Mitteilung entspricht den Regularien des § 12 des Artikel 10-Gesetzes.

§ 60 (Mitteilungsverbote)

Diese Norm entspricht inhaltlich weitestgehend dem bisherigen § 17. Der Begriff Maßnahmen wird spezifiziert zu Anordnungen und deren Umsetzungen. Sprachlich herausgestellt wird die Pflicht zur Verschwiegenheit. Verweisnormen werden angepasst.

§ 61 (Evaluierung)

Diese Pflicht zur Evaluierung entspricht dem Bedürfnis nach der Sicherstellung einer effektiven und umfassenden Rechtskontrolle (BVerfG, a.a.O., Randnummer 299). Die Bedingungen der Aufklärungsmaßnahmen wie deren Kontrolle können sich angesichts der Fortentwicklung der Technik schnell wandeln. Die Wirksamkeit der Kontrolle muss daher fortlaufend überprüft, um den Anforderungen gerecht zu werden. Gegenstand der Evaluierung sind daher ausschließlich die §§ 40 bis 58. Die Evaluierung erfolgt durch den Unabhängigen Kontrollrat selbst.

Kriterien, um die Effektivität der Kontrolle bewerten zu können, ist die Praktikabilität der Regelungen, die in Hinblick auf den vermeidbaren Erfüllungsaufwand zu prüfen ist. Dazu gehören die Bündelung von Aufgaben, ihre Verteilung und die administrativen Wege beispielsweise Beanstandungen nach § 52. Darüber hinaus sind auch die zur Verfügung stehenden personellen und sachlichen Mittel ein weiteres Indiz. Der Unabhängige Kontrollrat soll darstellen, inwieweit diese ausreichen oder gegebenenfalls aufgestockt für die Erfüllung der Aufgabe. Schließlich sind auch negative und positive Nebenfolgen und Akzeptanz der Regelungen und beispielsweise die Häufigkeit der Anrufung der gerichtlichen Kontrolle durch das administrative Kontrollorgan heranzuziehen. Schließlich muss bewertet werden, inwieweit die verwendeten finanziellen Mittel in einem angemessenen Ausgleich zu den erzielten Ergebnissen stehen. Dies muss nicht zwangsläufig eine rein monetäre Betrachtung sein.

Die Datengrundlage, welche eine solche Evaluation nach fünf Jahren ermöglicht, wird sich dabei erst nach Aufnahme der Arbeit durch das Unabhängige Kontrollorgan ergeben.

Das Bundeskanzleramt erhält vorab die Gelegenheit zur Stellungnahme zu diesem Bericht.

§ 62 (Dienstvorschriften)

§ 62 entspricht weitestgehend dem bisherigen § 6 Absatz 7, mit der Änderung, dass die Kontrollzuständigkeit in der Dienstvorschrift nicht mehr geregelt wird, da sie nun gesetzlich im Unterabschnitt 5 normiert ist und vom Unabhängigen Kontrollrat wahrgenommen wird.

Zu Nummer 22 (§ 63 Unabhängige Datenschutzkontrolle)

Diese Norm entspricht unverändert dem bisherigen § 32.

Zu Nummer 23 (§ 64 Anwendung des Bundesdatenschutzgesetzes)

Diese Norm entspricht weitgehend dem bisherigen § 32a. In der Nummer 2 wurde § 49 des Bundesdatenschutzgesetzes ergänzt, der die Zweckänderung bei der Datenverarbeitung regelt. Der Verweis auf § 49 Satz 1 BDSG soll es insbesondere ermöglichen, zum Zweck der Eigensicherung erhobene Daten (etwa Daten, die im Rahmen der Zugangssicherung der Dienstgebäude des Bundesnachrichtendienstes erhoben wurden) u.a. für arbeitsrechtliche und disziplinarrechtliche Maßnahmen zu verwenden. In der bisherigen Version der Norm fehlt eine derartige ausdrückliche Regelung der Zweckänderung, so dass dem Bundesnachrichtendienst eine zweckändernde Nutzung von Daten – im Gegensatz zu anderen Behörden, denen eine solche zweckändernde Nutzung bei Einhaltung der Vorgaben des § 49 BDSG gestattet ist – nicht möglich war. Diese Regelungslücke soll durch den Verweis auf § 49 BDSG geschlossen werden. Spezialregelungen zu Zweckänderungen, wie etwa in § 29 Absatz 5, sind vorrangig gegenüber der allgemeinen Vorschrift des § 49 BDSG anzuwenden und schränken damit den praktischen Anwendungsbereich des § 49 BDSG ein.

Ferner wurde § 50 BDSG ergänzt, der die Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken regelt. Damit wird bezweckt, dass auch der Bundesnachrichtendienst Daten zu anderen Zwecken als zu denjenigen, zu denen sie erhoben wurden, zu den vorgenannten Zwecken verwenden darf. § 50 BDSG soll insbesondere zur Anwendung gelangen, um die zur Ausführung des nachrichtendienstlichen Auftrags erforderliche Forschungsleistung (etwa im Bereich der Entschlüsselung von Daten) auch bei solchen Daten rechtssicher durchführen zu können, die ursprünglich zu anderen Zwecken erhoben werden und bei denen sich die Notwendigkeit einer wissenschaftlichen Analyse erst im Nachhinein ergeben hat. Auch die Forschung des Zentrums für Nachrichtendienstliche Aus- und Fortbildung als Teil der Hochschule des Bundes, das in den Bundesnachrichtendienst integriert ist, benötigt zum Teil – innerhalb der datenschutzrechtlichen Grenzen – Zugriff auf die auftragsbezogenen Daten, um beispielsweise die Prognosefähigkeit des Bundesnachrichtendienstes durch Analysen zu überprüfen und zu verbessern. Weiterhin ist es, auch aus datenschutzrechtlichen Gründen sinnvoll, ein Controlling der Datenverarbeitung im BND auf- bzw. auszubauen. Auch für dieses Controlling ist eine statistische Verarbeitung von Auftragsdaten erforderlich, so dass auch hier eine zweckändernde Nutzung der Daten erforderlich ist.

Zu Nummer 24 (§ 65 Berichtspflicht und Information der Öffentlichkeit)

Diese Norm orientiert sich am bisherigen § 33 der Satz 1 wird aufgehoben, Satz 2 wird sprachlich angepasst. Das Verhältnis von Satz 1 zu den Übermittlungsvorschriften wird durch einen entsprechenden Verweis klargestellt. In der Folge wurde die Überschrift angepasst.

Zu Nummer 25 (§ 66 Strafvorschriften)

Die Vorschrift entspricht dem bisherigen § 34 und ist abgesehen von der Anpassung der Verweisnorm unverändert.

Zu Nummer 26 (§ 67 Bußgeldvorschriften)

Diese Vorschrift entspricht dem bisherigen § 35 und ist abgesehen von Anpassungen der Verweisnormen unverändert.

Zu Nummer 27

§ 68 Einschränkung von Grundrechten

Das BVerfG hat in seinem Urteil klargestellt, dass das Zitiergebot auch dann zu beachten ist, wenn ein staatliches Handeln gegenüber Ausländern im Ausland vorliegt (vgl. BVerfG, a.a.O., Randnummer 135). Durch die Einfügung dieser Norm wird dem Zitiergebot des Artikel 19 Absatz 1 Satz 2 GG Rechnung getragen.

§ 69 Übergangsregelung

Da die Neufassung des Gesetzes dem Bundesnachrichtendienst weitreichende neue Verpflichtungen, insbesondere hinsichtlich Anordnungen und Datenkennzeichnungen auferlegt, bedarf es einer Übergangsvorschrift, die den Umgang mit Maßnahmen regelt die bereits vor Inkrafttreten dieses Gesetzes begonnen wurden sowie den Umgang mit personenbezogenen Daten, die auf Grundlage des bisher geltenden Gesetzes erhoben wurden.

Zu Absatz 1

Absatz 1 statuiert, dass die auf Grundlage des bisher geltenden Gesetzes begonnenen Maßnahmen, die mit Inkrafttreten dieses Gesetzes Anordnungsvorbehalten sowie der Rechtmäßigkeitsprüfung durch den Unabhängigen Kontrollrat unterliegen, für einen Übergangszeitraum fortgesetzt werden dürfen.

Hinsichtlich der neuen Anordnungspflichten besteht die Notwendigkeit, Übergangsfristen zu deren erstmaliger Erwirkung nach Einrichtung des Unabhängigen Kontrollrates als Kontrollinstanz vorzusehen, da diese Maßnahmen auf Basis des bisher geltenden Gesetzes weder anordnungsbedürftig noch anordnungsfähig waren und die Anordnungen daher erst mit Inkrafttreten dieses Gesetzes erwirkt werden können. Die genannte Umsetzungsfrist bis Ende 2022 trägt dem Umstand Rechnung, dass einerseits in diesem Zeitraum eine Vielzahl von Anordnungen erstmals erwirkt und durch den neu geschaffenen Unabhängigen Kontrollrat geprüft werden muss und andererseits die Vorgabe des Bundesverfassungsgerichts nach schnellstmöglicher Erreichung eines verfassungskonformen Zustands umgesetzt werden muss.

Zu Absatz 2

Absatz 2 besagt, dass Daten, die auf Grundlage des bisherigen Gesetzes erhoben und gespeichert wurden, nach Maßgabe des bei der Erhebung und Speicherung geltenden Rechts weiterhin gespeichert werden dürfen. Datenerhebungen nach Abschnitt 4 dieses Gesetzes unterliegen mit Inkrafttreten dieses Gesetzes erstmals einer Kennzeichnungspflicht (vgl. § 19 Absatz 10 und § 34 Absatz 8). Die Kennzeichnung kann regelmäßig nur für Daten, die nach Einführung dieser Kennzeichnungspflicht erhoben wurden, umgesetzt werden. Soweit die Kennzeichnung im Einzelfall auch bei Daten umgesetzt werden kann, die vor Einführung der Kennzeichnungspflicht erhoben wurden, bestimmt sich deren Speicherung nach den entsprechenden Vorschriften dieses Gesetzes.

Zu Absatz 3

Absatz 3 erklärt für Daten, die auf Grundlage des bisherigen BND-Gesetzes erhoben wurden, hinsichtlich der Datenübermittlung § 24 des bisherigen BND-Gesetzes für anwendbar. Dies ist notwendig, da die Vorschriften zur Datenübermittlung in diesem Gesetz neuerdings an Mittel und Zweck der Datenerhebung anknüpfen. Eine solche Anknüpfung ist jedoch nur dann möglich, wenn eine Kennzeichnung der Daten anhand der der Datenerhebung zugrunde liegenden Mittel und Zwecke erfolgt. Diese Kennzeichnung kann regelmäßig nur für Daten, die nach Einführung der Kennzeichnungspflicht erhoben wurden, umgesetzt werden (vergleiche Ausführungen bei Absatz 2). Soweit die Kennzeichnung im Einzelfall auch bei zuvor erhobenen Daten durchführbar ist, bestimmt sich deren Übermittlung nach den entsprechenden Vorschriften dieses Gesetzes.

Zu Absatz 4

Mit Absatz 4 wird eine Übergangsregelung für die Kennzeichnung und Weiterverarbeitung der nach Abschnitt 4 erhobenen personenbezogenen Daten eingefügt. Eine vollständige technische Umsetzung der in § 19 Absatz 10 Satz 1 und § 34 Absatz 8 Satz 1 vorgesehenen Kennzeichnung des Zwecks und des Mittels der Datenerhebung erfordert umfangreiche Anpassungen an den Dateien des Bundesnachrichtendienstes. Der Bundesnachrichtendienst verarbeitet die Daten aus der technischen Aufklärung in einer großen Anzahl unterschiedlicher Dateien. Diese müssen so verändert werden, dass sie die gesetzlich vorgesehenen Kennzeichnungen an jedem Einzeldatum ermöglichen. Aufgrund des damit einhergehenden beträchtlichen Umstellungsaufwandes kann die Zweck- und Mittelkennzeichnung bis zum Inkrafttreten des Gesetzes absehbar nicht vollständig in allen betroffenen Dateien technisch umgesetzt werden. Die Vorschrift erlaubt daher für einen

Übergangszeitraum bis zur Schaffung der technischen Voraussetzungen im Bundesnachrichtendienst ein Absehen von der Kennzeichnung in den betroffenen Dateien. Für die Weiterverarbeitung der Daten – insbesondere für die Übermittlung an Dritte – ist die Beachtung des Erhebungszwecks und -mittels dennoch notwendig. Der Bundesnachrichtendienst muss daher für die nach Inkrafttreten des Gesetzes erhobenen Daten anderweitig, also ohne technische Kennzeichnung, nachvollziehen können, zu welchem Zweck und mit welchem Mittel diese Daten gewonnen wurden. Bei der Übergangsvorschrift in Satz 1 handelt es sich daher nur um einen zeitweisen Verzicht auf die formale Kennzeichnung. Die materiellen Voraussetzungen zum Umgang mit den aus der technischen Aufklärung gewonnenen Daten, insbesondere die Einhaltung der Vorgaben der Übermittlungsvorschriften, bleiben hiervon unberührt. Etwas anderes gilt nur für Daten, die im Rahmen der technischen Aufklärung gewonnen wurden und aus denen Einzelerkenntnisse in so genannte strukturierte Grundlagendatenbanken des Bundesnachrichtendienstes überführt werden. In solchen Grundlagendatenbanken speichert der Bundesnachrichtendienst gezielt die mit unterschiedlichen nachrichtendienstlichen Mitteln gewonnenen Grundlagendaten, zum Beispiel nachrichtendienstlich relevante Informationen zu auftragsrelevanten Personen wie ausländischen politischen Entscheidungsträgern in Krisenstaaten. Bereits heute ist sichergestellt, dass die Herkunft der Information weitgehend nachvollziehbar ist. Zukünftig muss gewährleistet sein, dass Erhebungszweck und -mittel einer Information, sowohl der betroffenen Person, als auch jeder strukturierten Einzelinformation zu dieser Person (z.B. der politische Werdegang eines Entscheidungsträgers, Geburtsdatum, Wohnort) zugeordnet wird. Diese Anpassung bedarf aufwändiger technischer Vorarbeiten, die bis zum Inkrafttreten des Gesetzes nicht umgesetzt werden können. Weitermüssen auch die organisatorischen Abläufe angepasst, die zugehörigen Mitarbeiterinnen und Mitarbeiter geschult und komplexe technische Einzelfragen geklärt werden. Würden die Daten bis zur Anpassung der Systeme nicht in die Grundlagendatenbanken eingegeben, so würden empfindliche Wissenslücken entstehen, die nachträglich nicht zu kompensieren wären. Satz 2 sieht daher vor, dass Informationen, die im Rahmen der technischen Aufklärung gewonnen und in strukturierte Grundlagendatenbanken des BND eingegeben wurden, dort nach den bisherigen Regelungen behandelt werden dürfen. Dies betrifft die Übermittlung dieser Daten an externe in- und ausländische Stellen, da nur hier die Kennzeichnung praktische Relevanz entfaltet. Der Anteil an Daten, die mit Mitteln der technischen Aufklärung beschafft und aus den strukturierten Grundlagendatenbanken übermittelt werden ist gering. Denn im Regelfall erfolgt die Übermittlung der mit Mitteln der technischen Aufklärung erhobenen Daten nicht aus den Grundlagendatenbanken heraus, sondern unmittelbar. Zudem wird der Bundesnachrichtendienst die technische Anpassung der betroffenen Dateien an die geänderten gesetzlichen Vorgaben prioritär umsetzen. Dennoch soll, da es sich um eine inhaltlich und zeitlich begrenzte Ausnahme von dem durch das Bundesverfassungsgericht grundsätzlich festgelegten Gebot der Kopplung der erhobenen Daten an Aufklärungszweck und -mittel handelt, der Fortschritt der Umsetzung durch das Parlament begleitet werden. Satz 3 sieht daher eine jährliche Berichtspflicht des Bundeskanzleramtes gegenüber dem Parlamentarischen Kontrollgremium zu den Fortschritten bei der Schaffung der technischen Voraussetzungen für die Kennzeichnung des Erhebungszwecks und -mittels vor.

Zu Absatz 5

Die Neufassung bzw. Anpassung bestehender Absichtserklärungen mit ausländischen öffentlichen Stellen im Rahmen von Kooperationen in der strategischen Ausland-Fernmeldeaufklärung ist stets mit erheblichem Verhandlungsaufwand mit dem Kooperationspartner verbunden. Daher werden für diese Anpassung der entsprechenden

Erklärungen Übergangsfristen bis spätestens 31. Dezember 2024 gewährt. Die Übergangsfristen beziehen sich ausschließlich auf die Absichtserklärungen. Die in diesem Gesetz statuierten, darüber hinaus gehenden materiellen Verpflichtungen im Rahmen der Kooperationen bleiben hiervon unberührt und werden vollumfänglich erfüllt.

Zu Artikel 2 (Änderung des G 10)

Zu Nummer 1 (§ 4a Weiterverarbeitung von Verkehrsdaten durch den Bundesnachrichtendienst)

§ 4a regelt eine Befugnis zur Weiterverarbeitung von nach § 3 erhobenen Verkehrsdaten zu einem anderen Zweck als den in § 1 Absatz 1 Nummer 1 genannten. Dabei ist die Speicherung der Daten zum Zweck der Weiterverarbeitung im Rahmen einer Verkehrsdatenanalyse nach § 4a Absatz 1 Nummer 1 und 2 zulässig, ohne dass diese zuvor unkenntlich gemacht wurden. In Absatz 3 werden Kontrollmechanismen geregelt, die sicherstellen, dass die Zweckbindung bei der Nutzung der Verkehrsdaten eingehalten wird.

Zu Absatz 1

In Absatz 1 wird ergänzend zu § 3 Absatz 1 die Nutzungsmöglichkeit von Verkehrsdaten geregelt, die aufgrund einer angeordneten Maßnahme nach § 3 erhoben wurden. Eine Unkenntlichmachung der Verkehrsdaten ist hier nicht erforderlich, da die Daten im Rahmen einer G 10-Maßnahme erhoben wurden.

Nach Nummer 1 darf der Bundesnachrichtendienst die gespeicherten Verkehrsdaten weiterverarbeiten, um Personen zu erkennen, die einen Deutschlandbezug aufweisen und über die Informationen erlangt werden können, die für die Aufgabenerfüllung des Bundesnachrichtendienstes relevant sind. Die gespeicherten Verkehrsdaten sind solche, die Anschlusskennungen des Verdächtigen einer Straftat nach § 3 Absatz 1 oder eines Nachrichtensmittlers enthalten. Durch Nummer 1 sollen die Kontaktpersonen der Verdächtigen bzw. der Nachrichtensmittler (§ 3 Absatz 2: „Personen, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder, dass der Verdächtige ihren Anschluss benutzt“) für die Aufgabenerfüllung des Bundesnachrichtendienstes ohne Beschränkung auf die Zwecke nach § 4 Absatz 2 Satz 3 weiterverarbeitet werden, BND-spezifisch eben auch für die in § 1 Absatz 1 Satz 1 Nummer 2 bezeichneten Zwecke. Verkehrsdaten der erkannten Personen können unter den dafür geltenden Voraussetzungen durch den Bundesnachrichtendienst als Suchbegriffe für die strategische Fernmeldeaufklärung genutzt werden.

Eine weitere Zweckänderung ist in Nummer 2 geregelt. Danach können die Verkehrsdaten genutzt werden, um geeignete Telekommunikationsnetze im Sinne des § 10 Absatz 4 Satz 2 zu identifizieren (vgl. auch Begründung zu § 26 Absatz 1 BNDG und § 6 Absatz 4 und 5). Auch hier kann nur durch eine Analyse der über eine bestimmte Strecke laufenden Verkehre festgestellt werden kann, ob diese für die strategische Fernmeldeaufklärung geeignet ist. Geeignet kann eine Strecke beispielsweise sein, wenn eine hohe Anzahl von Verkehren übertragen wird, an denen Personen aus dem Inland beteiligt sind. Bevor eine Strecke nach dem G 10-Verfahren angeordnet wird, muss geprüft werden, ob sich diese überhaupt hierfür eignet, dies kann durch eine Abfrage nach § 114 TKG erfolgen. Durch die Analyse der unverhashten Verkehrsdaten kann jedoch eine besonders präzise Prüfung der Geeignetheit erfolgen. Die Analyse der Verkehrsdaten gibt Aufschluss über Start- und Endpunkt der Kommunikation sowie die Teilnehmer, hierdurch kann festgestellt werden, ob Verkehre enthalten sind, die für die Aufgabenerfüllung des Bundesnachrichtendienstes relevant sind und im Rahmen von Maßnahmen nach § 5 erhoben werden könnten.

Wird im Rahmen einer Analyse zum Zweck der Nutzung nach Satz 1 Nummer 1 und 2 erkannt, dass die Daten für die Aufgabenerfüllung des Bundesnachrichtendienstes relevant sind, ist eine darüberhinausgehende Nutzung der Verkehrsdaten im Rahmen des Satzes 2 zulässig. Im Rahmen einer Analyse kann es dazu kommen, dass der Bundesnachrichtendienst erkennt, dass es sich bei den Verkehrsdaten um relevante

Verkehre handelt, die über die in Satz 1 genannte Zwecke hinaus genutzt werden sollten. Beispielsweise könnte im Nachgang an eine terroristische Anschlagsserie in Afghanistan in der Nähe von dort stationierten Bundeswehrsoldaten erkannt werden, dass der Bundesnachrichtendienst Verkehrsdaten zu Personen gespeichert hat, die im Zusammenhang mit den Anschlagsvorbereitungen stehen. Die Verkehrsdaten deuten darauf hin, dass verschiedene Anschlagsbeteiligte insbesondere kurz vor den Anschlägen Kontakt zu einer Nummer in Deutschland hatten. Im genannten Beispiel könnten die Informationen zu der deutschen Nummer im Rahmen der in Satz 2 geregelten Befugnis an inländische Polizeibehörden übermittelt werden, damit diese Ermittlungsmaßnahmen zu einer möglichen Anschlagsbeteiligung aufnehmen können. Für die weitergehende Nutzung der Daten nach Satz 2 gilt folgende „Nutzungskaskade“: Sie dürfen immer zu Zwecken genutzt werden, zu denen gleiche oder geringere Voraussetzungen vorgesehen sind, als die, zu denen sie erhoben wurden. D.h. Daten, die im Rahmen von § 3 (Individualmaßnahme) erhoben wurden, dürfen neben dem Zweck aus § 3 auch für Zwecke nach § 5 (strategische Fernmeldeaufklärung zur Erkennung und Begegnung bestimmter Gefahren) und § 8 (Gefahr für Leib und Leben) genutzt werden. Daten, die nach § 5 erhoben wurden, dürfen demnach nur zu Zwecken nach § 8 sowie § 5 genutzt werden und Daten, die nach § 8 erhoben wurden, dürfen nur auch zu diesen Zwecken genutzt werden. Damit ist sichergestellt, dass die Nutzung der Daten nur zu einem Zweck erfolgen darf, zu dem sie auch hätten erhoben werden können. So ist die Nutzung von Verkehrsdaten nach Satz 2, die aufgrund einer Beschränkungsmaßnahme nach § 3 Absatz 1 erlangt wurden, auch zu den in den §§ 5 Absatz 1, 8 Absatz 1 genannten Zwecken zulässig (§ 6 Absatz 5 Satz 2 Nummer 1), da § 3 die strengsten Voraussetzungen normiert: Beschränkungsmaßnahmen nach § 3 knüpfen an das Vorliegen tatsächlicher Anhaltspunkte der Planung oder Begehung bestimmter Straftaten an; es handelt sich hierbei vor allem um Straftaten aus dem Bereich der Staatsschutz- und Kapitaldelikte, die Aufklärungsmaßnahme richtet sich hier gegen individuelles Handeln des Betroffenen. Eine Beschränkungsmaßnahme nach § 5 erfordert dagegen zwar einen Gefahrenverdacht, jedoch keine tatsächlichen Anhaltspunkte für eine konkrete Straftat. Außerdem darf sich eine Maßnahme nach § 5 nicht gezielt gegen Anschlüsse, deren Inhaber oder regelmäßige Nutzer deutsche Staatsangehörige sind, richten (§ 5 Absatz 2 Satz 3). Die in § 5 Absatz 1 genannten Gefahren stellen erhebliche Bedrohungen für die Sicherheit der Bundesrepublik Deutschland und für Freiheit, Leib und Leben ihrer Bürger dar, die die Durchführung strategischer Beschränkungsmaßnahmen nach § 5 legitimieren können. Gerade aufgrund der herausragenden Bedeutung der Erkennung und Begegnung solcher Gefahren erlaubt § 5 die Erhebung und Nutzung von personenbezogenen Daten aus Telekommunikation von deutschen Staatsangehörigen, inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen, auch wenn bei diesen vorher noch keine tatsächlichen Anhaltspunkte für eine Relevanz zur Erkennung und Begegnung dieser Gefahren vorgelegen haben. Die Nutzung von Verkehrsdaten aus Telekommunikationen von Personen, gegen die eine Individualbeschränkungsmaßnahme nach § 3 vorliegt, zur Erstellung von Verkehrsdatenanalysen ist vor diesem Hintergrund als legitime Zweckänderung zulässig. Die strategischen Beschränkungsmaßnahmen nach § 8 Absatz 1 dienen dem Zweck, eine im Einzelfall bestehende Gefahr für Leib und Leben einer Person im Ausland rechtzeitig zu erkennen und zu begegnen, wenn dadurch Belange der Bundesrepublik Deutschland unmittelbar in besonderer Weise berührt sind. Im Falle einer Maßnahme nach § 8 Absatz 1 besteht somit eine konkrete Gefahr für Leib und Leben einer Person, der es zu begegnen gilt. Es bedarf hier zwar einer konkreten Gefahrenlage. Diese ist jedoch inhaltlich stark begrenzt auf eine bestehende Gefahr für Leib und Leben einer Person. Die Nutzung von Verkehrsdaten aus Telekommunikationen von Personen, gegen die eine Individualbeschränkungsmaßnahme nach § 3 vorliegt, zur Erstellung von Verkehrsdatenanalysen ist vor diesem Hintergrund als legitime Zweckänderung zulässig.

Für die Zulässigkeit einer Nutzung von Verkehrsdaten, die aufgrund einer Beschränkungsmaßnahme nach § 5 erlangt wurden, zu den in § 8 Absatz 1 genannten Zwecken, gelten die vorstehenden Ausführungen entsprechend. Zulässig wäre demnach beispielsweise die Nutzung von nicht unkenntlich gemachten, d.h. unverhashten Verkehrsdaten, die nach § 5 Absatz 1 Satz 3 Nummer 2 zum Zweck der Erkennung und Begegnung der Gefahr der Begehung internationaler terroristischer Anschläge mit unmittelbarem Bezug zur Bundesrepublik Deutschland erhoben wurden, für eine Verkehrsdatenanalyse im Kontext der Entführung einer Person im Ausland z.B. durch eine terroristische Gruppierung. Unzulässig wäre dagegen beispielsweise die Nutzung von Verkehrsdaten aus einer Beschränkungsmaßnahme nach § 5 Absatz 1 für eine Verkehrsdatenanalyse, die ihrerseits nicht der Erkennung und Begegnung einer Gefahr nach § 5 Absatz 1 oder der Erkennung und Begegnung einer konkreten Gefahr für Leib und Leben einer Person dient (§ 8 Absatz 1), sondern zur Aufklärung eines der in § 3 Absatz 1 genannten Sachverhalte. So dürfen beispielsweise Verkehrsdaten, die nach § 5 Absatz 1 Satz 3 Nummer 2 zum Zweck der Erkennung und Begegnung der Gefahr der Begehung internationaler terroristischer Anschläge mit unmittelbarem Bezug zur Bundesrepublik Deutschland erhoben wurden, nicht für eine Verkehrsdatenanalyse im Rahmen des § 3 Absatz 1 Satz 1 Nummer 5 zum Zweck der Aufklärung einer Straftat gegen die Sicherheit von in Deutschland stationierten Truppen der NATO genutzt werden. Die – in den Fällen des § 4a tatsächlich mögliche – Mitteilung an Betroffene richtet sich nach § 12.

Zu Absatz 2

Die gespeicherten Verkehrsdaten sind drei Monate nach Erhebung daraufhin zu prüfen, ob die weitere Nutzung zu den in Absatz 1 genannten Zwecken erforderlich ist. Die besonders kurzen Fristen in Satz 1 und 2 korrespondieren der besonderen Zweckerweiterung der Weiterverarbeitung in § 4a Absatz 1 und synchronisieren zugleich den Bearbeitungsprozess aus verwaltungspraktischen Erwägungen mit der entsprechenden Regelung in § 6 Absatz 5, die ihrerseits der besonderen Sensitivität des Informationsaufkommens aus einem strategischen Aufklärungsansatz (der nicht an einen Individualverdacht anknüpft) Rechnung trägt. Wird im Rahmen der Prüfung festgestellt, dass diese nicht mehr zu Analysezwecken erforderlich ist, sind die Daten zu löschen. Wurde beispielsweise festgestellt, dass der Kontaktpartner einer Person, gegen die eine Individualmaßnahme nach § 3 durchgeführt wird, nicht nachrichtendienstlich relevant ist, ist der entsprechende Verkehr zu löschen. Zum Beispiel: Eine deutsche Staatsangehörige, die der Mitgliedschaft in einer terroristischen Vereinigung im Ausland verdächtig ist und zu der deshalb eine Beschränkungsmaßnahme nach § 3 angeordnet war, wendet sich von der Vereinigung ab und offenbart im Rahmen anschließender Vernehmungen glaubhaft, dass sie während ihres Aufenthaltes im Ausland in der terroristischen Vereinigung u.a. intensiv mit ihrer Schwester in Deutschland zu rein familiären Angelegenheiten kommuniziert hat. Eine nachrichtendienstliche Relevanz der zu diesen Kommunikationen vorliegenden Verkehrsdatenerfassungen ist nicht mehr gegeben. Nach einer weiteren Prüfung nach sechs Monaten sind die Daten zu löschen, es sei denn, es wurde im jeweiligen Einzelfall festgestellt, dass die weitere Nutzung für die Aufgabenerfüllung erforderlich ist.

Zu Absatz 3

Interne und externe verfahrenstechnische Kontrollmechanismen sollen sicherstellen, dass die Zweckbindungen des § 4a in der Praxis des Bundesnachrichtendienstes stets eingehalten werden. Die interne Kontrolle erfolgt (mindestens) durch einen hierzu beauftragten Mitarbeiter mit der Befähigung zum Richteramt. Ergibt die Prüfung eine unzulässige Zwecknutzung greifen Lösch- und Protokollierungspflichten (Satz 2 und 3). Die externe Kontrolle erfolgt durch die G 10-Kommission. Die G 10-Kommission hat dabei ein umfassendes Prüfrecht, siehe § 15 Absatz 5. Eine Möglichkeit für die G 10-Kommission ihr

Prüfrecht auszuüben ist es beispielsweise, die Einhaltung der Zweckbindung im Rahmen von Stichproben zu überprüfen, diese Praxis hat sich zum Beispiel bei der Kontrolle der Suchbegriffe, die nach § 5 angeordnet sind, bewährt.

Zu Nummer 2 (§ 6 Prüf-, Kennzeichnungs- und Löschungspflichten, Zweckbindung)

§ 6 regelt in seinem Absatz 4 die Erhebung und Weiterverarbeitung von unkenntlich gemachten Verkehrsdaten (sogenannte verhashten Verkehrsdaten), die auf den nach § 5 Absatz 1 Satz 1 in Verbindung mit § 10 Absatz 4 angeordneten Strecken erhoben wurden. Die unverhashte Nutzung von Verkehrsdaten, die im Rahmen von angeordneten G 10-Maßnahmen erhoben wurden, wird in Absatz 5 geregelt.

Zu Absatz 1

In Absatz 1 erfolgt eine Anpassung der Formulierung in Satz 4 zur Zweckbindung der Protokolldaten an die Parallelregelung in § 27 Absatz 1 Satz 4 BNDG. Auf die dortigen Aussagen wird verwiesen.

Zu Absatz 3

In Absatz 3 erfolgt ebenfalls eine Anpassung der Formulierung zur Zweckbindung der Protokolldaten an die Parallelregelung in § 27 Absatz 1 Satz 4 BNDG. Auf die dortigen Aussagen wird verwiesen.

Zu Absatz 4

Absatz 4 regelt die Erhebung und Weiterverarbeitung von Verkehrsdaten, welche auf nach § 5 Absatz 1 Satz 1 in Verbindung mit § 10 Absatz angeordneten Übertragungswege erhoben wurden. Die in Absatz 4 Satz 1 und 2 vorgesehene unverzügliche Unkenntlichmachung der Verkehrsdaten wird in gleicher Weise wie in dem in § 26 Absatz 3 Satz 2 Nummer 2 BNDG vorgesehenen Verfahren vorgenommen. Diesbezüglich wird auf die Ausführungen zu Artikel 1 Nummer 1 verwiesen. Da die den Daten zuzuordnende Person aufgrund der sogenannten Verhashung nicht identifizierbar ist, ist die in § 12 Absatz 2 für Beschränkungen nach § 5 grundsätzlich vorgesehene Mitteilung an Betroffene in diesen Fällen schon aus tatsächlichen Gründen unmöglich.

Absatz 4 Satz 4 und 5 normiert Speicher- und Prüfvorgaben parallel zu § 26 Absatz 5 in Verbindung mit § 27 BNDG, soweit angesichts der sogenannten Verhashung und daraus folgenden fehlenden Identifizierbarkeit eine gleichlautende Interessenlage vorliegt.

Die hiermit vorgenommene Änderung des § 6 bezweckt keine Änderung der geltenden Rechtslage. Das heißt, dass die Verarbeitung der auf der Grundlage von § 5 Absatz 1 erhobenen Verkehrsdaten für die Zwecke des § 5 Absatz 1 Satz 3 unberührt bleibt.

Zu Absatz 5

Voraussetzung für Absatz 5 wie für Absatz 4 ist, dass die Daten auf den nach § 5 Absatz 1 angeordneten Übertragungswegen erhoben wurden. Absatz 4 regelt die Weiterverarbeitung von verhashten Verkehrsdaten, welche auf nach § 5 Absatz 1 Satz 1 angeordneten Telekommunikationsnetzen erhoben wurden und bei der für keinen der beiden Kommunikationsteilnehmer eine Beschränkungsanordnung vorliegt. Da keine Beschränkungsanordnung vorliegt, darf die Weiterverarbeitung nur nach der sog. Verhashung erfolgen. Absatz 5 dagegen bildet die Rechtsgrundlage für die Weiterverarbeitung der Verkehrsdaten im Rahmen einer Zweckerweiterung, ohne dass die Identifizierung der Teilnehmer bzw. Anschlussinhaber durch eine Verhashung unmöglich gemacht wurde. Voraussetzung ist auch hier, dass die Daten auf den nach § 5 Absatz 1 Satz 1 angeordneten Übermittlungswegen erhoben wurden, zusätzlich muss die Datenerhebung auf der Grundlage eines angeordneten Suchbegriffs nach § 5 Absatz 2

vorliegen. Absatz 5 regelt also zusätzliche Nutzungsbefugnisse von Verkehrsdaten, die aufgrund von Beschränkungsmaßnahmen nach § 5 erhoben wurden.

In Satz 1 wird - wie § 4a Absatz 3 - die Prüfpflicht nach drei Monaten geregelt.

Die weitere Zweckänderung ist – analog zu § 4a Absatz 1 in Satz 1 Nummer 1 bis 2 sowie in Satz 2 geregelt und ist nur unter Einhaltung der dort genannten Voraussetzung zulässig. Zu der Zweckerweiterung wird insoweit auf die Begründung zu § 4a sowie auf die Ausführungen zu § 26 Absatz 3 Satz 2 Nummer 2 BNDG verwiesen.

Für die Nutzung nach Nummer 1 gilt, dass der Bundesnachrichtendienst zur Weiterverarbeitung befugt ist, um Personen zu erkennen, die einen Deutschlandbezug aufweisen und über die Informationen erlangt werden können, die für die Aufgabenerfüllung des Bundesnachrichtendienstes relevant sind. Es handelt sich bei den Verkehrsdaten nach Absatz 5 um solche, bei denen ein nach dem G 10-Verfahren angeordneter Suchbegriff enthalten ist. Bei den genutzten Suchbegriffen handelt es sich häufig um Telekommunikationsmerkmale. Dabei ist die Nutzung inländischer Telekommunikationsmerkmale unzulässig (vgl. § 5 Absatz 2 Satz 3). Bei den nach § 5 Absatz 1 erhobenen Daten handelt es sich daher in der Regel um Daten, bei denen ein Telekommunikationsteilnehmer bereits bekannt ist (der ausländische Anschluss, der bereits als Suchbegriff gesteuert wurde). Die im Rahmen eines erhobenen Verkehrs kontaktierte Person im Inland ist hingegen in der Regel nicht bekannt. Bei der Verkehrsdatenanalyse nach § 6 Absatz 5 sollen daher relevante Personen auf Seiten der kontaktierten inländischen Anschlüsse erkannt werden. Die Telekommunikationsmerkmale der inländischen Kontaktpersonen können dann u.a., bei Vorliegen der entsprechenden Voraussetzungen genutzt werden, um Maßnahmen nach § 3 zu beantragen. Für die strategische Fernmeldeaufklärung können die inländischen Verkehrsdaten nicht genutzt werden (vergleiche § 5 Absatz 2 Satz 3).

Zu Absatz 6

Interne und externe verfahrenstechnische Kontrollmechanismen sollen sicherstellen, dass die Zweckbindungen des Absatzes 5 in der Praxis des Bundesnachrichtendienstes stets eingehalten werden und entsprechen weitgehend der Regelung in § 4a Absatz 3.

Zu Nummer 3 (§ 8 Gefahr für Leib oder Leben einer Person im Ausland)

Zu Absatz 4

Mit Absatz 5 Satz 4 wird die Zweckänderung auch für die strategische Fernmeldeaufklärung bei Gefahren für Leib oder Leben einer Person im Ausland geregelt. Auf die Ausführungen zu § 6 Absatz 5 wird verwiesen.

Zu Absatz 5

In diesem Absatz wird der Verweis auf das BNDG redaktionell neu angepasst.

Zu Artikel 3 (Änderung des Bundesbesoldungsgesetzes)

(noch zu ergänzen)

Zu Artikel 4 (Telekommunikationsüberwachungsverordnung)

Es handelt sich um Folgeänderungen und Anpassungen, die sich aufgrund der Änderung des BND-Gesetzes ergeben.

Zu Artikel 5 (Zollverwaltungsgesetz)

Es handelt sich um Folgeänderungen und Anpassungen, die sich aufgrund der Änderung des BND-Gesetzes ergeben.

Zu Artikel 6 (Gesetz zum Schutz vor Gefährdung der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten)

Es handelt sich um Folgeänderungen und Anpassungen, die sich aufgrund der Änderung des BND-Gesetzes ergeben.

Zu Artikel 7 (Telekommunikationsgesetz)

Es handelt sich um Folgeänderungen und Anpassungen, die sich aufgrund der Änderung des BND-Gesetzes ergeben.

Zu Artikel 8 (Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen)

Es handelt sich um Folgeänderungen und Anpassungen, die sich aufgrund der Änderung des BND-Gesetzes ergeben.

Zu Artikel 9 (Gesetz über das Ausländerzentralregister)

Es handelt sich um Folgeänderungen und Anpassungen, die sich aufgrund der Änderung des BND-Gesetzes ergeben.

Zu Artikel 10 (Strafprozessordnung)

Es handelt sich um Folgeänderungen und Anpassungen, die sich aufgrund der Änderung des BND-Gesetzes ergeben.

Zu Artikel 11 (Einschränkung eines Grundrechts)

Um dem Zitiergebot des Artikel 19 Absatz 1 Satz 2 GG Rechnung zu tragen, werden die Grundrechtseingriffe im Abschnitt 4 des Artikel 1 (BNDG) sowie Artikel 2 (G10) aufgeführt. Es wird das Grundrecht des Post-, Brief- und Fernmeldegeheimnisses (Artikel 10 GG) eingeschränkt.

Zu Artikel 12 (Bekanntmachungserlaubnis)

Das BND-Gesetz wird umfassend neu nummeriert. Aus diesem Grund soll dem Bundeskanzleramt die Erlaubnis eingeräumt werden, den Wortlaut des BND-Gesetzes im Bundesgesetzblatt bekannt zu machen.

Zu Artikel 13 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten des Gesetzes.