

## Gesetzentwurf

### der Fraktionen der CDU/CSU und SPD

#### Entwurf eines Gesetzes zur Modernisierung der Rechtsgrundlagen der Bundespolizei

##### A. Problem und Ziel

Das geltende Bundespolizeigesetz, das zum überwiegenden Teil noch aus dem Jahr 1994 stammt und bisher nur in einzelnen Vorschriften angepasst worden ist, bedarf einer Modernisierung.

Die besonderen Fähigkeiten und die herausragende Stellung der Bundespolizei müssen, an ihren Kernkompetenzen orientiert und unter Wahrung des sonderpolizeilichen Charakters, gezielt gestärkt und an die technische Entwicklung sowie an die aktuellen sicherheitspolitischen Herausforderungen und Gefahrenlagen angepasst werden.

Der im Bundespolizeigesetz definierte Aufgabenkanon der Bundespolizei hat sich im Grundsatz bewährt. Beabsichtigt ist gleichwohl eine weitere Differenzierung und Fokussierung. Darüber hinaus soll die Bundespolizei im Bereich der Gefahrenabwehr mit neuen Befugnissen ausgestattet werden.

Das Bundesverfassungsgericht hat in seinem Urteil vom 20. April 2016 (Az. 1 BvR 966/09 und 1 BvR 1140/09; BVerfGE 141, 220) einige Vorschriften des damaligen Bundeskriminalamtgesetzes für verfassungswidrig erklärt. Da das Bundespolizeigesetz vergleichbare Vorschriften enthält, lassen sich die Aussagen des Bundesverfassungsgerichts insoweit auch auf das Bundespolizeigesetz übertragen.

Das Gesetz über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes (UZwG) umfasst keine Regelung des finalen Rettungsschusses, die in der Mehrzahl der Polizeigesetze der Länder vorhanden ist.

##### B. Lösung

Das Bundespolizeigesetz wird überarbeitet. Im Bereich der Gefahrenabwehr erforderliche Befugnisse werden aufgenommen. Dabei werden die Vorgaben des Bundesverfassungsgerichts aus seinem Urteil vom 20. April 2016 zum damaligen Bundeskriminalamtgesetz und die Regelungen der Richtlinie (EU) 2016/680 vom 27. April 2016 berücksichtigt.

Die Richtlinie (EU) 2016/680 vom 27. April 2016 wird weitgehend in Teil 3 des Bundesdatenschutzgesetzes umgesetzt. Im Bundespolizeigesetz sollen diese Vorschriften gleichwohl an einigen Stellen im Hinblick auf die Erfordernisse der Bundespolizei ergänzt und spezifiziert werden.

Im UZwG wird eine rechtliche Grundlage für den finalen Rettungsschuss eingeführt, um in besonderen Situationen (z. B. Geiselnahmen, Terroranschlag), die einen derartigen Schusswaffengebrauch erfordern, auf sicherer Rechtsgrundlage handeln zu können.

### **C. Alternativen**

Keine.

### **D. Haushaltsausgaben ohne Erfüllungsaufwand**

Keine.

### **E. Erfüllungsaufwand**

#### **E.1 Erfüllungsaufwand für Bürgerinnen und Bürger**

Keiner.

#### **E.2 Erfüllungsaufwand für die Wirtschaft**

Keiner.

#### **E.3 Erfüllungsaufwand der Verwaltung**

Durch die Änderung des Bundespolizeigesetzes entstehen sowohl dem Bund als auch den Ländern Erfüllungsaufwände.

Bund:

Durch die Änderung des Bundespolizeigesetzes entsteht dem Bund ein einmaliger Erfüllungsaufwand in Höhe von rd. 12 384 635 Euro. Hierin enthalten sind ein einmaliger Personalaufwand in Höhe von rd. 5 212 354 Euro sowie ein einmaliger Sachaufwand in Höhe von rd. 7 172 281 Euro für die Beschaffung entsprechender Hard- und Software.

Der jährliche Erfüllungsaufwand beträgt rd. 21 514 197 Euro. Hierin enthalten sind ein jährlicher Personalaufwand in Höhe von 17 436 657 Euro sowie ein sachbezogener Aufwand im Bereich der neuen Aufgaben und Befugnisse in Höhe von rd. 4 077 540 Euro.

Der vorstehend bezifferte Erfüllungsaufwand ist im Wesentlichen auf folgende Umstände zurückzuführen:

Die Bundespolizei wird – ebenso wie das Bundeskriminalamt – für die Umsetzung der Vorgaben aus dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 und der Umsetzung der Richtlinie (EU) 2016/680 vom 27. April 2016 die bestehende IT-Architektur, insbesondere die Verbundsysteme, anpassen. Die dort gestellten Anforderungen an die Verarbeitung personenbezogener Daten müssen

unter Beachtung des Grundsatzes der hypothetischen Datenneuerhebung in den IT-Systemen der Bundespolizei abgebildet werden.

Das Bundesverfassungsgericht macht in seinem Urteil vom 20. April 2016 detaillierte Vorgaben für den Schutz des Kernbereichs der privaten Lebensgestaltung und weitet den Richtervorbehalt aus. Insbesondere muss sichergestellt werden, dass bestimmte Erkenntnisse dem anordnenden Gericht vorgelegt werden, damit dieses unverzüglich über die Verwertbarkeit oder Löschung der Daten entscheiden kann. Dies erfordert eine systematische Erweiterung und Weiterentwicklung der bislang zur Durchführung von Maßnahmen genutzten Systeme. Dabei müssen die Anforderungen der IT-Sicherheit vollumfänglich umgesetzt werden.

Mit dem Wegfall der Erstattung der Selbstkosten in § 62 geht eine Entlastung des Bundeshaushalts um ca. 35 Millionen Euro beim Titel 671 04 und ca. 11 Millionen Euro beim Titel 517 01 (Bewirtschaftungskosten) einher.

Länder:

Es ergeben sich Möglichkeiten zur Einsparung für die Länder, wenn die Bundespolizei zusätzliche Aufgaben übernimmt.

Mit der bundespolizeilichen Durchführung von Maßnahmen des Zeugenschutzes entfällt die diesbezügliche Unterstützung durch die Polizeien der Länder. Damit einhergehend entfallen Erfüllungsaufwände für die Länder in nicht bezifferbarer Höhe.

Mit der Bearbeitung weiterer Straftatbestände durch die Bundespolizei geht eine Entlastung der Länder (und des Zolls) in nicht bezifferbarer Höhe einher.

Kommunen:

Für die Kommunen fällt kein Erfüllungsaufwand an.

## **F. Weitere Kosten**

Durch die Änderung des Bundespolizeigesetzes entsteht den zuständigen Gerichten ein Mehraufwand durch künftige Anordnungserfordernisse im Zusammenhang mit präventiven Maßnahmen sowie durch erforderliche Entscheidungen, ob gewonnene Erkenntnisse zu verwerten oder zu löschen sind. Einer auf Erfahrungswerten der letzten Jahre basierenden Schätzung zufolge werden durch die Bundespolizei im Jahr etwa 80 präventive Maßnahmen durchgeführt.

Sonstige Kosten für die Wirtschaft und für soziale Sicherungssysteme werden nicht erwartet, ebenso wenig Auswirkungen auf das Preisniveau, insbesondere auf das Verbraucherpreisniveau.



## Entwurf eines Gesetzes zur Modernisierung der Rechtsgrundlagen der Bundespolizei

Vom ...

Der Bundestag hat mit Zustimmung des Bundesrates das folgende Gesetz beschlossen:

### Artikel 1

#### Änderung des Bundespolizeigesetzes

Das Bundespolizeigesetz vom 19. Oktober 1994 (BGBl. I S. 2978, 2979), das zuletzt durch [...] geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

- a) Nach der Angabe zu § 12 wird folgende Angabe eingefügt:  
„§ 12a Zeugenschutz“.
- b) Nach der Angabe zu § 14 wird folgende Angabe eingefügt:  
„§ 14a Befugnisse für den Schutz von Zeugen“.
- c) Nach der Angabe zu § 25 wird folgende Angabe eingefügt:  
„§ 25a Meldeauflagen“.
- d) Nach der Angabe zu § 27c werden die folgenden Angaben eingefügt:  
„§ 27d Überwachung der Telekommunikation  
§ 27e Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten“.
- e) Nach der Angabe zu § 28a wird folgende Angabe eingefügt:  
„§ 28b Einsatz technischer Mittel gegen fernmanipulierte Geräte“.
- f) Die Angabe zu Teil 2 wird wie folgt gefasst:

„Teil 2

Weiterverarbeitung und Übermittlung von Daten“.

- g) Die Angabe zu § 29 wird wie folgt gefasst:  
„§ 29 Weiterverarbeitung personenbezogener Daten“.
- h) Nach der Angabe zu § 29 werden die folgenden Angaben eingefügt:  
„§ 29a Zweckbindung, Grundsatz der hypothetischen Datenneuerhebung  
§ 29b Daten zu Verurteilten, Beschuldigten, Tatverdächtigen und sonstigen Anlasspersonen  
§ 29c Daten zu anderen Personen  
§ 29d Weiterverarbeitung von Daten zur Aus- und Fortbildung, zur Vorgangsverwaltung oder zur befristeten Dokumentation des polizeilichen Handelns

- § 29e Kennzeichnung“.
- i) Die Angabe zu § 31a wird wie folgt gefasst:  
„§ 31a Ausschreibungen von Personen und Sachen zur gezielten und verdeckten Kontrolle oder Ermittlungsanfrage im Schengener Informationssystem“.
- j) Nach der Angabe zu § 31a wird folgende Angabe eingefügt:  
„§ 31b Übermittlung von Fluggastdaten“.
- k) Die Angaben zu den §§ 32 und 32a werden wie folgt gefasst:  
„§ 32 Übermittlung personenbezogener Daten im innerstaatlichen Bereich  
§ 32a Übermittlung personenbezogener Daten an Mitgliedstaaten der Europäischen Union und Schengen assoziierte Staaten“.
- l) Nach der Angabe zu § 32a wird folgende Angabe eingefügt:  
„§ 32b Übermittlung personenbezogener Daten im internationalen Bereich“.
- m) Die Angabe zu § 33 wird wie folgt gefasst:  
„§ 33 Übermittlungsverbote und Verweigerungsgründe“.
- n) Die Angabe zu § 33a wird gestrichen.
- o) Nach der Angabe zu § 34 wird folgende Angabe eingefügt:  
„§ 34a Speicherung von DNA-Identifizierungsmustern zur Erkennung von DNA-Trugspuren“.
- p) Die Angabe zu § 35 wird wie folgt gefasst:  
„§ 35 Aussonderungsprüffristen“.
- q) Nach der Angabe zu § 35 werden die folgenden Angaben eingefügt:  
„§ 35a Löschung von durch Besondere Mittel der Datenerhebung oder vergleichbare Maßnahmen erlangten personenbezogenen Daten  
§ 35b Berichtigung personenbezogener Daten, Einschränkung der Verarbeitung in Akten und Vernichtung von Akten  
§ 35c Benachrichtigung bei verdeckten und eingriffsintensiven Maßnahmen  
§ 35d Benachrichtigung über die Speicherung personenbezogener Daten von Kindern  
§ 35e Protokollierung  
§ 35f Protokollierung bei verdeckten und eingriffsintensiven Maßnahmen“.
- r) Die Angaben zu den §§ 36 und 37 werden wie folgt gefasst:  
„§ 36 Verzeichnis von Verarbeitungstätigkeiten  
§ 37 Ergänzende Befugnisse der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit“.
- s) Die Angabe zu Teil 3 wird wie folgt gefasst:  
  
„Teil 3  
Freiheitsbeschränkende Maßnahmen und Durchsuchung“.
- t) Nach der Angabe zu § 38 wird folgende Angabe eingefügt:  
„§ 38a Aufenthaltsverbot“.

- u) Nach der Angabe zu § 41 wird folgende Angabe eingefügt:  
„§ 41a Bild- und Tonüberwachung von Gewahrsamsräumen“.
  - v) Die Angabe zu § 43 wird wie folgt gefasst:  
„§ 43 Durchsuchung von Personen und Entnahme von Blutproben“.
  - w) Folgende Angabe wird angefügt:  
„§ 71 Berichtspflicht gegenüber dem Deutschen Bundestag“.
2. In § 1 Absatz 5 werden nach dem Wort „Straftaten“ die Wörter „und die Vorsorge für die künftige Verfolgung von Straftaten“ eingefügt.
3. § 12 wird wie folgt geändert:
- a) Absatz 1 wird wie folgt geändert:
    - aa) Satz 1 wird wie folgt geändert:
      - aaa) In dem Satzteil vor Nummer 1 werden die Wörter „eines Vergehens (§ 12 Abs. 2 des Strafgesetzbuches) besteht, das“ durch die Wörter „einer Straftat besteht, die“ ersetzt.
      - bbb) In Nummer 2 wird das Wort „es“ durch das Wort „sie“ ersetzt und werden nach den Wörtern „begangen wurde“ die Wörter „oder die Person, die einer solchen Straftat verdächtig ist, im Zuständigkeitsbereich der Bundespolizei festgestellt wurde“ eingefügt.
      - ccc) In Nummer 5 wird das Wort „und“ durch das Wort „oder“ ersetzt.
      - ddd) Folgende Nummer 7 wird angefügt:  
„7. gegen die Sicherheit der Anlagen oder des Betriebes des Luftverkehrs gerichtet ist und im Zuständigkeitsbereich der Bundespolizei festgestellt wird.“
      - eee) In dem Satzteil nach Nummer 7 werden die Wörter „darüber hinaus, soweit der Verdacht eines Verbrechens nach Nummer 2 oder nach § 315 Abs. 3 Nr. 1 des Strafgesetzbuches besteht sowie in Fällen der Nummer 6.“ gestrichen.
    - bb) Die Sätze 2 und 3 werden durch folgenden Satz ersetzt:  
„Der Bundespolizei obliegt im Fall der Nummer 5 die polizeiliche Aufgabe auf dem Gebiet der Strafverfolgung bei dem Verdacht eines Verbrechens nur dann, wenn der Verdacht einer Straftat nach den §§ 244a, 249, 250, 252, 255, 308 Absatz 1 oder 315 Absatz 3 des Strafgesetzbuches besteht.“
  - b) In Absatz 3 Satz 3 werden die Wörter „oder Absatz 1 Satz 1 letzter Halbsatz“ gestrichen.
  - c) In Absatz 5 Satz 2 werden die Wörter „und des Absatzes 1 Satz 1 letzter Halbsatz“ gestrichen.
4. Nach § 12 wird folgender § 12a eingefügt:

„§ 12a

Zeugenschutz

(1) In den Fällen des § 12 Absatz 1 und 2 Satz 1 obliegt der Bundespolizei der Schutz von Personen, deren Aussage zur Erforschung der Wahrheit von Bedeutung ist oder war. Gleiches gilt für Angehörige dieser Personen und sonstige ihnen nahestehende Personen. Die Bundespolizei unterrichtet die zuständigen Landeskriminalämter unverzüglich von der Übernahme des Zeugenschutzes.

(2) In Einzelfällen können Zeugenschutzmaßnahmen im Einvernehmen zwischen der Bundespolizei und einem Landeskriminalamt durch Polizeibeamtinnen und Polizeibeamte dieses Landes durchgeführt werden. Die Verpflichtung anderer Polizeibehörden, die zur Abwehr von Gefahren erforderlichen unaufschiebbaren Maßnahmen zu treffen, bleibt unberührt.“

5. Nach § 14 wird folgender § 14a eingefügt:

„§ 14a

Befugnisse für den Schutz von Zeugen

(1) Zur Erfüllung ihrer Aufgabe nach § 12a kann die Bundespolizei, soweit nicht dieses Gesetz oder das Zeugenschutz-Harmonisierungsgesetz die Befugnisse besonders regelt, die erforderlichen Maßnahmen treffen, um eine im Einzelfall bestehende Gefahr für Leib, Leben, Gesundheit, Freiheit der Willensentscheidung und -betätigung oder wesentliche Vermögenswerte der in § 12a genannten Personen abzuwehren. Die Maßnahmen können auch nach rechtskräftigem Abschluss des Strafverfahrens, in dem die Aussage erfolgt ist, fortgeführt werden. Für den Fall, dass noch die Strafvollstreckung betrieben wird, sind die Maßnahmen im Einvernehmen mit der Strafvollstreckungsbehörde und im Falle fortdauernder Inhaftierung auch im Einvernehmen mit der Justizvollzugsbehörde durchzuführen.

(2) Über Maßnahmen der Bundespolizei, die nach Absatz 1 getroffen werden, sind die zuständigen Landeskriminalämter und die für die Strafverfolgung zuständige Staatsanwaltschaft unverzüglich zu unterrichten. Nach Erhebung der öffentlichen Klage ist das Gericht unverzüglich zu unterrichten, ob die Bundespolizei Maßnahmen nach Absatz 1 durchführt. Sollen die Maßnahmen eingestellt werden, ist die Staatsanwaltschaft zu unterrichten.“

6. § 21 Absatz 2 wird wie folgt gefasst:

„(2) Zur Verhütung von Straftaten ist eine Erhebung personenbezogener Daten nur zulässig, soweit Tatsachen die Annahme rechtfertigen, dass

1. die Person Straftaten von erheblicher Bedeutung begehen will und die Daten zur Verhütung solcher Straftaten erforderlich sind oder
2. die Person mit einer in Nummer 1 genannten Person nicht nur flüchtig oder in zufälligem Kontakt in Verbindung steht und
  - a) von der Vorbereitung einer Straftat im Sinne von Nummer 1 Kenntnis hat,
  - b) aus der Verwertung der Tat Vorteile ziehen könnte oder
  - c) die Person nach Nummer 1 sich ihrer zur Begehung der Straftat bedienen könnte

und die Verhütung dieser Straftaten auf andere Weise aussichtslos oder wesentlich erschwert wäre.“

7. § 22a Absatz 3 Satz 6 wird wie folgt gefasst:

„§ 28 Absatz 5 Satz 4 und 5 gilt entsprechend.“

8. § 24 Absatz 1 Nummer 2 wird wie folgt gefasst:

„2. dies zur Verhütung oder Vorsorge der künftigen Verfolgung von Straftaten im Sinne des § 12 Absatz 1 erforderlich ist, weil Tatsachen die Annahme rechtfertigen, dass die Gefahr der Begehung einer solchen Straftat besteht, insbesondere der Betroffene verdächtig ist, eine Straftat begangen zu haben und wegen der Art oder Ausführung dieser Tat die Gefahr einer Wiederholung besteht.“

9. Nach § 25 wird folgender § 25a eingefügt:

„§ 25a

Meldeauflagen

(1) Die Bundespolizei kann gegenüber einer Person anordnen, sich an bestimmten Tagen zu bestimmten Zeiten bei einer bestimmten Dienststelle der Bundespolizei zu melden (Meldeaufgabe), wenn

1. Tatsachen die Annahme rechtfertigen, dass die Person eine Straftat nach § 12 Absatz 1 von erheblicher Bedeutung begehen wird, und die Meldeauflage zur vorbeugenden Bekämpfung der Straftat erforderlich ist oder
2. wenn die Meldeauflage zur Durchsetzung einer Ausreiseuntersagung erforderlich ist.

(2) Die Meldeauflage ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, sofern die Voraussetzungen der Anordnung weiterhin vorliegen.“

10. Nach § 27c werden die folgenden §§ 27d und 27e eingefügt:

„§ 27d

Überwachung der Telekommunikation

(1) Die Bundespolizei kann ohne Wissen der betroffenen Person die Telekommunikation einer Person überwachen und aufzeichnen,

1. die nach § 17 oder § 18 verantwortlich ist und dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt, geboten ist,
2. bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines übersehbaren Zeitraums eine zumindest ihrer Art nach konkretisierte Straftat begehen wird, die eine nicht unerhebliche Schädigung der in Nummer 1 genannten Rechtsgüter erwarten lässt,
3. bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie für eine Person nach Nummer 1 bestimmte oder von dieser herrührende Mitteilungen entgegennimmt oder weitergibt, oder
4. bei der bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person nach Nummer 1 deren Telekommunikationsanschluss oder Endgerät benutzen wird

und die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(2) Die Überwachung und Aufzeichnung der Telekommunikation darf ohne Wissen der betroffenen Person in der Weise erfolgen, dass mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird und
2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere in unverschlüsselter Form zu ermöglichen

und bestimmte Tatsachen die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraums eine zumindest ihrer Art nach konkretisierte Straftat im Zusammenhang mit lebensgefährdenden Schleusungen oder Menschenhandel begangen werden wird, die eine nicht unerhebliche Schädigung der in Absatz 1 Nummer 1 genannten Rechtsgüter erwarten lässt. Auf dem informationstechnischen System der betroffenen Person gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

(3) Es ist technisch sicherzustellen, dass

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

3. bei Maßnahmen nach Absatz 2 ausschließlich Inhalte und Umstände der Kommunikation überwacht und aufgezeichnet werden können, die ab dem Zeitpunkt der Anordnung nach Absatz 4 auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(4) Maßnahmen nach den Absätzen 1 und 2 dürfen nur auf Antrag der Präsidentin oder des Präsidenten des Bundespolizeipräsidiums oder der Präsidentin oder des Präsidenten der Bundespolizeidirektion, oder ihrer oder seiner Vertretung, durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung durch die nach Satz 1 Antragsberechtigten getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit die Anordnung nach Satz 2 nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(5) Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist,
3. Art, Umfang und Dauer der Maßnahme,
4. im Falle des Absatzes 2 auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
5. der Sachverhalt sowie
6. eine Begründung.

(6) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes,
4. im Falle des Absatzes 2 auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll, sowie
5. die wesentlichen Gründe.

Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(7) Auf Grund der Anordnung hat jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, der Bundespolizei die Maßnahmen nach Absatz 1 zu ermöglichen und die zur Auskunftserteilung erforderlichen Daten auf dem von der Bundespolizei bestimmten Weg unverzüglich zu übermitteln. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikationsüberwachungsverordnung. Für die Entschädigung der Diensteanbieter ist § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend anzuwenden.

(8) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach den Absätzen 1 und 2 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die

Maßnahme unzulässig. Soweit im Rahmen von Maßnahmen nach den Absätzen 1 und 2 neben einer automatischen Aufzeichnung eine unmittelbare Kenntnisnahme erfolgt, ist die Maßnahme unverzüglich zu unterbrechen, soweit sich während der Überwachung tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Bestehen insoweit Zweifel, darf nur eine automatische Aufzeichnung fortgesetzt werden. Automatische Aufzeichnungen sind unverzüglich dem anordnenden Gericht vorzulegen. Das Gericht entscheidet unverzüglich über die Verwertbarkeit oder Löschung der Daten. Ist die Maßnahme nach Satz 2 unterbrochen worden, so darf sie für den Fall, dass sie nicht nach Satz 1 unzulässig ist, fortgeführt werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach den Absätzen 1 und 2 erlangt worden sind, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist sechs Monate nach der Benachrichtigung nach § 35c oder sechs Monate nach Erteilung der gerichtlichen Zustimmung über das endgültige Absehen von der Benachrichtigung zu löschen. Ist die Datenschutzkontrolle noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.

(9) Bei Gefahr im Verzug kann die Präsidentin oder der Präsident des Bundespolizeipräsidiums oder die Präsidentin oder der Präsident der Bundespolizeidirektion, oder ihre oder seine Vertretung, im Benehmen mit der oder dem Datenschutzbeauftragten des Bundespolizeipräsidiums oder der Bundespolizeidirektion über die Verwertung der Erkenntnisse entscheiden. Bei der Sichtung der erhobenen Daten kann sie oder er sich der technischen Unterstützung von zwei weiteren Bediensteten der Bundespolizei bedienen, von denen eine oder einer die Befähigung zum Richteramt haben muss. Die Bediensteten der Bundespolizei sind zur Verschwiegenheit über die ihnen bekannt werdenden Erkenntnisse, die nicht verwertet werden dürfen, verpflichtet. Die gerichtliche Entscheidung nach Absatz 8 Satz 5 ist unverzüglich nachzuholen.

#### § 27e

##### Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten

(1) Die Bundespolizei kann unter den Voraussetzungen des § 27d Absatz 1 durch technische Mittel ermitteln:

1. die Gerätenummer eines Mobilfunkendgeräts und die Kartennummer der darin verwendeten Karte sowie
2. den Standort eines Mobilfunkendgeräts.

(2) Personenbezogene Daten Dritter dürfen anlässlich einer Maßnahme nach Absatz 1 nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zwecks nach Absatz 1 unvermeidbar ist. Über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer hinaus dürfen sie nicht verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen.

(3) § 27d Absatz 4 und 6 Satz 1 und 5 gilt entsprechend. Die Anordnung ist auf höchstens sechs Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als sechs Monate ist zulässig, soweit die in Absatz 1 bezeichneten Voraussetzungen fortbestehen.

(4) Auf Grund der Anordnung einer Maßnahme nach Absatz 1 Nummer 2 hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, der Bundespolizei die für die Ermittlung des Standortes des Mobilfunkendgeräts erforderliche Geräte- und Kartennummer unverzüglich mitzuteilen.“

11. § 28 wird wie folgt geändert:

- a) Absatz 1 Satz 1 wird wie folgt geändert:
  - aa) In Nummer 1 wird das Wort „oder“ am Ende gestrichen.

bb) Nummer 2 wird durch die folgenden Nummern 2 und 3 ersetzt:

- „2. Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise Straftaten im Sinne des § 12 Absatz 1 mit erheblicher Bedeutung, gewerbs-, gewohnheits-, bandenmäßig oder als kriminelle Vereinigung begehen werden, oder
3. Personen, die mit einer in Nummer 2 genannten Person entsprechend § 21 Absatz 2 Nummer 2 in Verbindung stehen,“

b) Die Absätze 3 bis 5 werden wie folgt gefasst:

„(3) Maßnahmen nach

1. Absatz 2 Nummer 1,
2. Absatz 2 Nummer 2 Buchstabe a, bei denen durchgehend länger als 24 Stunden oder an mehr als zwei Tagen Bildaufzeichnungen bestimmter Personen angefertigt werden sollen,
3. Absatz 2 Nummer 2 Buchstabe b,
4. Absatz 2 Nummer 3 und 4, die sich gegen eine bestimmte Person richten oder bei denen die Vertrauensperson oder der Verdeckte Ermittler eine Wohnung betritt, die nicht allgemein zugänglich ist,

dürfen nur durch das Gericht angeordnet werden.

Maßnahmen nach Satz 1 Nummer 3 und 4 dürfen nur auf Antrag der Präsidentin oder des Präsidenten des Bundespolizeipräsidiums oder der Präsidentin oder des Präsidenten der Bundespolizeidirektion, ihrer oder seiner Vertretung, oder durch die Leiterin oder den Leiter einer Abteilung des Bundespolizeipräsidiums durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung einer Maßnahme nach Satz 1 durch die nach Satz 2 Antragsberechtigten getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit die Anordnung nach Satz 2 nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft. Die übrigen Maßnahmen nach Absatz 2 Nummer 2 bis 4 dürfen, außer bei Gefahr im Verzug, nur durch die nach Satz 2 Antragsberechtigten angeordnet werden.

(4) Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. Art, Umfang und Dauer der Maßnahme,
3. der Sachverhalt sowie
4. eine Begründung.

(5) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. Art, Umfang und Dauer der Maßnahme sowie
3. die wesentlichen Gründe.

Die Anordnung ist auf höchstens einen Monat zu befristen; im Falle des Absatzes 2 Nummer 3 und 4 ist die Maßnahme auf höchstens drei Monate zu befristen. Die Verlängerung der Maßnahme bedarf einer neuen Anordnung. Absatz 3 Satz 4 und 5 gilt entsprechend. Zuständig ist das Amtsgericht, in dessen Bezirk die Bundespolizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.“

- c) Die Absätze 7 bis 9 werden durch die folgenden Absätze 7 und 8 ersetzt:

„(7) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 2 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Ergeben sich bei Maßnahmen nach Absatz 2 Nummer 3 und 4 während der Durchführung tatsächliche Anhaltspunkte dafür, dass der Kernbereich betroffen ist, ist die Maßnahme zu unterbrechen, sobald dies ohne Gefährdung der beauftragten Person möglich ist. Soweit im Rahmen einer Maßnahme nach Absatz 2 Nummer 1 und 2 eine unmittelbare Kenntnisnahme, auch neben einer automatischen Aufzeichnung, erfolgt, ist die Maßnahme unverzüglich zu unterbrechen, soweit sich während der Überwachung tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Bestehen insoweit Zweifel, darf die Maßnahme in den Fällen des Absatzes 2 Nummer 2 als automatische Aufzeichnung weiter fortgesetzt werden. Automatische Aufzeichnungen nach Satz 3 sind unverzüglich dem anordnenden Gericht vorzulegen. Das Gericht entscheidet unverzüglich über die Verwertbarkeit oder Löschung der Daten. Ist die Maßnahme nach Satz 3 unterbrochen worden, so darf sie für den Fall, dass sie nicht nach Satz 1 unzulässig ist, fortgeführt werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 2 erlangt worden sind, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist sechs Monate nach der Benachrichtigung nach § 35c oder sechs Monate nach Erteilung der gerichtlichen Zustimmung über das endgültige Absehen von der Benachrichtigung zu löschen. Ist die Datenschutzkontrolle noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.“

(8) Bei Gefahr in Verzug kann die Präsidentin oder der Präsident des Bundespolizeipräsidiums oder die Präsidentin oder der Präsident der Bundespolizeidirektion, ihre oder seine Vertretung, im Benehmen mit der oder dem Datenschutzbeauftragten des Bundespolizeipräsidiums oder der Bundespolizeidirektion über die Verwertung der Erkenntnisse entscheiden. Bei der Sichtung der erhobenen Daten kann sie oder er sich der technischen Unterstützung von zwei weiteren Bediensteten der Bundespolizei bedienen, von denen eine oder einer die Befähigung zum Richteramt haben muss. Die Bediensteten der Bundespolizei sind zur Verschwiegenheit über die ihnen bekannt gewordenen Erkenntnisse, die nicht verwertet werden dürfen, verpflichtet. Die gerichtliche Entscheidung nach Absatz 7 Satz 6 ist unverzüglich nachzuholen.“

12. § 28a wird wie folgt geändert:

- a) Absatz 2 wird wie folgt gefasst:

„(2) Ergeben sich bei der Maßnahme während der Durchführung tatsächliche Anhaltspunkte dafür, dass der Kernbereich privater Lebensgestaltung betroffen ist, ist die Maßnahme zu unterbrechen, sobald dies ohne Gefährdung der von der Bundespolizei beauftragten Personen möglich ist. Wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Aufzeichnungen über Vorgänge, die den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen. Erkenntnisse über solche Vorgänge dürfen nicht verwertet werden. Die Tatsache der Erfassung der Daten und ihrer Löschung sind zu dokumentieren. Diese Daten dürfen ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden. Sie sind sechs Monate nach der Benachrichtigung nach § 35c oder sechs Monate nach Erteilung der gerichtlichen Zustimmung über das endgültige Absehen von der Benachrichtigung zu löschen. Ist die Datenschutzkontrolle noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.“

- b) Absatz 5 Satz 2 wird aufgehoben.

13. Nach § 28a wird folgender § 28b eingefügt:

„§ 28b

Einsatz technischer Mittel gegen fernmanipulierte Geräte

Zur Abwehr einer Gefahr, die von fernmanipulierten Geräten ausgeht, die an Land, in der Luft oder zu Wasser betrieben werden, kann die Bundespolizei geeignete technische Mittel gegen das Fahrzeug, dessen Steuerungseinheit oder Steuerungsverbindung einsetzen, wenn die Abwehr der Gefahr durch andere Maßnahmen, insbesondere gegen die nach § 17 verantwortlichen Personen, aussichtslos oder wesentlich erschwert wäre. Für Maßnahmen zur Abwehr der in Satz 1 bezeichneten Gefahren kann die Bundespolizei technische Mittel zur Erkennung einer Gefahr einsetzen.“

14. Die Überschrift des Teils 2 wird wie folgt gefasst:

„Teil 2

Weiterverarbeitung und Übermittlung von Daten“.

15. § 29 wird durch die folgenden §§ 29 bis 29e ersetzt:

„§ 29

Weiterverarbeitung personenbezogener Daten

Die Bundespolizei kann personenbezogene Daten weiterverarbeiten, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist und soweit dieses Gesetz keine zusätzlichen besonderen Voraussetzungen vorsieht. Sie kann ferner personenbezogene Daten weiterverarbeiten, soweit dies zur Erledigung besonderer Ersuchen nach § 17 Absatz 2 des Bundesverfassungsschutzgesetzes erforderlich ist. Die Sätze 1 und 2 gelten auch für personenbezogene Daten, die die Bundespolizei ohne Anforderung von Dritten erhalten hat.

§ 29a

Zweckbindung, Grundsatz der hypothetischen Datenneuerhebung

- (1) Die Bundespolizei kann personenbezogene Daten, die sie selbst erhoben hat, weiterverarbeiten
1. zur Erfüllung derselben Aufgabe und
  2. zum Schutz derselben Rechtsgüter oder zur Verfolgung oder Verhütung derselben Straftaten.
- (2) Die Bundespolizei kann zur Erfüllung ihrer Aufgaben personenbezogene Daten zu anderen Zwecken, als denjenigen, zu denen sie erhoben worden sind, weiterverarbeiten, wenn
1. mindestens
    - a) vergleichbar schwerwiegende Straftaten verhütet, aufgedeckt oder verfolgt oder
    - b) vergleichbar bedeutsame Rechtsgüter geschütztwerden sollen und
  2. sich im Einzelfall konkrete Ermittlungsansätze
    - a) zur Verhütung, Aufdeckung oder Verfolgung solcher Straftaten ergeben oder
    - b) zur Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter erkennen lassen.

Die §§ 29d und 34 bleiben unberührt.

(3) Abweichend von Absatz 2 kann die Bundespolizei die vorhandenen Grunddaten einer Person gemäß der Rechtsverordnung nach § 20 des Bundeskriminalamtgesetzes auch weiterverarbeiten, um diese Person zu identifizieren.

(4) Bei der Weiterverarbeitung von personenbezogenen Daten stellt die Bundespolizei durch organisatorische und technische Vorkehrungen sicher, dass die Absätze 1 bis 3 beachtet werden.

### § 29b

#### Daten zu Verurteilten, Beschuldigten, Tatverdächtigen und sonstigen Anlasspersonen

(1) Die Bundespolizei kann, soweit gesetzlich nichts anderes bestimmt ist, personenbezogene Daten weiterverarbeiten, die sie bei Wahrnehmung der polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung über

1. Verurteilte,
2. Beschuldigte,
3. Personen, die einer Straftat verdächtig sind, sofern die Weiterverarbeitung der Daten erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind, und
4. Personen, bei denen Anlass zur Weiterverarbeitung der Daten besteht, weil tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffenen Personen in naher Zukunft Straftaten von erheblicher Bedeutung begehen werden (Anlasspersonen)

erlangt hat, soweit dies zur Abwehr von Gefahren im Rahmen der der Bundespolizei obliegenden Aufgaben oder für Zwecke künftiger Strafverfahren wegen Straftaten im Sinne des § 12 Absatz 1 erforderlich ist.

(2) Die Bundespolizei kann weiterverarbeiten

1. von Personen nach Absatz 1 Nummer 1 bis 4
  - a) die Grunddaten gemäß der Rechtsverordnung nach § 20 des Bundeskriminalamtgesetzes und
  - b) soweit erforderlich, andere zur Identifizierung geeignete Merkmale,
  - c) die kriminalaktenführende Dienststelle der Bundespolizei und die Kriminalaktennummer,
  - d) die Tatzeiten und Tatorte und
  - e) die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere Bezeichnung der Straftaten oder Ordnungswidrigkeiten;
2. von Personen nach Absatz 1 Nummer 1 und 2 weitere personenbezogene Daten, soweit die Weiterverarbeitung der Daten erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind;
3. von Personen nach Absatz 1 Nummer 3 und 4 weitere personenbezogene Daten.

(3) Die Bundespolizei kann personenbezogene Daten weiterverarbeiten, um festzustellen, ob die betreffenden Personen die Voraussetzungen nach Absatz 1 erfüllen. Die Daten dürfen ausschließlich zu diesem Zweck weiterverarbeitet werden. Die Daten sind nach Abschluss der Prüfung, spätestens jedoch nach zwölf Monaten zu löschen, soweit nicht festgestellt wurde, dass die betreffende Person die Voraussetzungen nach Absatz 1 erfüllt.

(4) Wird der Beschuldigte rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt, ist die Weiterverarbeitung unzulässig, wenn sich aus den Gründen der Entscheidung ergibt, dass er die Tat nicht oder nicht rechtswidrig begangen hat.

#### § 29c

##### Daten zu anderen Personen

- (1) Die Bundespolizei kann nach Maßgabe von § 29 personenbezogene Daten solcher Personen,
1. die bei einer künftigen Strafverfolgung als Zeugen in Betracht kommen,
  2. die als Opfer einer künftigen Straftat in Betracht kommen,
  3. die mit in § 29b Absatz 1 Nummer 1 bis 3 bezeichneten Personen nicht nur flüchtig oder in zufälligem Kontakt und in einer Weise in Verbindung stehen, die erwarten lässt, dass Hinweise für die Verfolgung oder vorbeugende Bekämpfung dieser Straftaten gewonnen werden können, weil Tatsachen die Annahme rechtfertigen, dass die Personen von der Planung oder der Vorbereitung der Straftaten oder der Verwertung der Tatvorteile Kenntnis haben oder daran mitwirken, oder
  4. die Hinweisgeber oder sonstige Auskunftspersonen sind,

außer zur Abwehr einer Gefahr nur dann weiterverarbeiten, wenn Anhaltspunkte dafür vorliegen, dass dies zur Verhütung von Straftaten im Sinne des § 12 Absatz 1 mit erheblicher Bedeutung oder für Zwecke künftiger Strafverfahren wegen solcher Straftaten erforderlich ist. Die Weiterverarbeitung nach Satz 1 ist zu beschränken auf die in § 29b Absatz 2 Nummer 1 bis 3 bezeichneten Daten sowie auf die Angabe, in welcher Eigenschaft der Person und in Bezug auf welchen Sachverhalt die Weiterverarbeitung der Daten erfolgt. Personenbezogene Daten über Personen nach Absatz 1 Nummer 1, 2 und 4 dürfen nur mit Einwilligung der betroffenen Person weiterverarbeitet werden. Die Einwilligung ist nicht erforderlich, wenn das Bekanntwerden der Speicherungsabsicht den mit der Speicherung verfolgten Zweck gefährden würde.

(2) Die Bundespolizei kann personenbezogene Daten weiterverarbeiten, um festzustellen, ob die betreffenden Personen die Voraussetzungen nach Absatz 1 erfüllen. Die Daten dürfen ausschließlich zu diesem Zweck weiterverarbeitet werden. Die Daten sind nach Abschluss der Prüfung, spätestens jedoch nach zwölf Monaten zu löschen, soweit nicht festgestellt wurde, dass die betreffende Person die Voraussetzungen nach Absatz 1 erfüllt.

#### § 29d

##### Weiterverarbeitung von Daten zur Aus- und Fortbildung, zur Vorgangsverwaltung oder zur befristeten Dokumentation des polizeilichen Handelns

(1) Die Bundespolizei kann bei ihr vorhandene personenbezogene Daten zur polizeilichen Aus- und Fortbildung weiterverarbeiten. Die Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren. Die Anonymisierung kann unterbleiben, wenn

1. sie nur mit unverhältnismäßigem Aufwand möglich ist und die berechtigten Interessen der betroffenen Person an der Geheimhaltung der Daten nicht offensichtlich überwiegen oder
2. der Aus- und Fortbildungszweck mit anonymisierten Daten nicht erreicht werden kann und die berechtigten Interessen der betroffenen Person an der Geheimhaltung der Daten nicht offensichtlich überwiegen.

Eine solche Weiterverarbeitung von personenbezogenen Daten, die aus den in § 27d genannten Maßnahmen erlangt wurden, ist ausgeschlossen.

(2) Die Bundespolizei kann personenbezogene Daten zur Vorgangsverwaltung oder zur befristeten Dokumentation des polizeilichen Handelns weiterverarbeiten. Die §§ 29a bis 29c finden keine Anwendung.

## § 29e

## Kennzeichnung

(1) Bei der Speicherung sind personenbezogene Daten wie folgt zu kennzeichnen:

1. Angabe des Mittels der Erhebung der Daten einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden,
2. Angabe der Kategorie nach den §§ 29b und 29c bei Personen, zu denen Grunddaten angelegt wurden,
3. Angabe der
  - a) Rechtsgüter oder sonstiger Rechte, deren Schutz die Erhebung dient, oder
  - b) Straftaten oder Ordnungswidrigkeiten, deren Verfolgung oder Verhütung die Erhebung dient,
4. Angabe der Stelle, die sie erhoben hat, sofern nicht die Bundespolizei die Daten erhoben hat.

Die Kennzeichnung nach Satz 1 Nummer 1 kann auch durch Angabe der Rechtsgrundlage der jeweiligen Mittel der Datenerhebung ergänzt werden. Personenbezogene Daten, die die Bundespolizei ohne Anforderung von einem Dritten erhalten hat, sind, soweit möglich, nach Satz 1 zu kennzeichnen; dabei sind die erste datenverarbeitende Stelle und der Dritte, von dem die Daten erlangt wurden, soweit möglich, anzugeben.

(2) Personenbezogene Daten, die nicht entsprechend den Anforderungen des Absatzes 1 gekennzeichnet sind, dürfen so lange nicht weiterverarbeitet oder übermittelt werden, bis eine Kennzeichnung entsprechend den Anforderungen des Absatzes 1 erfolgt ist.

(3) Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung nach Absatz 1 durch diese Stelle aufrechtzuerhalten.

(4) Personenbezogene Daten, die nach den §§ 26 bis 27c und 41a erhoben worden sind, müssen erst mit der Speicherung in einem Vorgangs- oder Fallbearbeitungssystem gekennzeichnet werden.

(5) Abweichend von Absatz 2 ist eine Weiterverarbeitung oder Übermittlung personenbezogener Daten auch zulässig nach den Bestimmungen der für die Daten am ... [einsetzen: Datum des Tages vor dem Tag des Inkrafttretens dieses Gesetzes nach Artikel 4] jeweils geltenden Errichtungsanordnung nach § 36 des Bundespolizeigesetzes in der bis zum ... [einsetzen: Datum des Tages vor dem Tag des Inkrafttretens dieses Gesetzes nach Artikel 4] geltenden Fassung.“

16. § 31 Absatz 4 Satz 6 wird wie folgt gefasst:

„§ 28 Absatz 5 Satz 5 findet Anwendung.“

17. Nach § 31 wird folgender § 31a eingefügt:

## „§ 31a

Ausschreibungen von Personen und Sachen zur gezielten und verdeckten Kontrolle oder Ermittlungsanfrage im Schengener Informationssystem

(1) Die Bundespolizei kann im Rahmen ihrer Aufgaben nach § 1 Absatz 2 und 3 sowie den §§ 2 bis 7, 12 und 12a personenbezogene Daten der in § 30 Absatz 1 Satz 1 bezeichneten Art im Schengener Informationssystem zur gezielten und verdeckten Kontrolle oder Ermittlungsanfrage nach Maßgabe des für die Inbetriebnahme des Schengener Informationssystems geltenden Unionsrechts ausschreiben.

(2) Die Ausschreibung zur Ermittlungsanfrage nach Absatz 1 darf nur eine Erhebung von Informationen nach § 22 bezwecken.“

18. Der bisherige § 31a wird § 31b.

19. § 32 wird wie folgt gefasst:

„§ 32

Übermittlung personenbezogener Daten im innerstaatlichen Bereich

(1) Die Bundespolizei kann unter Beachtung von § 29a Absatz 2 und 3 Behörden des Polizeivollzugsdienstes und, wenn sie Aufgaben nach § 2 Absatz 2 oder Aufgaben auf dem Gebiet der Strafverfolgung wahrnehmen, Behörden der Zollverwaltung personenbezogene Daten übermitteln, soweit dies zur Erfüllung polizeilicher Aufgaben erforderlich ist.

(2) Die Bundespolizei kann personenbezogene Daten unter Beachtung von § 29a Absatz 2 und 3 an andere inländische öffentliche Stellen übermitteln, soweit dies erforderlich ist zur

1. Erfüllung einer ihr obliegenden Aufgabe,
2. Abwehr von Gefahren,
3. Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Einzelner,
4. Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Strafvollstreckung und zum Strafvollzug oder
5. Erledigung besonderer Ersuchen nach § 17 Absatz 2 des Bundesverfassungsschutzgesetzes.

(3) Die Bundespolizei kann personenbezogene Daten unter Beachtung von § 29a Absatz 2 und 3 an inländische nicht öffentliche Stellen übermitteln, soweit dies zulässig und erforderlich ist zur

1. Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl,
2. Erfüllung einer ihr obliegenden Aufgabe, oder
3. Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Einzelner.

(4) In den Fällen der Absätze 2 bis 3 darf die Übermittlung von Daten, die § 41 oder § 61 des Bundeszentralregistergesetzes unterfallen, nicht zu einer Erweiterung des Kreises der dort bezeichneten Stellen führen. Die Verwertungsverbote nach den §§ 51, 52 und 63 des Bundeszentralregistergesetzes sind zu beachten.

(5) Der Empfänger darf die übermittelten personenbezogenen Daten nur zu dem Zweck verarbeiten, für den sie ihm übermittelt worden sind. Eine Verarbeitung für andere Zwecke ist unter Beachtung des § 29a Absatz 2 und 3 zulässig; im Falle des Absatzes 3 gilt dies nur, soweit zusätzlich die Bundespolizei zustimmt. Bei Übermittlungen an nicht öffentliche Stellen hat die Bundespolizei die empfangende Stelle darauf hinzuweisen.

(6) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die Bundespolizei. Erfolgt die Übermittlung auf Grund eines Ersuchens einer öffentlichen Stelle nach den Absätzen 1 und 2, trägt diese die Verantwortung. In diesem Fall prüft die Bundespolizei nur, ob das Ersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht.

(7) Die Bundespolizei hat Anlass, Inhalt, Empfänger und Tag der Übermittlung zu dokumentieren. In den Fällen des Absatzes 3 hat die Bundespolizei einen Nachweis zu führen, aus dem die in Satz 1 bezeichneten Angaben sowie die Aktenfundstelle ersichtlich sind. Die Nachweise sind gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr ihrer Erstellung folgt, zu vernichten. Die Vernichtung unterbleibt, solange der Nachweis für Zwecke der Datenschutzkontrolle benötigt wird oder Grund zu der Annahme besteht, dass im Fall einer Vernichtung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden.

(8) Sind mit personenbezogenen Daten, die nach den Absätzen 1 und 2 übermittelt werden dürfen, weitere personenbezogene Daten der betroffenen Person oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unverhältnismäßigem 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 Verwendung dieser Daten ist unzulässig.

(9) Die Einrichtung eines automatisierten Abrufverfahrens, das die Übermittlung von bei der Bundespolizei verarbeiteten personenbezogenen Daten ermöglicht, ist nur zur Erfüllung polizeilicher Aufgaben mit Zustimmung des Bundesministeriums des Innern, für Bau und Heimat zulässig, soweit diese Form der Datenübermittlung unter Berücksichtigung der schutzwürdigen Interessen der betroffenen Person wegen der Vielzahl der Übermittlungen oder wegen ihrer besonderen Eilbedürftigkeit angemessen ist. Die Berechtigung zum Abruf darf, soweit gesetzlich nichts anderes bestimmt ist, nur den in Absatz 1 bezeichneten Stellen eingeräumt werden.

(10) Die Bundespolizei darf zur Erfüllung ihrer Aufgaben auch außerhalb des polizeilichen Informationsverbunds nach § 2 Absatz 3 des Bundeskriminalamtgesetzes an einem polizeilichen Datenverbund mit anderen Landes- und Bundesbehörden teilnehmen, der auch eine automatisierte Datenübermittlung ermöglicht.

(11) Völkerrechtliche Vereinbarungen über die Übermittlung personenbezogener Daten bleiben unberührt.“

20. Die §§ 32a und 33 werden durch die folgenden §§ 32a bis 33 ersetzt:

#### „§ 32a

Übermittlung personenbezogener Daten an Mitgliedstaaten der Europäischen Union und Schengen assoziierte Staaten

§ 32 gilt entsprechend für die Übermittlung von personenbezogenen Daten an

1. öffentliche und nicht öffentliche Stellen in Mitgliedstaaten der Europäischen Union,
2. zwischen- und überstaatliche Stellen der Europäischen Union oder deren Mitgliedstaaten, die mit Aufgaben der Verhütung und Verfolgung von Straftaten befasst sind und
3. öffentliche und nicht öffentliche Stellen in Staaten, welche die Bestimmungen des Schengen-Besitzstandes aufgrund eines Assoziierungsübereinkommens mit der Europäischen Union über die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes anwenden.

Die Verantwortung für die Zulässigkeit der Datenübermittlung trägt die Bundespolizei.

#### § 32b

Übermittlung personenbezogener Daten im internationalen Bereich

(1) Die Bundespolizei kann unter Beachtung des § 29a Absatz 2 und 3 und unter Beachtung der §§ 78 bis 80 des Bundesdatenschutzgesetzes an Polizei- und Justizbehörden sowie an sonstige für die Verhütung oder Verfolgung von Straftaten zuständige öffentliche Stellen in anderen als den in § 32a genannten Staaten (Drittstaaten) und an andere als die in § 32a genannten zwischen- und überstaatlichen Stellen, die mit Aufgaben der Verhütung oder Verfolgung von Straftaten befasst sind, personenbezogene Daten übermitteln, soweit dies erforderlich ist

1. zur Erfüllung einer ihr obliegenden Aufgabe,
2. zur Abwehr einer im Einzelfall bestehenden erheblichen Gefahr für die öffentliche Sicherheit.

Entsprechendes gilt, wenn Anhaltspunkte dafür vorliegen, dass Straftaten von erheblicher Bedeutung begangen werden sollen.

(2) Die Bundespolizei kann unter den Voraussetzungen des § 81 des Bundesdatenschutzgesetzes und unter Beachtung des § 29a Absatz 2 und 3 personenbezogene Daten an die in § 81 des Bundesdatenschutzgesetzes genannten Stellen übermitteln. Zusätzlich kann sie unter den Voraussetzungen des Satzes 1 an andere als die in Absatz 1 genannten zwischen- und überstaatlichen Stellen personenbezogene Daten übermitteln, soweit dies erforderlich ist

1. zur Erfüllung einer ihr obliegenden Aufgabe oder
2. zur Abwehr einer im Einzelfall bestehenden erheblichen Gefahr für die öffentliche Sicherheit.

Entsprechendes gilt, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass Straftaten von erheblicher Bedeutung begangen werden sollen.

(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die Bundespolizei. Die Bundespolizei hat die Übermittlung und ihren Anlass aufzuzeichnen. Die empfangende Stelle personenbezogener Daten ist darauf hinzuweisen, dass sie nur zu dem Zweck genutzt werden dürfen, zu dem sie übermittelt worden sind. Ferner ist ihr der bei der Bundespolizei vorgesehene Lösungszeitpunkt mitzuteilen.

(4) Besondere Rechtsvorschriften über die Übermittlung personenbezogener Daten bleiben unberührt.

### § 33

#### Übermittlungsverbote und Verweigerungsgründe

(1) Die Übermittlung unterbleibt, wenn für die Bundespolizei erkennbar ist, dass unter Berücksichtigung der Art der Daten und ihrer Erhebung die schutzwürdigen Interessen der betroffenen Person das Allgemeininteresse an der Übermittlung überwiegen.

(2) Die Datenübermittlung nach den §§ 32a und 32b unterbleibt über die in Absatz 1 genannten Gründe hinaus auch dann,

1. wenn hierdurch wesentliche Sicherheitsinteressen des Bundes oder der Länder beeinträchtigt würden,
2. wenn hierdurch der Erfolg laufender Ermittlungen oder Leib, Leben oder Freiheit einer Person gefährdet würde,
3. soweit Grund zu der Annahme besteht, dass durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde,
4. wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung der Daten zu den in der Charta der Grundrechte der Europäischen Union enthaltenen Grundsätzen, insbesondere dadurch, dass durch die Nutzung der übermittelten Daten im Empfängerstaat Verletzungen von elementaren rechtsstaatlichen Grundsätzen oder Menschenrechtsverletzungen drohen, in Widerspruch stünde.“

21. § 33a wird aufgehoben.

22. Nach § 34 wird folgender § 34a eingefügt:

#### „§ 34a

##### Speicherung von DNA-Identifizierungsmustern zur Erkennung von DNA-Trugspuren

(1) Die Bundespolizei kann von ihren Beschäftigten, die Umgang mit Spurenmaterial haben oder die Bereiche in ihren Liegenschaften und Einrichtungen betreten müssen, in denen mit Spurenmaterial umgegangen oder dieses gelagert wird,

1. mittels eines Mundschleimhautabstrichs oder einer hinsichtlich ihrer Eingriffsintensität vergleichbaren Methode Körperzellen entnehmen,
2. diese zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersuchen und
3. die festgestellten DNA-Identifizierungsmuster mit den an Spurenmaterial festgestellten DNA-Identifizierungsmustern automatisiert abgleichen,

um zur Erkennung von DNA-Trugspuren festzustellen, ob an Spurenmaterial festgestellte DNA-Identifizierungsmuster von diesen Personen stammen. Die Entnahme der Körperzellen darf nicht erzwungen werden. Die entnommenen Körperzellen dürfen nur für die in Satz 1 genannte molekulargenetische Untersuchung

verwendet werden; sie sind unverzüglich zu vernichten, sobald sie hierfür nicht mehr erforderlich sind. Bei der Untersuchung dürfen andere Feststellungen als diejenigen, die zur Ermittlung des DNA-Identifizierungsmusters erforderlich sind, nicht getroffen werden; hierauf gerichtete Untersuchungen sind unzulässig.

(2) Untersuchungen und Abgleiche nach Absatz 1 bei Personen, die nicht Mitarbeiterinnen und Mitarbeiter der Bundespolizei sind, dürfen nur mit deren schriftlicher Einwilligung erfolgen.

(3) Die nach den Absätzen 1 und 2 erhobenen Daten sind zu pseudonymisieren und darüber hinaus in einem gesonderten Informationssystem zu speichern. Eine Verwendung dieser Daten zu anderen als den in den Absätzen 1 und 2 genannten Zwecken ist unzulässig. Die DNA-Identifizierungsmuster sind zu löschen, wenn sie für die genannten Zwecke nicht mehr erforderlich sind. Die Löschung hat spätestens drei Jahre nach dem letzten Umgang der betreffenden Person mit Spurenmaterial oder dem letzten Zutritt zu einem in Absatz 1 Satz 1 genannten Bereich zu erfolgen. Betroffene Personen sind schriftlich über den Zweck und die Weiterverarbeitung sowie die Löschung der erhobenen Daten zu informieren.“

23. § 35 wird wie folgt gefasst:

#### „§ 35

##### Aussonderungsprüffristen

(1) Die Bundespolizei prüft nach § 75 des Bundesdatenschutzgesetzes bei der Einzelfallbearbeitung und nach festgesetzten Fristen, ob gespeicherte personenbezogene Daten zu berichtigen oder zu löschen sind. Die Aussonderungsprüffristen nach § 75 Absatz 3 des Bundesdatenschutzgesetzes dürfen bei Erwachsenen zehn Jahre, bei Jugendlichen fünf Jahre und bei Kindern zwei Jahre nicht überschreiten, wobei nach Zweck der Speicherung sowie Art und Schwere des Sachverhalts zu unterscheiden ist. Die Beachtung der Aussonderungsprüffristen ist durch geeignete technische Maßnahmen zu gewährleisten.

(2) In den Fällen von § 29c Absatz 1 dürfen die Aussonderungsprüffristen bei Erwachsenen fünf Jahre und bei Jugendlichen drei Jahre nicht überschreiten. Personenbezogene Daten der in § 29c Absatz 1 Satz 1 Nummer 1, 2 und 4 bezeichneten Personen können ohne Zustimmung der betroffenen Person nur für die Dauer eines Jahres gespeichert werden. Die Speicherung für jeweils ein weiteres Jahr ist zulässig, soweit die Voraussetzungen des § 29c Absatz 1 weiterhin vorliegen. Die maßgeblichen Gründe für die Aufrechterhaltung der Speicherung nach Satz 3 sind aktenkundig zu machen. Die Speicherung nach Satz 2 darf jedoch insgesamt drei Jahre nicht überschreiten.

(3) Die Fristen beginnen mit dem Tag, an dem das letzte Ereignis eingetreten ist, das zur Speicherung der Daten geführt hat, jedoch nicht vor Entlassung der betroffenen Person aus einer Justizvollzugsanstalt oder Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung. Die Speicherung kann über die in Absatz 1 Satz 2 genannten Fristen hinaus auch allein für Zwecke der Vorgangsverwaltung aufrechterhalten werden, sofern dies erforderlich ist; in diesem Falle können die Daten nur noch für diesen Zweck oder zur Behebung einer bestehenden Beweisnot verwendet werden.“

24. Nach § 35 werden die folgenden §§ 35a bis 35f eingefügt:

#### „§ 35a

##### Löschung von durch Besondere Mittel der Datenerhebung oder vergleichbare Maßnahmen erlangten personenbezogenen Daten

(1) Sind personenbezogene Daten, die durch eine Maßnahme nach den §§ 14 und 14a oder durch Maßnahmen nach den §§ 21 bis 28b erlangt worden ist und die nicht dem Kernbereich privater Lebensgestaltung zuzuordnen sind, zur Erfüllung des der Maßnahme zugrundeliegenden Zwecks und für eine etwaige gerichtliche Überprüfung der Maßnahme nicht mehr erforderlich, sind sie unverzüglich zu löschen, soweit keine Weiterverarbeitung der Daten nach den Vorschriften des Abschnitts 2 Unterabschnitt 2 Teil 2 erfolgt. Die Tatsache der Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist sechs Monate nach der Benachrichtigung nach § 35c oder

sechs Monate nach Erteilung der gerichtlichen Zustimmung über das endgültige Absehen von der Benachrichtigung zu löschen. Ist die Datenschutzkontrolle noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.

(2) Absatz 1 gilt entsprechend für personenbezogene Daten, die

1. der Bundespolizei übermittelt worden sind und
2. durch Maßnahmen erlangt wurden, die den Maßnahmen nach § 14 oder den §§ 21 bis 28b entsprechen.

#### § 35b

Berichtigung personenbezogener Daten, Einschränkung der Verarbeitung in Akten und Vernichtung von Akten

(1) Stellt die Bundespolizei die Unrichtigkeit personenbezogener Daten in Akten fest, ist die in § 75 Absatz 1 des Bundesdatenschutzgesetzes genannte Berichtigungspflicht dadurch zu erfüllen, dass dies in der Akte vermerkt oder auf sonstige Weise festgehalten wird. Bestreitet die betroffene Person die Richtigkeit sie betreffender personenbezogener Daten und lässt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, sind die Daten entsprechend zu kennzeichnen, um eine Verarbeitungseinschränkung nach § 58 Absatz 1 Satz 2 des Bundesdatenschutzgesetzes zu ermöglichen.

(2) Die Bundespolizei hat die Verarbeitung personenbezogener Daten in Akten einzuschränken, wenn

1. die Verarbeitung unzulässig ist oder
2. aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass die Kenntnis der Daten zur Erfüllung der der Bundespolizei obliegenden Aufgaben nicht mehr erforderlich ist.

Die Akte ist zu vernichten, wenn sie insgesamt zur Erfüllung der Aufgaben der Bundespolizei nicht mehr erforderlich ist. Die Vernichtung unterbleibt, wenn

1. Grund zu der Annahme besteht, dass andernfalls schutzwürdige Interessen der betroffenen Person beeinträchtigt würden oder
2. die personenbezogenen Daten für Zwecke eines gerichtlichen Verfahrens weiter aufbewahrt werden müssen.

In diesen Fällen ist die Verarbeitung der Daten einzuschränken und sind die Unterlagen mit einem entsprechenden Einschränkungsvermerk zu versehen.

(3) In ihrer Verarbeitung eingeschränkte Daten dürfen nur für den Zweck verarbeitet werden, für den die Vernichtung der Akte unterblieben ist; sie dürfen auch verarbeitet werden, wenn dies zur Behebung einer bestehenden Beweisnot unerlässlich ist oder die betroffene Person einwilligt.

(4) Anstelle der Vernichtung nach Absatz 2 Satz 2 sind die Akten an das zuständige Archiv abzugeben, sofern diesen Unterlagen bleibender Wert im Sinne des § 1 Nummer 10 in Verbindung mit § 3 des Bundesarchivgesetzes zukommt.

(5) § 75 Absatz 4 des Bundesdatenschutzgesetzes gilt entsprechend.

#### § 35c

Benachrichtigung bei verdeckten und eingriffsintensiven Maßnahmen

(1) Über eine Maßnahme nach den §§ 27d, 27e, 28, 28a, 30 bis 31a sind zu benachrichtigen im Fall

1. des § 27d (Telekommunikationsüberwachung) die Beteiligten der überwachten Telekommunikation,
2. des § 27e (Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten) die Zielperson,

3. des § 28a, bei der Vorgänge außerhalb von Wohnungen erfasst wurden, und des § 28 Absatz 2 Nummer 1 und 2 (längerfristige Observation, Bildaufnahmen, Tonaufnahmen) die Zielperson sowie die erheblich mitbetroffenen Personen,
4. des § 28a, bei der Vorgänge innerhalb von Wohnungen erfasst wurden, und des § 28 Absatz 2 Nummer 3 und 4 (Einsatz Vertrauensperson und Verdeckter Ermittler)
  - a) die Zielperson,
  - b) die erheblich mitbetroffenen Personen,
  - c) die Personen, deren nicht allgemein zugängliche Wohnung die beauftragte Person, die Vertrauensperson oder der Verdeckte Ermittler betreten hat,
5. der §§ 30 bis 31a (Ausschreibungen) die Zielperson und die Personen, deren personenbezogene Daten gemeldet worden sind.

Die Benachrichtigung unterbleibt, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen. Zudem kann die Benachrichtigung einer in Satz 1 Nummer 1 bezeichneten Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen ist und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat. Nachforschungen zur Feststellung der Identität einer in Satz 1 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist.

(2) Die Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Zwecks der Maßnahme, des Bestandes des Staates, von Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt, möglich ist. Im Fall des § 28 Absatz 2 Nummer 3 und 4 und des § 28a erfolgt die Benachrichtigung erst, sobald dies auch ohne Gefährdung der Möglichkeit der weiteren Verwendung des Verdeckten Ermittlers oder der Vertrauensperson möglich ist. Wird wegen des zugrundeliegenden Sachverhaltes ein strafrechtliches Ermittlungsverfahren geführt, entscheidet die Strafverfolgungsbehörde entsprechend den Vorschriften des Strafverfahrensrechts, ob eine Benachrichtigung vorgenommen wird. Die Benachrichtigung erfolgt durch die Bundespolizeibehörde, die die Maßnahme veranlasst hat. Wird die Benachrichtigung aus einem der vorgenannten Gründe zurückgestellt, ist dies zu dokumentieren.

(3) Erfolgt die nach Absatz 2 zurückgestellte Benachrichtigung nicht binnen zwölf Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der gerichtlichen Zustimmung. Das Gericht bestimmt die Dauer der weiteren Zurückstellung. Fünf Jahre nach Beendigung der Maßnahme kann mit gerichtlicher Zustimmung endgültig von der Benachrichtigung abgesehen werden, wenn die Voraussetzungen für die Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden, eine weitere Verwendung der Daten gegen den Betroffenen ausgeschlossen ist und die Daten gelöscht werden. Sind mehrere Maßnahmen in einem engen zeitlichen Zusammenhang durchgeführt worden, beginnt die in Satz 1 genannte Frist mit der Beendigung der letzten Maßnahme.

#### § 35d

##### Benachrichtigung über die Speicherung personenbezogener Daten von Kindern

Werden personenbezogene Daten von Kindern, die ohne Kenntnis der Sorgeberechtigten durch die Bundespolizei erhoben worden sind, gespeichert, sind die Sorgeberechtigten zu benachrichtigen, sobald die Aufgabenerfüllung hierdurch nicht mehr gefährdet wird. Von der Benachrichtigung kann abgesehen werden, solange zu besorgen ist, dass die Benachrichtigung zu erheblichen Nachteilen für das Kind führt.

## § 35e

## Protokollierung

(1) Die Protokollierung nach § 76 des Bundesdatenschutzgesetzes erfolgt ergänzend zu den dort genannten Anforderungen in einer Weise, dass die Protokolle

1. den Datenschutzbeauftragten der Bundespolizeibehörden und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in elektronisch auswertbarer Form für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung zur Verfügung stehen und
2. eine Überprüfung ermöglichen, dass Zugriffe auf personenbezogene Daten innerhalb der Zugriffsberechtigungen erfolgen.

(2) Die nach § 76 des Bundesdatenschutzgesetzes und unter Beachtung von Absatz 1 generierten Protokolldaten sind nach zwölf Monaten zu löschen, soweit sie nicht mehr für Zwecke der Datenschutzkontrolle benötigt werden.

## § 35f

## Protokollierung bei verdeckten und eingriffsintensiven Maßnahmen

(1) Bei der Erhebung von Daten nach den §§ 27d, 27e, 28, 28a, 30 bis 31a sind zu protokollieren:

1. das zur Datenerhebung eingesetzte Mittel,
2. der Zeitpunkt des Einsatzes,
3. Angaben, die die Feststellung der erhobenen Daten ermöglichen, sowie
4. die Organisationseinheit, die die Maßnahme durchführt.

(2) Zu protokollieren sind auch

1. bei Maßnahmen nach § 27d
  - a) die Beteiligten der überwachten Telekommunikation sowie
  - b) im Falle, dass Überwachung mit einem Eingriff in von der betroffenen Person genutzte informationstechnische Systeme verbunden ist, die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
2. bei Maßnahmen nach § 27e die Zielperson,
3. bei Maßnahmen nach § 28a, bei denen Vorgänge außerhalb von Wohnungen erfasst wurden, und nach § 28 Absatz 2 Nummer 1 und 2 die Zielperson sowie die erheblich mitbetroffenen Personen,
4. bei Maßnahmen nach § 28a, bei denen Vorgänge innerhalb von Wohnungen erfasst wurden, und nach § 28 Absatz 2 Nummer 3 und 4
  - a) die Zielperson,
  - b) die erheblich mitbetroffenen Personen sowie
  - c) die Personen, deren nicht allgemein zugängliche Wohnung die beauftragte Person, die Vertrauensperson oder der Verdeckte Ermittler betreten haben,
5. bei Maßnahmen nach den §§ 30 bis 31a die Zielperson und die Personen, deren personenbezogene Daten gemeldet worden sind.

(3) Nachforschungen zur Feststellung der Identität einer in Absatz 2 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist. Die Zahl der Personen, deren Protokollierung unterblieben ist, ist im Protokoll anzugeben.

(4) Die Protokolldaten dürfen nur verwendet werden für Zwecke der Benachrichtigung nach § 35c und um der betroffenen Person oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahmen rechtmäßig durchgeführt worden sind. Sie sind nach zwölf Monaten zu löschen, soweit sie nicht mehr für Zwecke der Datenschutzkontrolle benötigt werden.“

25. Die §§ 36 und 37 werden wie folgt gefasst:

#### „§ 36

##### Verzeichnis von Verarbeitungstätigkeiten

(1) Die Bundespolizei nimmt in das Verzeichnis nach § 70 des Bundesdatenschutzgesetzes zusätzlich Angaben auf

1. zu den Zugriffsberechtigungen,
2. zur Übermittlung im Wege eines automatisierten Abrufverfahrens und
3. zur Auftragsverarbeitung.

(2) Das Verzeichnis von Verarbeitungstätigkeiten wird beim Bundespolizeipräsidium geführt. Die Datenschutzbeauftragten der Bundespolizeibehörden sind bei der Erstellung und Aktualisierung zu beteiligen.

(3) Die Bundespolizei stellt das Verzeichnis und dessen Aktualisierungen der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und den Datenschutzbeauftragten der Bundespolizeibehörden zur Verfügung.

#### § 37

Ergänzende Befugnisse der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit führt, unbeschadet ihrer oder seiner in § 14 des Bundesdatenschutzgesetzes genannten Aufgaben, Kontrollen bezüglich der Datenverarbeitung bei Maßnahmen nach den §§ 22a, 27d, 27e, 28 oder § 28a und von Übermittlungen nach § 32b mindestens alle zwei Jahre durch.

(2) Sofern die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Verstöße nach § 16 Absatz 2 des Bundesdatenschutzgesetzes beanstandet hat, kann sie oder er geeignete Maßnahmen anordnen, wenn dies zur Beseitigung eines erheblichen Verstoßes gegen datenschutzrechtliche Vorschriften erforderlich ist.“

26. Die Überschrift des Teils 3 wird wie folgt gefasst:

#### „Teil 3

##### Freiheitsbeschränkende Maßnahmen und Durchsuchung“.

27. Nach § 38 wird folgender § 38a eingefügt:

„§ 38a

Aufenthaltsverbot

Die Bundespolizei kann einer Person für höchstens drei Monate den Aufenthalt an einem Ort untersagen, wenn Tatsachen die Annahme rechtfertigen, dass die Person dort innerhalb eines überschaubaren Zeitraums eine Straftat im Sinne des § 12 Absatz 1 von erheblicher Bedeutung begehen oder zu ihrer Begehung beitragen wird. Das Verbot ist zeitlich und örtlich auf den zur Verhütung der Straftat erforderlichen Umfang zu beschränken. Es hat berechnete Interessen der betroffenen Person zu berücksichtigen. Die Vorschriften des Versammlungsrechts bleiben unberührt.“

28. Nach § 41 wird folgender § 41a eingefügt:

„§ 41a

Bild- und Tonüberwachung von Gewahrsamsräumen

(1) Die Bundespolizei kann in ihren polizeilichen Gewahrsamsräumen durch die offene Anfertigung von Bild- und Tonaufzeichnungen personenbezogene Daten erheben und weiterverarbeiten, soweit diese Maßnahme zum Schutz der festgehaltenen Person oder von anwesenden Polizeivollzugsbeamtinnen oder Polizeivollzugsbeamten erforderlich ist.

(2) Befindet sich keine Polizeivollzugsbeamtin und kein Polizeivollzugsbeamter in dem Gewahrsamsraum der festgehaltenen Person, darf die Bundespolizei durch die offene Anfertigung von Bildaufzeichnungen personenbezogene Daten nur erheben und weiterverarbeiten, soweit dies zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben der festgehaltenen Person oder der höchstens kurzzeitigen Erforschung dieser Gefahr erforderlich ist.

(3) Die Datenerhebung ist für die festgehaltene Person wahrnehmbar und verständlich durch ein optisches oder akustisches Signal anzuzeigen. Der Schutz der Intimsphäre der festgehaltenen Person ist zu wahren.

(4) Beginn, Ende, Umfang und Anlass der Maßnahmen nach den Absätzen 1 und 2 sind zu dokumentieren.

(5) Für die Fälle des Absatzes 1 findet § 27a Absatz 4 entsprechende Anwendung. In den Fällen des Absatzes 2 findet keine Speicherung statt.“

29. § 43 wird wie folgt geändert:

a) Die Überschrift wird wie folgt gefasst:

„§ 43

Durchsuchung von Personen und Entnahme von Blutproben“.

b) Folgender Absatz 6 wird angefügt:

„(6) Die Bundespolizei kann zur Abwehr einer Gefahr für Leib oder Leben die Entnahme von Blutproben anordnen. Dies gilt insbesondere, wenn Tatsachen die Annahme rechtfertigen, dass eine Übertragung besonders gefährlicher Krankheitserreger auf eine andere Person stattgefunden haben könnte. Die Maßnahme bedarf, außer bei Gefahr im Verzug, der richterlichen Anordnung. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Maßnahmen nach Satz 1 dürfen nur von Ärztinnen oder Ärzten durchgeführt werden.“

30. § 62 Absatz 3 wird wie folgt gefasst:

„(3) Die in Absatz 2 genannten Unternehmen stellen die erforderlichen Einrichtungen, insbesondere Dienst- und Lagerräume gemäß den polizeilichen Anforderungen sowie Parkplätze für die Dienstkraftfahrzeuge der Bediensteten der Bundespolizei unentgeltlich zur Verfügung. Soweit die Unternehmen keine oder nicht ausreichend eigene Flächen bereitstellen können, sind sie verpflichtet, der Bundespolizei vergleichbare Ersatzflächen unentgeltlich zur Verfügung zu stellen. Ist dies nicht möglich, da die Unternehmen die für die Wahrnehmung der Aufgabe der Bundespolizei erforderlichen Betriebsflächen nach Inkrafttreten dieses Gesetzes veräußert haben, tritt der Erwerber in die Verpflichtung des Unternehmens ein. Der Umfang der Verpflichtung beschränkt sich auf die zum Zeitpunkt der Veräußerung bereitgestellten Flächen, wenn nicht veränderte Sicherheitslagen einen anderen Flächenbedarf begründen. Sofern den Unternehmen oder Erwerbern die Bereitstellung der erforderlichen Einrichtungen auf Grund bestehender Nutzungsverträge mit Dritten nicht möglich ist, sind sie verpflichtet, auslaufende Verträge nicht zu verlängern. Die Unternehmen oder Erwerber sind verpflichtet, die Einrichtungen in einem guten Zustand zu überlassen und sie während der gesamten Nutzung in diesem Zustand zu erhalten.“

31. In § 69a Absatz 1 wird die Angabe „§ 31a Abs. 1“ durch die Angabe „§ 31b Absatz 1“ ersetzt.

32. Folgender § 71 wird angefügt:

#### „§ 71

##### Berichtspflicht gegenüber dem Deutschen Bundestag

Die Bundespolizei berichtet dem Bundesministerium des Innern, für Bau und Heimat alle zwei Jahre, erstmals bis zum ... [einsetzen: Datum des ersten Tages des vierundzwanzigsten auf die Verkündung folgenden Kalendermonats] über die Ausübung ihrer Befugnisse nach den §§ 26, 27, 27b, 27d, 27e, 28, 28a, 28b, 30 bis 31a und diesbezüglichen Übermittlungen nach § 32b. In dieser Unterrichtung wird insbesondere dargestellt, in welchem Umfang von welchen Befugnissen Gebrauch gemacht wurde und inwieweit die betroffenen Personen hierüber benachrichtigt wurden. Das Bundesministerium des Innern, für Bau und Heimat leitet diese Unterrichtung der Bundesregierung und dem Deutschen Bundestag innerhalb von zwei Monaten zu. Der Deutsche Bundestag macht die Unterrichtung öffentlich zugänglich.“

## Artikel 2

### **Änderung des Gesetzes über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes**

§ 12 Absatz 2 Satz 1 des Gesetzes über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes in der im Bundesgesetzblatt Teil III, Gliederungsnummer 2015, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 43 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt gefasst:

„Ein Schuss, der mit an Sicherheit grenzender Wahrscheinlichkeit tödlich wirken wird, ist nur zulässig, wenn er das einzige Mittel zur Abwehr einer gegenwärtigen Lebensgefahr oder einer gegenwärtigen Gefahr einer schwerwiegenden Verletzung der körperlichen Unversehrtheit ist.“

### Artikel 3

#### Änderung des Aufenthaltsgesetzes

Nach § 71 Absatz 3 des Aufenthaltsgesetzes in der Fassung der Bekanntmachung vom 25. Februar 2008 (BGBl. I S. 162), das zuletzt durch Artikel 10 des Gesetzes vom 9. Dezember 2020 (BGBl. I S. 2855) geändert worden ist, wird folgender Absatz 3a eingefügt:

„(3a) Ungeachtet der Zuständigkeit nach Absatz 3 ist die Bundespolizei für Abschiebungen und Zurückschiebungen von Drittstaatsangehörigen zuständig, sofern

1. diese im Zuständigkeitsbereich der Bundespolizei festgestellt wurden,
2. diese vollziehbar ausreisepflichtig sind und
3. deren Abschiebung nicht ausgesetzt ist oder deren Abschiebung innerhalb von sechs Monaten durchführbar ist, insbesondere, wenn nach § 60a Absatz 2 Satz 1 Alternative 1 die Abschiebung aufgrund von fehlenden Reisedokumenten ausgesetzt ist und nach Einschätzung der Bundespolizei die notwendigen Reisedokumente innerhalb dieser Frist beschafft werden können.

Die Zuständigkeit der Bundespolizei nach Satz 1 endet, wenn

1. im Falle der Aussetzung der Abschiebung aufgrund von fehlenden Reisedokumenten nicht innerhalb von sechs Monaten nach der Feststellung des Drittstaatsangehörigen im Zuständigkeitsbereich der Bundespolizei die Beschaffung von Reisedokumenten gelungen ist und eine Beschaffung nicht unmittelbar bevorsteht oder
2. nach Feststellung des Drittstaatsangehörigen im Zuständigkeitsbereich der Bundespolizei andere rechtliche oder tatsächliche Gründe aufgetreten sind oder fortbestehen, die einer Abschiebung innerhalb von sechs Monaten nach der Feststellung entgegenstehen oder
3. die zuständige oberste Landesbehörde widerspricht.

Die Zuständigkeiten nach Absatz 3 Nummer 1e und 2 gelten in den Fällen des Satzes 1 entsprechend.“

### Artikel 4

#### Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Berlin, den 9. Februar 2021

**Ralph Brinkhaus, Alexander Dobrindt und Fraktion**  
**Dr. Rolf Mützenich und Fraktion**

## Begründung

### A. Allgemeiner Teil

#### I. Zielsetzung und Notwendigkeit der Regelungen

Das geltende Bundespolizeigesetz, das zum überwiegenden Teil noch aus dem Jahr 1994 stammt und nur in einzelnen Vorschriften angepasst worden ist, bedarf einer Modernisierung. Die Bundespolizei soll einzelne neue Aufgaben (unter Wahrung des sonderpolizeilichen Charakters) und ein verbessertes Befugnisinstrumentarium erhalten.

Das Bundesverfassungsgericht hat in seinem Urteil vom 20. April 2016 das bisherige Bundeskriminalamtgesetz in Teilen für verfassungswidrig erklärt. Es hat geurteilt, dass bei solchen Maßnahmen, die tief in das Privatleben Betroffener hineinreichen, besondere Anforderungen an den Verhältnismäßigkeitsgrundsatz zu stellen sind. Insbesondere verlangen die Befugnisse besondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung sowie zum Schutz von Berufsgeheimnisträgern. Sie unterliegen bestimmten Anforderungen an Transparenz, individuellen Rechtsschutz und datenschutzaufsichtliche Kontrolle.

Mit seinem Urteil hat das Bundesverfassungsgericht zudem ein Grundsatzurteil zum polizeilichen Datenschutz gesprochen, mit dem es die bisherige Rechtsprechung zu den einzelnen verdeckten Ermittlungsbefugnissen zusammenführt, sie in übergreifende Prinzipien systematisiert, die verfassungsrechtlichen Anforderungen an Zweckbindung und Zweckänderung von Daten fortentwickelt und erstmals Aussagen zur Übermittlung von Daten an öffentliche Stellen im Ausland trifft. Es hat insbesondere ausgeführt, dass sich die Anforderungen an die Nutzung und Übermittlung staatlich erhobener Daten nach den Grundsätzen der Zweckbindung und Zweckänderung richten und sich die Verhältnismäßigkeitsanforderungen für eine solche Zweckänderung am Grundsatz der hypothetischen Datenneuerhebung zu orientieren haben. Auch die Übermittlung von Daten an öffentliche Stellen im Ausland unterliegt diesen verfassungsrechtlichen Grundsätzen der Zweckänderung und Zweckbindung.

Außerdem ist die Richtlinie (EU) 2016/680 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr umzusetzen. Mit dieser Richtlinie soll der Datenschutz im Polizeibereich weiter harmonisiert werden, um zum einen ein vergleichbar hohes Schutzniveau für personenbezogene Daten – unter anderem durch Stärkung von Betroffenenrechten – zu gewährleisten und zum anderen den unionsweiten Informationsaustausch zu erleichtern und zu verbessern. Die Richtlinie wird weitgehend bereits durch Artikel 3 des Bundesdatenschutzgesetzes umgesetzt. Für die Bundespolizei müssen die Vorschriften ergänzt und spezifiziert werden.

Die erforderliche Überarbeitung wird auch zum Anlass genommen, das Bundespolizeigesetz um bislang fehlende, aber erforderliche Befugnisse, insbesondere im Bereich der Gefahrenabwehr, zu ergänzen.

Im UZwG fehlt eine in der Mehrzahl der Polizeigesetze der Länder enthaltene Regelung des finalen Rettungsschusses.

#### II. Wesentlicher Inhalt des Entwurfs

Der Gesetzentwurf passt die Regelungen zur Erhebung von Daten, die durch den Einsatz verdeckter Maßnahmen erlangt wurden, an die Vorgaben des Bundesverfassungsgerichtsurteils vom 20. April 2016 an. Er führt hierzu umfangreiche Änderungen der Voraussetzungen zur Anordnungsbefugnis – auch durch erweiterte richterliche Kontrollbefugnisse –, zum Schutz des Kernbereichs privater Lebensgestaltung, zur Transparenz, zum individuellen Rechtsschutz, zur aufsichtlichen Kontrolle durch eine unabhängige Stelle und zu Löschungs- und Benachrichtigungspflichten ein.

Zudem setzt der Gesetzentwurf die Vorgaben des Bundesverfassungsgerichts zur Nutzung der in den Datenbeständen der Bundespolizei vorhandenen personenbezogenen Daten und zur Übermittlung dieser Daten an andere nationale und internationale Stellen um. Insbesondere umfasst der Entwurf dabei Regelungen zu den Voraussetzungen, unter denen die Daten zu einem anderen Zweck genutzt werden können, als zu dem sie ursprünglich erhoben worden sind und führt den Grundsatz der hypothetischen Datenerhebung ein.

Des Weiteren enthält der Gesetzesentwurf Vorschriften zum Datenschutz, welche der Umsetzung der EU-Richtlinie 2016/680 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr dienen. Er stärkt insbesondere die Rechte des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, welcher die Befugnis erhält, Maßnahmen zur Beseitigung von erheblichen Verstößen gegen datenschutzrechtliche Vorschriften anzuordnen. Der Gesetzentwurf sieht eine umfassende Protokollierung zum Zwecke der Datenschutzkontrolle vor und verpflichtet die Bundespolizei durch technische und organisatorische Vorkehrungen sicherzustellen, dass die Datenschutzgrundsätze und die Anforderungen an die Datensicherheit bereits bei der Datenverarbeitung beachtet werden. Es wird ein umfassendes Verzeichnis von Verarbeitungstätigkeiten eingerichtet, das das bestehende System der Errichtungsanordnungen ablöst. Die Datenverarbeitung aufgrund von bereits bestehenden Errichtungsanordnungen bleibt aufgrund einer Übergangsregelung weiter zulässig.

Die Harmonisierung und Standardisierung im EU-Kontext zur Verbesserung des Informationsflusses wird durch die Gleichstellung der EU-internen Übermittlungen mit innerstaatlichen Übermittlungen zur Erreichung des unionsrechtlich vorgegebenen Ziels, den freien Datenverkehr auch im Bereich Polizei und Justiz zu erleichtern, die Überarbeitung der Regelungen zur Datenübermittlung an Stellen in Drittstaaten und die neue Systematisierung und Präzisierung der Einschränkungen der Übermittlungsbefugnisse gefördert.

Um eine effektive Kriminalitätsbekämpfung auch künftig gewährleisten zu können, werden auch zusätzliche, neue Befugnisse für die Bundespolizei geschaffen. Hierzu zählt etwa die Überwachung der Telekommunikation (§ 27d), die Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten (§ 27e), der Einsatz technischer Mittel gegen fernmanipulierte Geräte (§ 28b), die Möglichkeit, eine Meldeauflage (25a) oder ein Aufenthaltsverbot (§ 38a) zu erlassen, oder der Schutz von Zeugen (§ 14a).

Der Gesetzentwurf zur Änderung des UZwG sieht die Einführung einer rechtlichen Grundlage für den finalen Rettungsschuss vor, um in besonderen Situationen (z. B. Geiselnahmen, Terroranschlag) ergänzend zu den Notwehrbestimmungen den Schusswaffengebrauch zu legitimieren.

### III. Alternativen

Keine.

### IV. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes für die Regelungen in Artikel 1 des Gesetzentwurfs folgt aus Artikel 73 Absatz 1 Nummern 5 (Grenzschutz), 6 (Luftverkehr) und 6a (Eisenbahnen) des Grundgesetzes (GG), aus Artikel 74 Absatz 1 Nummer 1 GG (Strafverfolgung) sowie aus der Natur der Sache (u. a. Schutz von Bundesorganen, Verwendung zur Unterstützung anderer Bundesbehörden sowie der Länder) sowie für die datenschutzrechtlichen Regelungen als Annex zu den jeweiligen Sachkompetenzen.

Die Gesetzgebungskompetenz des Bundes für Artikel 2 ergibt sich kraft Sachzusammenhangs, insbesondere zu Artikel 1, für Artikel 3 aus Artikel 74 Absatz 1 Nummer 4 in Verbindung mit Artikel 72 Absatz 2 GG. Eine bundeseinheitliche Regelung ist zur Wahrung der Rechtseinheit erforderlich, um einen einheitlichen und umfassenden Vollzug der Ausreisepflicht bei Feststellungen im Zuständigkeitsbereich der Bundespolizei zu ermöglichen.

## 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. Der Gesetzentwurf dient auch der Umsetzung der Richtlinie (EU) 2016/680.

## VI. Gesetzesfolgen

Die Regelungen tragen zum besseren Schutz der öffentlichen Sicherheit bei und verbessern die Rechte der durch die Datenverarbeitung der Bundespolizei betroffenen Personen.

### 1. Rechts- und Verwaltungsvereinfachung

Durch den Wegfall der Errichtungsordnung nach dem bisherigen § 36 entfällt das dort vorgesehene Verwaltungsverfahren, das die Erstellung der Errichtungsanordnung, die Zustimmung des Bundesministeriums des Innern, für Bau und Heimat und die Anhörung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit umfasste.

Aufgrund Übernahme von Zuständigkeiten von den Ländern entfallen Abstimmungsprozesse (§ 12 Absatz 1), bei der Übernahme von Zeugenschutzmaßnahmen (§§ 12a, 14a) auch in Bezug auf das BKA.

### 2. Nachhaltigkeitsaspekte

Der Gesetzentwurf steht im Einklang mit den Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Nationalen Nachhaltigkeitsstrategie. Die Wirkungen des Gesetzentwurfs zielen mittelbar auf eine nachhaltige Entwicklung, weil er der Bundespolizei rechtssichere Befugnisse zum Schutz der Bürgerinnen und Bürger an die Hand gibt. Die Schutzgüter im Wesentlichen aus Artikel 73 GG bilden den strukturellen Rahmen, in dem sich individuelle Sicherheit realisiert. Eine Operationalisierung statistischer Messbarkeit der Wirkungen des Gesetzes in Bezug auf den Nachhaltigkeitsindikator ist daher nicht möglich, mithin sind auch prognostische Einschätzungen gegenständlich nicht eröffnet. Gleichwohl ist davon auszugehen, dass die effektive Aufgabewahrnehmung der Bundespolizei sich positiv niederschlägt. Dies gilt auch für die Stärkung des Datenschutzes zugunsten der Bürgerinnen und Bürger.

### 3. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

### 4. Erfüllungsaufwand

#### 4.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

#### 4.2 Erfüllungsaufwand für die Wirtschaft

Durch § 27d entsteht für die Wirtschaft (Telekommunikationsunternehmen) insofern kein Erfüllungsaufwand, als die Kosten für die Einrichtung der Überwachung eines Anschlusses der Bundesregierung in Rechnung gestellt werden.

Im Übrigen fallen die für die Wirtschaft entstehenden Belastungen nicht unter die sogenannte One-in-one-out-Regel der Bundesregierung, denn die gesetzlichen Änderungen dienen der Gefahrenabwehr.

Die Erweiterung der Unterstützungspflichten auf weitere Unternehmen und von diesen unentgeltlich zu erbringende Unterstützungsleistungen führt zu einer finanziellen Zusatzbelastung der Unternehmen, die nicht näher zu beziffern ist.

Im Gegenzug geht die Abschaffung der Selbstkostenerstattungspflicht im Rahmen des § 62 Absatz 3 mit einer Entlastung des Bundeshaushalts von mindestens 37 Millionen Euro einher.

## 4.3 Erfüllungsaufwand der Verwaltung

## Bundespolizei

Übersicht Bürokratiekosten in Euro					
Vorgabe Prozess	Personalauf- wand jährlich	Personalauf- wand einmalig	Sachaufwand jährlich	Sachaufwand einmalig	Sonstige Kosten
Zeugenschutz § 12a BPolG, § 14a BPolG	868.480		450.000	200.000	
Ermittlungen § 12 Abs. 1 BPolG	4.780.160			940.709	
Meldeauflagen § 25a BPolG	11.192				
VP Führung § 28 BPolG	35.200				
VE Führung § 28 BPolG	35.200				
Grundsatz § 28 BPolG	69.440			12.217	
TKÜ § 27d BPolG	232.407		14.000		
Identifizierung und Lokalisie- rung von Mo- bilfunkkarten und -endgeräten § 27e BPolG	13.968		1.605		
Hypothetische Datenneuerhe- bung § 29a BPolG	1.940.000				
Schulung § 29 bis 29e BPolG		5.200.442			
VBS § 29e BPolG	50.021				
b-case, PIAV § 29a BPolG	126.752				
INPOL § 29e BPolG	126.752				
Referenzdaten- bank/Kontami- nationsfälle § 34a BPolG	2.117	11.912	1.935	19.355	
Benachrichti- gungspflichten § 35c BPolG	43.400				
Protokollie- rungspflichten § 35f BPolG	69.440				

Übersicht Bürokratiekosten in Euro					
Vorgabe Prozess	Personalauf- wand jährlich	Personalauf- wand einmalig	Sachaufwand jährlich	Sachaufwand einmalig	Sonstige Kosten
Video Gewährsam § 41a BPolG			150.000	6.000.000	
Berichtspflicht § 71 BPolG	20.128				
Aufenthaltsbe- endigung § 71 AufenthG	9.012.000		3.460.000		
Gesamtsumme	17.436.657	5.212.354	4.077.540	7.172.281	

Im Einzelnen:

a) Anpassung der Befugnisnormen, Kernbereichsschutz

Die Aufnahme von Bestimmungen für den **Zeugenschutz** in das Bundespolizeigesetz eröffnet eine neue Aufgabe. Für die Berechnung der Kosten wird von jährlich fünf Zeugenschutzfällen ausgegangen. Dadurch entstehen Personalkosten von 870 00 Euro sowie ein jährlicher Sachaufwand von 450 000 Euro und ein einmaliger Sachaufwand von 200 000 Euro.

Die Bundespolizei ist nach dem Inkrafttreten der Neuregelung für die abschließende Bearbeitung von aufgabenbezogenen **Straftatbeständen** (ohne ausgewählte Verbrechenstatbestände), die bisher an die Landespolizei oder den Zoll abgegeben wurden, zuständig. Aus der Übernahme dieser neuen Aufgabe resultiert ein Erfüllungsaufwand für jährliche Personalkosten in Höhe von 4,8 Millionen Euro und 940 000 Euro für den einmaligen Sachaufwand.

Die Einführung einer Befugnis zum Erlass von **Meldeauflagen** stellt einen hohen Mehrwert für die Bundespolizei dar und trägt insbesondere signifikant zur Befriedung des schienenengebundenen Fußballfanreiseverkehrs bei. Hier wird von einer Größenordnung von etwa 150 Fällen je Saison ausgegangen, woraus sich ein jährlicher Personalaufwand in Höhe von 11 192 Euro ergibt.

Der Entscheidungsvorbehalt bei einem präventiven **Einsatz einer Vertrauensperson (VP)**, der sich gegen eine bestimmte Person richtet oder das Betreten von Wohnungen bedingt, soll nur noch bei Personen liegen, die die genannten Ämter innehaben, analog dem präventiven **Einsatz von Verdeckten Ermittlern (VE)**. Diese Einsatzanordnungen unterliegen der Entscheidung des zuständigen Gerichts und sind gemäß § 28 durch die dort Genannten zu beantragen. Ein Erfüllungsaufwand für den jährlichen Personalaufwand ergibt sich in Höhe von 139 000 Euro sowie für den einmaligen Sachaufwand in Höhe von 12 300 Euro.

Zur Berechnung der Bürokratiekosten im Falle einer festgestellten **Kontamination** (§ 34a) wurde aufgrund vorliegender Erfahrungen die Größenordnung von zehn Fällen angenommen. Hieraus ergeben sich ein einmaliger Personalaufwand in Höhe von 13 135 Euro, ein jährlicher Personalaufwand in Höhe von 2 117 Euro, ein einmaliger Sachaufwand in Höhe von 19 355 Euro und ein jährlicher Sachaufwand 1 935 Euro.

b) Datenverarbeitung

Die präventive **Telekommunikationsüberwachung** kommt im Zuständigkeitsbereich der Bundespolizei insbesondere im Zusammenhang mit Schleusungskriminalität und der Ankündigung von Bombenexplosionen auf Bahnhöfen oder Flughäfen in Betracht. Die Androhungen von Anschlägen gegen Anlagen der Eisenbahnen oder des Luftverkehrs erfolgt etwa durchschnittlich in 70 Fällen pro Jahr. Der Erfüllungsaufwand für die neue zusätzliche Aufgabe der präventiven Telekommunikationsüberwachung umfasst einen jährlichen Personalaufwand in Höhe von 232 000 Euro sowie einen jährlichen Sachaufwand in Höhe von 14 000 Euro.

Die **Videoüberwachung von Gewahrsamsräumen** ist als technische Möglichkeit der vorgeschriebenen Kontrolle des Gewahrsamsraumes zu betrachten und kann als zusätzliche Option zur persönlichen Kontrolle der Gewahrsamsräume herangezogen werden.

Von der Bundespolizei werden 347 Gewahrsamsräume betrieben, von denen bisher 25 mit entsprechender Technik ausgerüstet sind. Für die Ausstattung der übrigen Gewahrsamsräume der Bundespolizei entsteht jährlich ein Sachaufwand in Höhe von 150 000 Euro ab 2020 (für vier Jahre). Für die Unterhaltung der Videoüberwachungsanlagen (Sicherung eigener Einrichtungen sowie Überwachung der Gewahrsamsräume) werden jährlich 150 000 Euro erforderlich.

#### c) Grundsatz der hypothetischen Datenneuerhebung, Kennzeichnung

Durch den Grundsatz der **hypothetischen Datenneuerhebung** werden eingehendere datenschutzrechtliche Prüfschritte erforderlich. Der zeitliche Mehraufwand pro Jahr wird mit 2 Millionen Euro Personalaufwand bemessen. Personalaufwand fällt hierbei auch für die Erstellung von Schulungsunterlagen für die Aus- und Fortbildung an. Für die einmalige Ausbildung aller @rtus-Bund und b-case/eFBS Anwender wird von einem reinen Personalaufwand von 5 Millionen Euro ausgegangen.

Um die **Kennzeichnung der personenbezogenen Daten** umzusetzen, müssen die durch die Bundespolizei geführten IT-Systeme ertüchtigt und gewartet werden. Für das Vorgangsbearbeitungssystem (VBS) der Bundespolizei entsteht ein jährlicher Personalaufwand in Höhe von 50 021 Euro. Für das Fallbearbeitungssystem b-case im Verbundsystem PIAV beträgt der jährliche Personalaufwand 127 000 Euro. Für das INPOL-System beläuft sich der jährliche Personalaufwand ebenfalls auf 127 000 Euro.

### 5. Weitere Kosten

Mit der Einführung des Richtervorbehaltes für verdeckte Maßnahmen zur Gefahrenabwehr ist eine Erreichbarkeit rund um die Uhr des für die Bundespolizei zuständigen Richters zwingend erforderlich. Ein weiterer Mehraufwand entsteht für das Gericht durch die erhöhten Anforderungen an den Kernbereichsschutz bei besonders eingriffsintensiven Maßnahmen. Bei verdeckten Überwachungsmaßnahmen der Telekommunikation, besonderen Mitteln der Datenerhebung zur Gefahrenabwehr sieht das Gesetz vor, die so gewonnenen Erkenntnisse sofort dem Gericht vorzulegen, welches unverzüglich über die Verwertung oder Löschung zu entscheiden hat. Zur Abwicklung des dabei anfallenden Geschäftsverkehrs muss eine Geschäftsstelle eingerichtet werden.

### 6. Weitere Gesetzesfolgen

Der Entwurf hat keine erkennbaren gleichstellungspolitischen Auswirkungen. Auswirkungen auf demografierelevante Belange sind nicht zu erwarten.

## VII. Befristung; Evaluation

Eine Befristung ist nicht vorgesehen.

Dieses Regelungsvorhaben wird spätestens fünf Jahre nach dem Inkrafttreten hinsichtlich des mit dem Vorhaben verbundenen Erfüllungsaufwands evaluiert. Dabei wird die Bundesregierung untersuchen, wie sich der Erfüllungsaufwand für die neuen Aufgaben und Befugnisse sowie die Umsetzung der Datenschutzerfordernisse entwickelt hat und ob die Entwicklung des Erfüllungsaufwands in einem angemessenen Verhältnis zu den festgestellten Regelungswirkungen steht. Die Evaluierung wird die Frage nach unbeabsichtigten Nebenwirkungen sowie nach der Akzeptanz und Praktikabilität der Regelungen einschließen.

§ 28 Absatz 2 Nummer 4 sollte bereits im Rahmen des Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus evaluiert werden. Da beim Einsatz Verdeckter Ermittler zunächst entsprechende Strukturen aufgebaut und etabliert werden müssen, befanden sich drei Jahre nach Inkrafttreten des BVerfSchG noch keine VE im Einsatz, so dass zu den Regelungswirkungen keine Aussagen getroffen werden konnten und die Evaluierung in dieses Gesetzgebungsvorhaben übernommen wurde.

## B. Besonderer Teil

### Zu Artikel 1 (Änderung des Bundespolizeigesetzes)

#### Zu Nummer 1 (Inhaltsübersicht)

Die Änderungen in der Inhaltsübersicht sind durch die nachfolgenden Änderungen der Nummern 2 bis 32 veranlasst.

#### Zu Nummer 2 (§ 1 Absatz 5)

Die ergänzende Nennung der „Vorsorge für die künftige Verfolgung von Straftaten“ dient der Klarstellung, dass Maßnahmen zur Strafverfolgungsvorsorge auch der Gefahrenabwehr dienen und hierunterfallen. Entsprechende Regelungen finden sich ebenfalls in mehreren Polizeigesetzen der Länder.

#### Zu Nummer 3 (§ 12)

##### Zu Buchstabe a (Absatz 1)

##### Zu Buchstabe a Doppelbuchstabe aa (Satz 1)

In Bezug auf die Zuständigkeit der Bundespolizei für polizeiliche Maßnahmen auf dem Gebiet der Strafverfolgung wird die bisher bestehende grundsätzliche Beschränkung auf Vergehen weitestgehend aufgegeben. Nachdem die Bundespolizei nach dem bisherigen BPolG im Grundsatz für Vergehen zuständig war und nur ausnahmsweise für Verbrechen, soll diese Differenzierung künftig prinzipiell unterbleiben und eine Zuständigkeit im eigenen Bereich im Regelfall unabhängig von der angedrohten Mindestfreiheitsstrafe eines Delikts bestehen.

Diese Änderung liegt maßgeblich darin begründet, dass sich die nach dem bisherigen BPolG bestehende Unterscheidung zwischen Vergehen und Verbrechen als nicht zweckmäßig erwiesen hat, sondern verschiedene Zuständigkeiten vielmehr oftmals zu einem künstlichen Aufspalten eines einheitlichen Lebenssachverhalts führten. Dies wurde besonders deutlich in Sachverhalten, in denen zunächst wegen des Verdachts eines Vergehens ermittelt wurde und sich im Laufe der Ermittlungen ein Verdacht eines Verbrechens ergab, sich zum Beispiel der gewerbsmäßige Taschendiebstahl auf dem Bahnhof gemäß § 243 Absatz 1 Satz 2 Nummer 3 Strafgesetzbuch (Vergehen) später als bandenmäßiger gewerbsmäßiger Diebstahl nach § 244a Absatz 1 in Verbindung mit § 243 Absatz 1 Satz 2 Nummer 3 Strafgesetzbuch (Verbrechen) darstellte. Insoweit ergeben sich bislang ermittlungshindernde Schnittstellen in Fällen, in denen nach Durchführung möglicherweise eines Großteils der Ermittlungen aufgrund eines weiteren hinzutretenden Umstandes (Bande) die Abgabe der Ermittlungen an die neu zuständige Behörde erforderlich wird. Derartige Schnittstellen gilt es künftig zu vermeiden.

Auch im Übrigen scheint es aus polizeitaktischen Gründen sachgerecht, ein paralleles Ermitteln mehrerer Behörden innerhalb eines deliktischen Bereichs (z. B. Diebstähle an Bahnhöfen) zugunsten einer verbleibenden Verantwortlichkeit aufzugeben.

##### Zu Buchstabe a Doppelbuchstabe aa Dreifachbuchstabe bbb (Nummer 2)

Nach der in Nummer 2 eingefügten Ergänzung wird die Bundespolizei für polizeiliche Maßnahmen im Rahmen der Strafverfolgung von unerlaubten Aufenthalten zuständig, sofern sie Drittstaatsangehörige in ihrem Zuständigkeitsbereich feststellt, in Bezug auf die ein Verdacht einer solchen Straftat besteht (z. B. auf dem Gebiet der Bahnanlagen oder im Bereich Luftsicherheit). Außerhalb dieser bundespolizeilichen Zuständigkeit sind die Landesbehörden weiterhin für die Bekämpfung des unerlaubten Aufenthaltes zuständig. Damit einhergehend ist die Bundespolizei auch für die Verfolgung des qualifizierten unerlaubten Aufenthaltes mit angedrohter Höchstfreiheitsstrafe von drei Jahren nach § 95 Absatz 2 Nummer 1b und Nummer 2 AufenthG zuständig, sofern die Feststellung des Tatverdachts im Rahmen der bundespolizeilichen Aufgabenwahrnehmung erfolgt. Die Strafverfolgungszuständigkeit für den unerlaubten Aufenthalt, sofern der Ausländer bei der Wahrnehmung bundespolizeilicher Aufgaben festgestellt wird, ist ein wesentlicher Baustein eines ganzheitlichen Bekämpfungsansatzes, der untrennbar mit der Ergänzung des § 71 AufenthG um den neuen Absatz 3a verknüpft ist (siehe dortige Begründung), welcher der Bundespolizei die Zuständigkeit für aufenthaltsbeendende Maßnahmen in diesen Fällen (Feststellen vollziehbar ausreisepflichtiger Drittstaatsangehöriger im eigenen Zuständigkeitsbereich) zuweist.

**Zu Buchstabe a Doppelbuchstabe aa Dreifachbuchstabe ccc (Nummer 5)**

Die bislang durch die „Und“-Verknüpfung bestehende Einschränkung ist nicht sachgerecht und soll deshalb zugunsten einer „Oder“-Verknüpfung aufgegeben werden. Die Zuständigkeit der Bundespolizei soll danach begründet sein, wenn entweder eine Straftat auf dem Gebiet der Bahnanlagen des Bundes begangen wurde oder sich eine Straftat gegen die Sicherheit eines Benutzers, der Anlagen oder des Betriebes der Bahn richtet. Eine Einschränkung der Zuständigkeit aus Nummer 5 ergibt sich aus dem neuen Satz 2.

**Zu Buchstabe a Doppelbuchstabe aa Dreifachbuchstabe ddd (Nummer 7)**

Nach Nummer 5 obliegt der Bundespolizei bereits die Zuständigkeit für polizeiliche Maßnahmen im Rahmen der Strafverfolgung, sofern sich Angriffe gegen die Sicherheit der Anlagen oder des Betriebes der Bahn richten. Gleichmaßen soll dies nach Nummer 7 in Bezug auf Angriffe der Fall sein, die sich gegen die Sicherheit und den Betrieb des Luftverkehrs richten. Umfasst sind insbesondere solche Straftaten, die im Zusammenhang mit Drohnenangriffen verwirklicht werden können (z. B. §§ 315, 316b StGB). Der Bundespolizei sind in diesem Zusammenhang zahlreiche Fälle bekannt, in denen beispielsweise durch fernmanipulierte Luftfahrzeuge (Drohnen) im Bereich von Flughäfen, durch den Einsatz von Lichtzeigern (sog. Laserpointer) gegen im Einsatz befindliche Polizeihubschrauber oder andere, gleichsam gefährliche Eingriffe die Sicherheit des Luftverkehrs beeinträchtigt wurde. Damit korrespondierend normiert § 28b die präventivpolizeiliche Befugnis zur Abwehr von Drohnenangriffen.

Eine Einschränkung ergibt sich daraus, dass der Tatverdacht im Zuständigkeitsbereich der Bundespolizei festgestellt worden sein muss. Ausgenommen sind danach solche Fälle, die in den Zuständigkeitsbereich einer anderen Behörde fallen, etwa ausdrücklich dem Bundeskriminalamt zugewiesen sind.

Durch die bisher fehlende Zuständigkeit zwischen den Behörden der Bundespolizei und der Polizeien der Länder kam es zu Doppelarbeit: Die Bundespolizei nimmt den Sachverhalt als Luftsicherheitsbehörde auf und übergibt den Sachverhalt nach bereits erfolgtem ersten Zugriff an eine andere Behörde, die zumeist vor Ort ebenfalls derartige Maßnahmen vornimmt. Das Verfahren vor Ort wird aufgrund notwendiger Übergaben somit verlängert. Die Landespolizei ist insbesondere an kleineren Flughäfen zudem nicht zeitnah am Ereignisort. Außerdem werden bei der Bearbeitung dieser Straftaten regelmäßig wichtige Informationen für die künftige Wahrnehmung der präventivpolizeilichen Luftsicherheitsaufgaben der Bundespolizei gewonnen.

**Zu Buchstabe a Doppelbuchstabe bb (Satz 2)**

Der neue Satz 2 beschränkt die Zuständigkeit der Bundespolizei für polizeiliche Aufgaben auf dem Gebiet der Strafverfolgung nach Satz 1 Nummer 5 auf Verbrechenstatbestände, die typischerweise auf Bahnanlagen der Eisenbahnen verwirklicht werden.

**Zu Buchstabe b und c (Absätze 3 und 5)**

Bei den Änderungen handelt es sich um redaktionelle Folgeänderungen.

**Zu Nummer 4 (§ 12a)**

Der neue § 12a ermöglicht der Bundespolizei den Schutz von Zeugen innerhalb von durch die Bundespolizei geführten Strafverfahren. § 12a entspricht § 7 Absatz 1 und Absatz 3 BKAG.

Eine gesetzliche Regelung im BPolG für den Schutz von Zeugen ist aus kriminalstrategischen und praktischen Erwägungen für die Ermittlungstätigkeiten der Bundespolizei erforderlich. Insbesondere im Bereich der Schleusungskriminalität sind regelmäßig Einschüchterungen von Zeugen zu beobachten. Dabei ist der Zeugenbeweis unverändert von wesentlicher Bedeutung zur Überführung der Täter. Der Erhalt der Aussagefähigkeit und -bereitschaft ist in diesen Fällen nur durch einen effektiven Zeugenschutz zu gewährleisten.

Die bislang bestehende Abhängigkeit zu anderen Behörden wird durch die Neuregelung beendet und Zeugenschutzmaßnahmen können ohne zeitlichen Verzug unmittelbar in eigener Zuständigkeit durchgeführt werden. Bisher ist die bei der Bundespolizei eingerichtete Koordinationsstelle für Maßnahmen zum Schutz gefährdeter aussagebereiter Personen zunächst gehalten, einen geeigneten Kooperationspartner zu finden, der über die erforderlichen Kapazitäten zur Übernahme eines behördenfremden Zeugenschutzfalls verfügt und außerdem die im konkreten Fall notwendigen Rahmenbedingungen gewährleisten kann. Bis zum Vollzug der Maßnahme vergehen nach dieser bisherigen Praxis teilweise 6 bis 8 Wochen.

Nicht nur in zeitlicher Hinsicht, sondern auch im Übrigen kann die Neuregelung einen effektiveren Zeugenschutz bewirken. Denn nach derzeitiger Rechtslage wird infolge der bestehenden Aufgabenteilung zum einen zwangsläufig ein breiterer Personenkreis mit sensiblen Informationen in Bezug auf das Ermittlungsverfahren und die gefährdete Zeugin oder den gefährdeten Zeugen versorgt. Der beabsichtigte Schutz der Zeugin oder des Zeugen kann hierdurch beeinträchtigt werden. Die durch die Neuregelung bezweckte Vermeidung von Schnittstellen minimiert dieses Risiko. Zum anderen verfügt im Vergleich zu den in Amtshilfe tätig werdenden Behörden die ermittelungsverfahrensführende Behörde selbst naturgemäß über die größere Sachkenntnis. Insbesondere im Bereich der Schleusungskriminalität kann der Zeugenschutz aufgrund der speziellen milieu- und deliktsspezifischen Kenntnisse der Bundespolizei bestmöglich durch diese erfolgen.

Durch die Regelung in Absatz 2 bleibt die Möglichkeit erhalten, dass Zeugenschutzmaßnahmen in Einzelfällen unverändert durch die Länder wahrgenommen werden.

#### **Zu Nummer 5 (§ 14a)**

§ 14 legt fest, dass die Bundespolizei im Rahmen der neuen Aufgabe gemäß § 12a auch die im Einzelfall erforderlichen Maßnahmen treffen kann. Die Regelung orientiert sich an § 66 BKAG. Nach der enumerativen Auflistung von Rechtsgütern ist fraglich, ob auch vor einer Nachstellung nach § 238 StGB geschützt werden dürfte. Dort ist das Rechtsgut umstritten, wird bisweilen aber etwa im „individuellen Rechtsfrieden“ oder in der „Freiheit der Lebensgestaltung“ gesehen.

Dies wirft die Frage auf, ob der Staat hier seiner grundrechtlichen Schutzpflicht für die Betroffenen hinreichend effektiv nachkommt. Im Rahmen des weitgehend gleichartigen § 66 BKAG sind jedenfalls noch weitergehende Maßnahmen der Gefahrerforschung nach § 66 Absatz 1 Satz 3 i. V. m. § 63 BKAG eröffnet. Womöglich bietet die hiesige Norm aber auch so schon ausreichenden Spielraum für hinreichend effektives Vorgehen (insoweit Fachfrage).

#### **Zu Nummer 6 (§ 21 Absatz 2)**

Durch die Neufassung von Absatz 2 entfällt in Nummer 1 die bisherige Einschränkung einer Datenerhebung nur in Bezug auf Straftaten nach § 12 Absatz 1. Bei den Änderungen in Nummer 2 handelt es sich um redaktionelle Anpassungen, die vorgenommen werden, um einen Gleichlauf mit § 39 Absatz 2 BKAG zu erreichen.

#### **Zu Nummer 7 (§ 22a Absatz 3 Satz 6)**

Es handelt sich um redaktionelle Folgeänderungen.

#### **Zu Nummer 8 (§ 24 Absatz 1 Nummer 2)**

Entsprechend der Änderung in § 1 Absatz 5 wird auch hier die Strafverfolgungsvorsorge klarstellend ergänzt. Im Übrigen wird dahingehend präzisiert, dass die Annahme einer Gefahr auf Tatsachen gestützt sein muss.

#### **Zu Nummer 9 (§ 25a)**

Die Bundespolizei erhält nach Absatz 1 Nummer 1 die Befugnis zum Erlass von Meldeauflagen, wenn Tatsachen die Annahme rechtfertigen, dass eine Straftat im Sinne des § 12 Absatz 1 begangen werden wird, die für sich genommen oder aufgrund des wiederholenden Charakters erhebliche Bedeutung hat, und diese durch eine Meldeauflage vorbeugend bekämpft werden kann.

Nach Absatz 1 Nummer 2 soll eine Meldeauflage ferner erforderlichenfalls zur Durchsetzung einer Ausreiseuntersagung gemäß § 10 Absatz 1 PassG möglich sein.

Eine solche Befugnis trägt insbesondere signifikant zur Befriedung des schienengebundenen grenzüberschreitenden Fußballfanreiseverkehrs bei, indem bevorstehende Ausreisen gewaltbereiter Fußballfans zu Auslandsspielen auf diese Weise weniger wahrscheinlich gemacht werden können. Außerdem fallen hierunter Fälle, in denen etwa mutmaßlich extremistische und/oder gewaltbereite Personen nach den ermittelten Umständen zu ausländischen Veranstaltungen auszureisen beabsichtigen.

#### **Zu Nummer 10 (§§ 27d und 27e)**

##### **Zu § 27d**

Der neue § 27d regelt die Überwachung der Telekommunikation durch die Bundespolizei.

**Zu Absatz 1**

Die Einführung einer Befugnis zur präventiven Telekommunikationsüberwachung ist kriminaltaktisch insbesondere bei der Bekämpfung der Schleusungskriminalität sowie bahnpolizeilich relevanten banden- und gewerbsmäßig begangenen Straftaten geboten. Regelmäßig werden etwa Personen durch Schleuserorganisationen unter bewusster Inkaufnahme von Gefahren für Leib und Leben nach Deutschland geschleust, z. B. in geschlossenen Behältnissen. Die Bundespolizei enthält in etwa 20 Fällen pro Jahr Hinweise auf derartige Behältnisschleusungen. Ferner kommt es jährlich zu durchschnittlich etwa 70 Ankündigungen von Anschlägen gegen Anlagen der Eisenbahnen oder von Flughäfen. Hier kommt einem schnellen Erkennen sowie einer zügigen Intervention entscheidende Bedeutung bei der Abwehr dieser Gefahren zu.

Die präventive Telekommunikationsüberwachung soll hier eine Erkenntnislücke der Bundespolizei schließen und sich gegen Personen richten, gegen die noch kein Tatverdacht begründet ist und daher noch keine strafprozessuale Maßnahme nach § 100a StPO angeordnet werden kann. Überdies ermöglicht eine Telekommunikationsüberwachung neben der Erlangung inhaltlicher Erkenntnisse zu dem geplanten Vorhaben, dass neben der bereits anvisierten Zielperson weitere Beteiligte bekannt werden. Normzweck ist vor allem die Abwehr von Gefahren für Leib und Leben, insbesondere von unter unmenschlichen Bedingungen geschleusten Migranten. Die Norm orientiert sich in ihrer Ausgestaltung an § 51 BKAG.

Die Maßnahme ist nach Nummer 1 gegen Verantwortliche nur möglich, wenn dies zur Abwehr einer dringenden Gefahr für eines der benannten bedeutenden Rechtsgüter geboten ist. Unter Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt, fallen dabei primär Infrastrukturen im Bahn- und Flugbereich.

Auch ist die Maßnahme nach Nummer 2 im Vorfeld einer dringenden Gefahr im Sinne von Nummer 1 möglich.

Nummer 3 erfasst den sog. Nachrichtenmittler. Notwendig für die Anordnung sind tatsächliche Anhaltspunkte für eine gewisse Tat- oder Gefahrennähe des Mittlers.

Nummer 4 erfasst Dritte. Notwendig für die Anordnung sind tatsächliche Anhaltspunkte für eine gewisse Tat- oder Gefahrennähe des Dritten.

**Zu Absatz 2**

Absatz 2 erweitert die herkömmliche Telekommunikationsüberwachung um die Möglichkeit der Quellen-TKÜ, welche das Abhören verschlüsselter IP-Telefonie ermöglicht, sofern bestimmte Tatsachen die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraums eine konkretisierte Straftat im Zusammenhang mit einer der beiden benannten Sachverhalte aus dem Zuständigkeitsbereich der Bundespolizei mit höchstem Schädigungspotential für Leib und Leben und bedeutende Infrastrukturen droht. Namentlich sind hier lebensgefährdende (Behältnis-)Schleusungen in den Blick genommen sowie gefährliche Eingriffe in den See-, Luft- oder Bahnverkehr.

Vermehrt findet Kommunikation über Internettelefonie statt. Dabei muss der Nutzer von Programmen gängiger Anbieter, wie beispielsweise Skype oder Whatsapp, eine Verschlüsselung des von ihm Gesprochenen oder Geschriebenen bzw. eine Entschlüsselung empfangener Nachrichten nicht erst aktiv durch entsprechende technische Maßnahmen herbeiführen. Verschlüsselungen von Daten sind vielmehr bereits standardisiert in die Software implementiert. Infolge der Verschlüsselung sind in diesen Fällen mittels herkömmlicher Telekommunikationsüberwachung nur kryptierte, also verschlüsselte und nicht lesbare, Daten der Kommunikation festzustellen.

Aus diesem Grunde erfreuen sich Kommunikationsformen via Internet größter Beliebtheit, zuvörderst im Rahmen der Vorbereitung grenzüberschreitender organisierter Kriminalität, um auf diese Weise „abhörsicher“ Straftaten zu planen. Mittlerweile ist diese Möglichkeit jedoch bereits über den Kreis organisierter Banden hinaus allgemeinbekannt und wird deliktsbereichsübergreifend zur Umgehung einer üblichen Telekommunikationsüberwachung bevorzugt genutzt. Im Ergebnis kann es indes keinen Unterschied machen, ob die Zielperson herkömmlich telefoniert und Nachrichten via Short Message Service (SMS) versendet oder sich hierzu Anbietern wie Skype oder Whatsapp bedient. Diese Unterscheidung ist vielmehr ungerechtfertigt.

Eine erfolgreiche Überwachung muss daher im Fall von Datenübertragungen, die auf dem Weg zum Empfänger verschlüsselt sind, auf die Daten zugreifen können, bevor sie am Versendergerät verschlüsselt werden oder nachdem sie am Empfängergerät entschlüsselt wurden. Es werden im Vergleich zur herkömmlichen Telekommunikationsüberwachung daher nicht mehr Daten erfasst, es werden vielmehr dieselben Daten nur an anderer Stelle

aufgenommen, namentlich nicht während des Übertragungsvorgangs, sondern am Gerät des Versenders oder Empfängers.

Dass nur Inhalte von laufender Kommunikation überwacht werden dürfen und dies zudem durch die eingesetzte Überwachungssoftware technisch sichergestellt sein muss, stellt Satz 1 Nummer 1 klar. Nach Satz 1 Nummer 2 bedarf es ferner der Notwendigkeit des Eingriffs, was nicht der Fall ist, wenn unverschlüsselte Daten übertragen werden. Denn nicht verschlüsselte Daten können mittels herkömmlicher Telekommunikationsüberwachung observiert werden, was einen Zugriff auf das Versender- oder Empfängergerät obsolet macht. Die Quellen-TKÜ ist damit subsidiär zur herkömmlichen Telekommunikationsüberwachung.

Nach Satz 2 dürfen auch gespeicherte Inhalte der (ge-)laufenden Telekommunikation überwacht werden. In Abgrenzung zur sog. Online-Durchsuchung dürfen indes nur solche Inhalte erhoben werden, die auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form erhoben werden könnten, nicht also bereits vor der Anordnung abgelegte Kommunikationsinhalte oder gar andere Inhalte als solche die Kommunikation betreffend.

Ein Beispiel für eine konkrete Anwendung der neuen Befugnis durch die Bundespolizei ergibt sich im Bereich von gewerbs- und bandenmäßig durchgeführten Schleusungen: Erhält die Bundespolizei Kenntnis von unmittelbar bevorstehenden oder gerade stattfindenden Schleusungshandlungen, die unter lebensgefährlichen Bedingungen für die geschleusten Personen vollzogen werden (z. B. auf ungesicherten Landeflächen, im lebensgefährlichen Fahrwerksbereich von Güterwaggons oder Lkw, in Behältnissen ohne ausreichende Luftzirkulation), bedarf es einer gefahrenabwehrenden Sofortintervention. Verläuft dabei die durch den Schleuser und dessen Kontaktpersonen geführte Kommunikation (über die geplante Schleusungsrouten, Ausweichstrecken im Falle von Verkehrsbehinderungen oder geplante Logistikstopps) via verschlüsselter Kurznachrichten oder Internettelefonie, können die dieserart ausgetauschten Informationen nur über eine durchgeführte Quellen-TKÜ der Bundespolizei zur Kenntnis gelangen.

Auch im Fall eines bevorstehenden gefährlichen Eingriffs in Anlagen der Eisenbahnen des Bundes oder des Luftverkehrs ist eine Überwachung von Gesprächsinhalten und Kurznachrichten durch die Bundespolizei unabdingbar, um die Ernsthaftigkeit der Drohung zu verifizieren, die Modalitäten des geplanten Angriffs und die mögliche Beteiligung evtl. weiterer Gefahrenmitverursacher polizeilich aufklären zu können.

Die Bundespolizei bedarf zur Gefahrenabwehr daher der Befugnis zur Vornahme der Quellen-TKÜ, um nicht hinter dem technischen Fortschritt zurückbleiben zu müssen, dem sich die Verantwortlichen einer Gefahr bedienen. Die im Rahmen der Vorbereitung einer Tat oder sonstigen Gefahr ausgetauschten Informationen sind unverzichtbar für eine effektive Gefahrenabwehr.

Die grundsätzliche Verfassungsmäßigkeit der Quellen-TKÜ nimmt auch das BVerfG in seinem Urteil vom 20. April 2016 (BVerfGE 141, 220 – Rn. 234) im Hinblick auf die präventive Regelung der Quellen-TKÜ im BKA-Gesetz an. Vergleichbare Regelungen finden sich ferner bereits in einigen Landespolizeigesetzen.

### **Zu Absatz 3**

Es ist ferner technisch zu gewährleisten, dass der Eingriff nach Absatz 2 nur unabdingbare Veränderungen im informationstechnischen System bewirkt und vorgenommene Veränderungen, soweit technisch möglich, wieder rückgängig gemacht werden müssen.

### **Zu Absatz 4**

Maßnahmen nach Absatz 1 und 2 stehen unter Richtervorbehalt. Es besteht ferner ein Antragsersfordernis der Präsidentin oder des Präsidenten des Bundespolizeipräsidiums oder der zuständigen Bundespolizeidirektion, oder deren jeweiligen Vertretung. Nach Satz 2 sind diese Personen bei Gefahr im Verzug auch zur Anordnung der Maßnahme befugt, in Bezug auf die nach Satz 3 unverzüglich eine richterliche Bestätigung einzuholen ist. Dieser alternativen Möglichkeit der Entscheidung über die Anordnung bedarf es für den Gefahr-im-Verzugs-Fall, da die Sichtung der bei einem Verantwortlichen gespeicherten Informationen in Bezug auf eine unmittelbar drohende Gefahr naturgemäß regelmäßig keinen Aufschub duldet.

### **Zu Absatz 5**

Absatz 5 regelt Antragsersfordernisse.

**Zu Absatz 6**

Absatz 6 bestimmt die Anordnungsinhalte sowie die möglichen Höchstfristen der Maßnahmen.

**Zu Absatz 7**

In Absatz 7 findet sich die mit der Eingriffsbefugnis korrelierende Verpflichtung der Diensteanbieter zur Mitwirkung.

**Zu den Absätzen 8 und 9**

Absätze 8 und 9 normieren Verfahrensregelungen für die Klärung der Frage der Verwertbarkeit von Daten, die möglicherweise den Kernbereich privater Lebensgestaltung betreffen. Es gilt das sog. Richterband, Absatz 8. Nach Absatz 9 darf ausnahmsweise bei Gefahr im Verzug die Präsidentin oder der Präsident des Bundespolizeipräsidiums oder einer Bundespolizeidirektion oder deren jeweilige Vertretung über die Verwertung entscheiden, die unverzüglich richterlicher Bestätigung bedarf.

**Zu § 27e**

Der neue § 27e gibt der Bundespolizei die Befugnis zur Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten. Er entspricht inhaltlich dem § 53 BKAG.

Im Rahmen der Aufgabenwahrnehmung der Bundespolizei besteht das Erfordernis zur Identifizierung und Lokalisierung von Mobilfunkendgeräten. Die Vorschrift ergänzt § 39 und ermöglicht den Versand von sogenannten „stillen SMS“ bzw. der Einsatz von anderen technischen Möglichkeiten (bspw. IMSI-Catcher) zur Ortung der überwachten Mobilfunknummer. Ohne die Befugnis wäre eine Standortbestimmung ohne Einsatz technischer Mittel nur bei aktiver Telekommunikation des Mobilfunknutzers möglich.

Hintergrund ist der Beschluss des BGH vom 8. Februar 2018 – 3 StR 400/17 mit dem Leitsatz: „Rechtsgrundlage für das Versenden sogenannter „stiller SMS“ durch die Ermittlungsbehörden ist § 100i Absatz 1 Nummer 2 StPO“. Insofern kann der Versand „stiller SMS“ nicht mehr wie bisher auf Grundlage des § 100a StPO bzw. in Analogie auf Grundlage des § 39 BPolG erfolgen. Für einen präventiven Einsatz dieses Mittels ist daher eine gesonderte Rechtsgrundlage zu schaffen.

**Zu Absatz 1**

Die Vorschrift stellt die Maßnahme unter die Voraussetzungen, die auch für die Telekommunikationsüberwachung nach § 39 Absatz 1 gelten. Hierzu sei deshalb auf die Ausführungen in der dortigen Begründung verwiesen.

Anwendungsfälle bei der Bundespolizei ergeben sich insbesondere im Rahmen der Verhinderung der Durchführung von Schleusungen. Erfolgt beispielsweise eine transeuropäische Behältnisschleusung durch Deutschland, ist eine Standortbestimmung mittels „stiller SMS“ die erfolgversprechendste Maßnahme, um effektive Interventionsmaßnahmen einleiten zu können. Ein weiterer Anwendungsfall ist die Ortung/Lokalisierung eines Verursachers von Androhungen von Anschlägen gegen Anlagen der Eisenbahnen oder des Luftverkehrs.

In diesen Fällen besteht das Erfordernis, unterhalb der eingriffsintensiveren Gesprächsüberwachung Mobiltelefone und deren Nutzer zu lokalisieren. Während polizeilich relevante Personen ihre Identitäten häufig wechseln, werden erfahrungsgemäß Mobiltelefone und/oder Mobiltelefonkarten über einen längeren Zeitraum mitgeführt (vor diesem Hintergrund wurden auch die gesetzlichen Befugnisse des Auslesens von Mobiltelefonen zur Identifizierung von Drittstaatsangehörigen eingeführt, § 15a AsylG, § 48 Absatz 3a AufenthG).

Folgende weitere Anwendungsbeispiele kommen in Betracht:

Aufklärung des Standortes bei einem Suizidverdacht mit Bahnbezug: Hier sind unmittelbar nach der Ankündigung unverzüglich Sofortmaßnahmen zur Lokalisierung der suizidgefährdeten Person unter Berücksichtigung der besonderen örtlichen Begebenheiten der betreffenden Bahnanlagen und des Bahnverkehrs unter Einbindung der Landespolizei einzuleiten. Die Übergabe der erforderlichen Sofortmaßnahme der Standortermittlung an die Landespolizei würde aufgrund der zusätzlichen Schnittstelle zu einer zeitlichen Verzögerung führen, die in diesen Fällen des unmittelbar bevorstehenden Schadenseintritts für Leib und Leben vermeidbar gewesen wäre.

Aufklärung des Standortes einer zur Einreiseverweigerung ausgeschriebenen Person: Die Bundespolizei hat derzeit in eigener Zuständigkeit über 41.000 Personen zur Einreiseverweigerung ausgeschrieben. Von den über

20.000 zur schengenweiten Einreiseverweigerung im SIS ausgeschriebenen Personen weisen ca. 14.000 einen Terrorismusbezug auf. Diese Ausschreibungen basieren gemäß Artikel 24 Absatz 2 VO 1087/2006 (SIS II) auf einer einzelfallbezogenen Gefahrenprognose (tatbestandliches Regelbeispiel für eine solche Gefahr: Planung oder Begehung schwerer Straftaten). Bei derart schwerwiegenden Sachverhalten muss es der Bundespolizei in begründeten Einzelfällen auch möglich sein, vorhandene Mobiltelefondaten dahingehend zu überprüfen, ob sich der Gerätenutzer – d. h. die gefährliche Person – bereits nach unerlaubter bzw. unbemerkter Einreise im Inland befindet. Eine erfolgreiche Lokalisierung ermöglicht sodann polizeiliche Anschlussmaßnahmen, die im Einvernehmen mit Landes- und Bundesbehörden angepasst bzw. eingeleitet werden (z. B. Identifizierung des Handynutzers, zusätzliche Fahndungsausschreibung mit anderer Zweckrichtung, z. B. Ausschreibung zur Festnahme).

Lokalisierung von Personen zum Zwecke der Prüfung von Ausreiseuntersagungen im Binnengrenzraum: Derzeit hat die Bundespolizei 123 Personen zur Ausreiseuntersagung mit Terrorismusbezug ausgeschrieben. In den Fällen, in denen sicherheitsbehördliche Informationen zu bevorstehenden Ausreisen zum Zwecke des späteren Anschlusses an eine terroristische Organisation in Krisengebieten vorliegen, obliegt es der Bundespolizei, auf der Basis einer Gefahrenprognose die Ausreise zu untersagen (§ 10 i. V. m. 7 Absatz 1 PassG, § 46 Absatz 2 AufenthG), sofern im Vorfeld durch die Passbehörde nicht bereits der Pass entzogen wurde. Häufig erhält die Bundespolizei in zeitkritischen Sachverhalten lediglich die Information über die mögliche Abfahrtszeit (z. B. mit dem Pkw von Wolfsburg Richtung Konstanz, um über die Schweiz auszureisen). Bei bekannter Mobiltelefonnummer könnte durch eine Bestimmung des Mobiltelefonstandortes mittels „stiller SMS“ die Zielperson lokalisiert werden. Bei nicht vorhandener Grenzkontrolle an den Binnengrenzen wird dadurch die Erfolgswahrscheinlichkeit des Antreffens deutlich erhöht.

#### **Zu Absatz 2**

Absatz 2 beschränkt die Maßnahme auf die Erhebung nur solcher personenbezogener Daten, die zur Zweckerreichung unvermeidbar erhoben werden müssen. Ein Abgleich ist ausschließlich mit der gesuchten Geräte-/Kartennummer möglich.

#### **Zu Absatz 3**

Über den Verweis auf § 39 Absatz 4 steht die Maßnahme unter Richtervorbehalt. Es besteht ferner ein Antragsfordernis der Präsidentin oder des Präsidenten des Bundespolizeipräsidiiums oder einer Bundespolizeidirektion, oder deren jeweiligen Vertretung. Die Antragsberechtigten sind nach Satz 2 bei Gefahr im Verzug auch zur Anordnung der Maßnahme befugt, in Bezug auf die nach Satz 3 unverzüglich eine richterliche Bestätigung einzuholen ist. Dieser alternativen Möglichkeit der Entscheidung über die Anordnung bedarf es für den Gefahr-im-Verzugs-Fall, da die Sichtung der bei einem Verantwortlichen gespeicherten Informationen in Bezug auf eine unmittelbar drohende Gefahr naturgemäß regelmäßig keinen Aufschub duldet.

Über den weiteren Verweis auf § 39 Absatz 5 hat die Anordnung schriftlich zu ergehen. Bei Wegfall der Voraussetzungen ist die Maßnahme unverzüglich zu beenden.

#### **Zu Absatz 4**

Absatz 4 enthält die mit der Eingriffsbefugnis korrelierende Verpflichtung der Diensteanbieter zur Auskunfterteilung.

#### **Zu Nummer 11 (§ 28)**

##### **Zu Buchstabe a (Absatz 1 Satz 1)**

In Nummer 2 und 3 werden die Anforderungen des BVerfG (vgl. BVerfGE 141, 220 – Rn. 165 i. V. m. Rn. 111 ff. zu § 20g BKAG a.F.) an eine hinreichend gehaltvolle Ausgestaltung der Prognoseanforderungen bei Maßnahmen zur Straftatenverhütung umgesetzt. Die Formulierung orientiert sich an § 45 Absatz 1 Satz 1 Nummer 2 BKAG.

##### **Zu Buchstabe b (Absätze 3 bis 5)**

Die Änderungen in Absatz 3 erstrecken sich, wie vom Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 gefordert (BVerfGE 141, 220 – Rn. 174), auf einen Richtervorbehalt und ggf. erforderliche Antragsbefugnisse.

Eine bestimmte Ausgestaltung gesetzlicher Regelungen wird verfassungsrechtlich zwar nicht eingefordert (BVerfGE 141, 220 – Rn. 117). Das Bundesverfassungsgericht führt aus, dass „eingriffsintensive Überwachungs-

und Ermittlungsmaßnahmen, bei denen damit zu rechnen ist, dass sie auch höchstprivate Informationen erfassen, und gegenüber den Betroffenen heimlich durchgeführt werden, grundsätzlich einer vorherigen Kontrolle durch eine unabhängige Stelle, etwa in Form einer richterlichen Anordnung, bedürfen“.

Eine Differenzierung ist demnach bei Maßnahmen nach Absatz 3 Nummern 1 und 2 und Nummern 3 und 4 dergestalt erfolgt, dass in letzteren Fällen wegen der besonderen Eingriffsqualität ein Richtervorbehalt besteht und zudem ein Antrag der Präsidentin oder des Präsidenten des Bundespolizeipräsidiums oder der zuständigen Bundespolizeidirektion, der Vertretung oder der Abteilungsleitung erforderlich ist. Bei den etwas weniger eingriffsintensiven Maßnahmen nach Absatz 3 Nummer 1 und 2 besteht demgegenüber ein Richtervorbehalt ohne besondere Antragsanforderungen. Bei den verbleibenden am wenigsten eingriffsintensiven Maßnahmen nach Absatz 2 Nummer 2 bis 4 genügt die Anordnung durch die vorgenannten Antragsberechtigten.

Die neue Regelung des Absatz 4 entspricht § 45 Absatz 4 BKAG und setzt die vom Bundesverfassungsgericht an den Antrag gestellten Anforderungen um.

Die Änderung in Absatz 5 setzt die Anforderungen des Bundesverfassungsgerichts (BVerfGE 141, 220 – Rn. 118) an die grundrechtssichernde Funktion der unabhängigen Richterkontrolle um.

Im Gleichklang mit § 45 Absatz 5 Satz 2 BKAG wird die Höchstdauer der Erstanordnung des Einsatzes von Vertrauenspersonen und verdeckten Ermittlern auf drei Monate festgelegt. Hierdurch soll dem Umstand Rechnung getragen werden, dass die Regelanordnung nach § 110b Absatz 1 und 2 StPO ebenfalls drei Monate beträgt.

Bei den übrigen Änderungen handelt es sich um Folgeänderungen.

Absatz 7 normiert, wie vom Bundesverfassungsgericht gefordert (BVerfGE 141, 220 – Rn. 177), eine ausdrückliche gesetzliche Kernbereichsregelung für die besonderen Mittel der Datenerhebung.

Nach Satz 1 ist daher vor der Durchführung der Maßnahme, also auf der Erhebungsebene, eine Prognose dahingehend zu treffen, dass mit der Maßnahme voraussichtlich keine Äußerungen erfasst werden, die allein den Kernbereich der persönlichen Lebensgestaltung betreffen. Diese Prognose muss sich auf tatsächliche Anhaltspunkte stützen, welche sich beispielsweise aus der Art der zu überwachenden Räumlichkeiten oder dem Verhältnis der zu überwachenden Personen zueinander ergeben können; eine vollständige Gewissheit ist nicht erforderlich. Schützenswert ist insbesondere die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens. Ist aufgrund dieser Prognose eine Anordnung zulässig, kann bei entsprechenden Erkenntnissen nach einer strengen Verhältnismäßigkeitsprüfung auch eine nur automatische Aufzeichnung zulässig sein.

Diese den Kernbereichsschutz sichernden Verfahrensvorschriften zielen in Umsetzung der verfassungsrechtlichen Vorgaben des Bundesverfassungsgerichts darauf ab, nach Möglichkeit bereits auf der Erhebungsebene einen Eingriff in den Kernbereich der privaten Lebensgestaltung weitestgehend auszuschließen.

Satz 2 stellt zum Schutz des Kernbereiches privater Lebensgestaltung beim Einsatz von verdeckten Ermittlern und Vertrauenspersonen sicher, dass die Maßnahme bei einer möglichen Kernbereichsrelevanz zu unterbrechen ist, sobald dies ohne Gefährdung der beauftragten Person möglich ist.

Satz 3 enthält das Gebot der unverzüglichen Unterbrechung der Maßnahmen nach Absatz 2 Nummer 1 bis 3 und regelt, was zu unternehmen ist, wenn sich während der Überwachung unerwartet tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte aus dem Kernbereich der persönlichen Lebensgestaltung erfasst werden. In solchen Fällen regelt Satz 4 die Zulässigkeit des sogenannten Richterbandes. Die Regelung dient dem Schutz des Kernbereichs, indem sie bestimmt, dass auch in solchen Fällen, in denen keine eindeutigen Anhaltspunkte für eine Kernbereichsrelevanz sprechen, eine unmittelbare Überwachung durch die ermittelnden Stellen ausgeschlossen ist. In Zweifelsfällen darf der Kommunikationsinhalt daher automatisch aufgezeichnet werden.

Nach Satz 5 sind Aufzeichnungen von Zweifelsfällen unverzüglich dem anordnenden Gericht vorzulegen, welches nach Satz 6 anschließend unverzüglich die Feststellung zu treffen hat, ob eine Kernbereichsrelevanz vorliegt oder nicht und damit eine Entscheidung über die Löschung oder Verwertbarkeit der Daten trifft.

In solchen Zweifelsfällen werden die Grundrechte der Betroffenen dadurch geschützt, dass ein Richter als unabhängige Stelle die Auswertung einer automatischen Aufzeichnung übernimmt.

Satz 7 regelt, dass die unterbrochenen Maßnahmen nur fortgeführt werden dürfen, wenn dadurch keine Erkenntnisse aus dem Kernbereich privater Lebensgestaltung mehr erhoben werden. Da trotz aller gebotenen Vorsorge

nicht ausgeschlossen werden kann, dass zuweilen Daten erfasst werden, die den Kernbereich betreffen, werden die Regelungen verfahrensrechtlich abgesichert und durch das in Satz 8 enthaltene Verwertungsverbot und die in Satz 9 normierte Lösungsverpflichtung flankiert.

Die nachfolgenden Sätze dienen der Umsetzung des Urteils des Bundesverfassungsgerichts vom 20. April 2016 zur Aufbewahrungsfrist der Lösungsprotokolle zwecks effektiver Ausübung der Betroffenenrechte und einer wirksamen Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Absatz 8 macht von der durch das Bundesverfassungsgericht (BVerfGE 141, 220 – Rn. 129) eröffneten Möglichkeit des Gesetzgebers Gebrauch, die notwendigen Regelungen zu treffen, um den Ermittlungsbehörden für Ausnahmefälle bei Gefahr im Verzug auch kurzfristig erste Handlungsmöglichkeiten einzuräumen. Die gerichtliche Entscheidung ist nach Satz 4 unverzüglich nachzuholen.

#### **Zu Nummer 12 (§ 28a)**

##### **Zu Buchstabe a (Absatz 2)**

In Absatz 2 sind die verfassungsrechtlichen Vorgaben zum Kernbereichsschutz umgesetzt worden, entsprechend § 34 Absatz 2 BKAG.

Bei den übrigen Änderungen handelt es sich um redaktionelle Folgeänderungen.

##### **Zu Buchstabe b (Absatz 5 Satz 2)**

Es handelt sich um redaktionelle Folgeänderungen. Die im bisherigen § 28 Absatz 7 bis 9 geregelten Benachrichtigungspflichten werden im neuen § 35c aufgenommen.

#### **Zu Nummer 13 (§ 28b)**

Aktuelle technische Entwicklungen schaffen eine neue Gefahrenlage. Zweck dieser Regelung ist die Detektion und Abwehr von Land-, Luft und Wasserfahrzeugen, die nicht durch eine an Bord befindliche Person gesteuert werden (z. B. fernmanipulierte Geräte). Rechtlich abgesichert wird damit insbesondere die Abwehr von Drohnen mit geeigneten technischen Mitteln.

Zum Einsatz gegen fernmanipulierte Geräte kommen in der polizeilichen Praxis moderne Techniken wie Laser, elektromagnetische Impulse, Jamming, GPS-Störung und die Nutzung von Detektionstechnik (Überwachung des elektromagnetischen Wellenspektrums).

#### **Zu Nummer 14 (Überschrift Abschnitt 2 Unterabschnitt 2 Teil 2)**

Es handelt sich um redaktionelle Anpassungen.

#### **Zu Nummer 15 (§§ 29 bis 29e)**

An die Stelle des bisherigen § 29, der die Speicherung, Veränderung und Nutzung von personenbezogenen Daten geregelt hat, treten die neuen §§ 29 bis 29e. Unter Anpassung der Terminologie und Regelungssystematik an das BKAG erfolgt damit die Umsetzung Vorgaben der Richtlinie (EU) 2016/680 und des Urteils des Bundesverfassungsgerichts vom 20. April 2016 (BVerfGE 141, 220) an die Weiterverarbeitung von personenbezogenen Daten.

##### **Zu § 29**

Der neue § 29 (Weiterverarbeitung personenbezogener Daten) enthält in Satz 1 wie der bisherige § 29 Absatz 1 die Generalklausel zur Weiterverarbeitung von Daten, die die Bundespolizei selbst erhoben hat oder die ihr von anderen Behörden übermittelt wurden oder die sonst von der Bundespolizei nicht selbst aktiv beschafft wurden.

Mit Satz 2 wird auch die Befugnis der Bundespolizei zur Weiterverarbeitung personenbezogener Daten zur Erledigung besonderer Ersuchen nach § 17 Absatz 2 des Bundesverfassungsschutzgesetzes aus den bisherigen § 29 Absatz 1 Satz 2 übernommen.

Der neue Satz 3 stellt klar, dass die Bundespolizei unter den Voraussetzungen von Satz 1 und 2 auch Daten verarbeiten darf, die sie nicht aktiv beschafft, sondern die ihr „aufgedrängt“ werden, d. h. von der betroffenen Person selbst oder von Dritten ohne Aufforderung übermittelt werden. Entsprechende Regelungen finden sich im Landesrecht, beispielsweise in § 22 Absatz 1 Satz 2 LSA SOG und § 20 Absatz 1 Satz 2 HSOG. Bei aufgedrängten

Daten ist davon auszugehen, dass eine Datenerhebung vorliegt, wenn die Polizei zur Kenntnisnahme verpflichtet ist, wenn die Daten also ein polizeiliches Tätigwerden erforderlich machen oder machen könnten.

#### **Zu § 29a**

Der neue § 29a (Zweckbindung, Grundsatz der hypothetischen Datenneuverarbeitung) setzt das vom Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 konkretisierte und geprägte Kriterium der hypothetischen Datenneuerhebung für den Bereich der Bundespolizei um.

Satz 1 stellt klar, dass die Verarbeitung von personenbezogenen Daten zur Erfüllung derselben Aufgabe und zum Schutz derselben Rechtsgüter oder zur Verfolgung oder Verhütung derselben Straftaten durch die Bundespolizei nicht den verfassungsrechtlichen Anforderungen an eine Zweckänderung unterliegt. Aufgaben im Sinne der Vorschrift sind die Gefahrenabwehr die Strafverfolgung (nicht die Einzelaufgaben der Bundespolizei nach Abschnitt 1).

Satz 2 trägt den besonderen Anforderungen des Bundesverfassungsgerichts (BVerfG, a. a. O. – Rn. 283) an die Zweckbindung für Daten aus Maßnahmen durch den Einsatz technischer Mittel in oder aus Wohnungen (§ 42) Rechnung. Aufgrund des besonderen Eingriffsgewichts solcher Datenerhebungen sieht Satz 2 vor, dass im Einzelfall eine dringende Gefahr oder eine Gefahrenlage im Sinne des § 42 Absatz 1 vorliegen muss, was eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz ausschließt.

Absatz 2 entspricht § 12 Absatz 2 BKAG. Satz 1 setzt die Vorgaben des Bundesverfassungsgerichts an die zweckändernde Verarbeitung von personenbezogenen Daten um und führt damit den Grundsatz der hypothetischen Datenneuerhebung in das Bundespolizeigesetz ein.

Satz 2 stellt klar, dass der Grundsatz der hypothetischen Datenneuerhebung insbesondere die Nutzung personenbezogener Daten zu Zwecken der Aus- und Fortbildung (neuer § 29d) zum Datenabgleich (§ 34) nicht einschränkt.

Absatz 3 entspricht § 12 Absatz 4 BKAG. Er sieht vor, dass die strengen Vorgaben der Zweckbindung und der Grundsatz der hypothetischen Datenneuerhebung nicht gelten, wenn die Grunddaten einer Person zu Identifizierungszwecken verwendet werden sollen. Da die Datenverwendung so in doppelter Weise eng begrenzt ist – nur Grunddaten nach § 18 Absatz 2 Nummer 1 Buchstabe a BKAG und nur zum Zweck der Identifizierung – ist das Eingriffsgewicht dieser Maßnahme mit der Rechtsprechung des Bundesverfassungsgerichts zu vereinbaren. Weitere Daten – etwa die weiteren zu einer als „Treffer“ identifizierten Person gespeicherten Ereignisse – sind hingegen nach Absatz 5 nicht verfügbar; insoweit bleibt es bei den Begrenzungen nach den Absätzen 2 und 3.

Die zweifelsfreie Klärung der Identität einer Person ist notwendig, um Identitätsverwechslungen auszuschließen und damit zu verhindern, dass Eingriffe in die Grundrechte von unbeteiligten Personen stattfinden. Die Bundespolizei muss daher zur Erfüllung ihrer Aufgaben die Grunddaten einer Person stets zu diesem Zweck verarbeiten können. Der Begriff Grunddaten wird in der BKA-Daten-Verordnung für die verschiedenen Personenkategorien der §§ 18 und 19 legaldefiniert.

Absatz 4 sieht die Verpflichtung der Bundespolizei vor, bei der Verarbeitung von personenbezogenen Daten durch technische und organisatorische Vorkehrungen sicherzustellen, dass die Voraussetzungen des Grundsatzes der hypothetischen Datenneuerhebung beachtet werden. Die in Absatz 5 geregelte Verpflichtung findet ihre nähere Ausgestaltung in § 29e (Kennzeichnung), der festlegt, wie der Grundsatz der hypothetischen Datenneuerhebung technisch durch die Bundespolizei umzusetzen ist. Der Absatz 4 gilt für die Erhebung von neuen Daten sowie grundsätzlich auch für Altdatenbestände. Bei Letzteren ist jedoch zu beachten, dass sich die Mittel der Datenerhebung teilweise nur mit einem erheblichen Aufwand feststellen und kennzeichnen lassen. Die Bundespolizei trifft vor diesem Hintergrund alle angemessenen Maßnahmen, die geeignet sind, die neuen gesetzlichen Vorgaben auch auf Altdatenbestände anzuwenden, ohne die Funktionsfähigkeit der Bundespolizei zu beeinträchtigen.

#### **Zu § 29b**

Der neue § 29b (Daten zu Verurteilten, Beschuldigten, Tatverdächtigen und sonstigen Anlasspersonen) übernimmt die wesentlichen Regelungen aus dem bisherigen § 29 Absatz 2 und systematisiert und ergänzt diese. Die Neufassung dient der Umsetzung des Artikels 6 der Richtlinie (EU) 2016/680, der fordert, dass die Mitgliedstaaten für die Unterscheidbarkeit zwischen den personenbezogenen Daten verschiedener Personenkategorien Sorge zu tragen haben. Hierunter fallen insbesondere Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden, verurteilte Straftäter, Opfer einer Straftat

oder Personen, bei denen bestimmte Fakten darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und andere Parteien im Zusammenhang mit einer Straftat, wie Personen, die bei Ermittlungen in Verbindung mit der betreffenden Straftat oder beim anschließenden Strafverfahren als Zeugen in Betracht kommen, Personen, die Hinweise zur Straftat geben können, oder Personen, die mit Verurteilten, Beschuldigten oder Tatverdächtigen in Kontakt oder in Verbindung stehen.

Absatz 1 entspricht im Wesentlichen dem bisherigen § 29 Absatz 2 und legt – wie auch § 18 Absatz 1 BKAG – fest, dass die Bundespolizei zur Erfüllung ihrer Aufgaben auf dem Gebiet der Strafverfolgung personenbezogene Daten von Verurteilten, Beschuldigten, Tatverdächtigen oder Personen, bei denen ein Anlass dafür besteht (Anlasspersonen) verarbeiten kann. Klarstellend aufgenommen wird die Befugnis zur Verarbeitung personenbezogener Daten von Verurteilten wie in Artikel 6 Buchstabe b der Richtlinie (EU) 2016/680 vorgesehen. Den Verurteilten sind Personen i. S. d. § 81g Absatz 4 StPO gleichgestellt.

Der neue Absatz 2 systematisiert in den Nummern 1 bis 3 die Kategorien der personenbezogenen Daten, die von den in Absatz 1 aufgeführten Personen gespeichert werden dürfen. Eine inhaltliche Änderung ist mit der Neuregelung nicht verbunden. Der bislang verwendete Begriff der „Personendaten“ wird ohne inhaltliche Änderung durch den Begriff der „Grunddaten“ ersetzt. Die Grunddaten von Verurteilten, Beschuldigten, Tatverdächtigen oder Anlasspersonen bilden die entscheidenden Faktoren für die zweifelsfreie, schnelle und effektive Identifizierung der betreffenden Person in den Datenbeständen der Bundespolizei.

Der neue Absatz 3 regelt – wie § 18 Absatz 3 BKAG – die sogenannten Prüffälle. Erhält die Bundespolizei durch Hinweisgeber, aber auch durch in- oder ausländische Polizeidienststellen, Erkenntnisse und Angaben zu Personen, die der Bundespolizei bislang unbekannt waren und bei denen daher auch noch nicht feststeht, ob die betroffenen Personen einer der in Absatz 1 genannten Kategorien unterfallen. Nachdem das Bundeskriminalamt im Rahmen eines ersten Prüfungsschritts feststellen muss, ob die mitgeteilten personenbezogenen Daten und Erkenntnisse zu dieser Person zur Erfüllung seiner Aufgaben benötigt werden, hat sie in einem zweiten Schritt zu ermitteln, welcher Personenkategorie die Betroffenen unterfallen. Die neuen Sätze 1 und 2 legen für diesen zweiten Prüfungsschritt strenge datenschutzrechtliche Maßstäbe fest. Die Verarbeitung und gegebenenfalls Anreicherung der personenbezogenen Daten darf nur zu dem Zweck erfolgen, festzustellen, ob die betroffenen Personen den Kategorien als Verurteilte, Beschuldigte, Tatverdächtige oder Anlasspersonen unterfallen. Satz 4 bestimmt, dass die Daten nach Abschluss der Prüfung, spätestens jedoch nach zwölf Monaten zu löschen sind, soweit nicht festgestellt wurde, dass die betreffende Person die Voraussetzungen nach Absatz 1 erfüllt.

Die Regelungen in Absatz 4 entsprechen denen im bisherigen § 29 Absatz 2 Satz 3 und auch § 18 Absatz 5 BKAG.

### **Zu § 29c**

Der neue § 29c (Daten zu anderen Personen) regelt, unter welchen Voraussetzungen die Bundespolizei personenbezogene Daten von anderen Personen weiterverarbeiten kann.

Absatz 1 greift bisher in § 29 Absatz 3 enthaltene Regelungen auf und entspricht § 19 Absatz 1 BKAG; er dient der Umsetzung von Artikel 6 Buchstabe d der Richtlinie (EU) 2016/680.

Nummer 3 umschreibt den Begriff der Kontakt- und Begleitperson. Hiernach ist eine Kontakt- und Begleitperson eine Person, die mit in Absatz 6 Nummer 1 bis 3 bezeichneten Personen nicht nur flüchtig oder in zufälligem Kontakt, sondern in einer Weise in Verbindung steht, die die Erhebung ihrer personenbezogenen Daten zur Verfolgung oder vorbeugenden Bekämpfung dieser Straftaten erfordert. Die gewählte Begriffsbestimmung entspricht dem vom Bundesverfassungsgericht (BVerfGE 141, 220 – Rn. 168) aufgestellten Voraussetzungen an die Definition einer Kontakt- und Begleitperson, insbesondere fordert sie konkrete Tatsachen für einen objektiven Tatbezug.

Unter die Auskunftspersonen der Nummer 4 fällt auch der Personenkreis des § 44 Satz 1 Nummer 2 (Eigentümer und rechtmäßiger Inhaber der tatsächlichen Gewalt). Dies ist erforderlich vor dem Hintergrund der Ausschreibung von durch Verlust abhanden gekommenen Dokumenten über die Personalien in der Sachfahndung ohne Straftatbezug.

Der neue Absatz 2 regelt wie § 29b Absatz 3 die Prüffälle.

**Zu § 29d**

Der neue § 29d (Weiterverarbeitung von Daten zur Aus- und Fortbildung, zur Vorgangsverwaltung und zur befristeten Dokumentation des polizeilichen Handelns) übernimmt im Wesentlichen die Regelungen aus den Absätzen 5 und 6 des bisherigen § 29.

Absatz 1 entspricht inhaltlich dem bisherigen § 29 Absatz 6. Er wird redaktionell überarbeitet und an die neue Terminologie der Weiterverarbeitung von Daten angepasst.

Absatz 2 entspricht inhaltlich dem bisherigen § 29 Absatz 5. Er wird redaktionell angepasst und an die neue Terminologie der Weiterverarbeitung von Daten angepasst.

**Zu § 29e**

Der neue § 29e (Kennzeichnung) ermöglicht die Umsetzung des Grundsatzes der hypothetischen Datenneuerhebung. Dessen Umsetzung setzt voraus, dass gespeicherte personenbezogene Daten mit den notwendigen Zusatzinformationen versehen sind, das heißt gekennzeichnet, sind.

Absatz 1 Satz 1 sieht dementsprechend vor, dass personenbezogene Daten durch Angabe des Mittels der Erhebung der Daten einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden (Nummer 1), bei Personen, zu denen Grunddaten angelegt wurden, durch die Angabe der Kategorie nach den §§ 29b und 29c (Nummer 2), durch die Angabe der Rechtsgüter, deren Schutz die Erhebung dient oder Straftaten und Ordnungswidrigkeiten, deren Verfolgung oder Verhütung die Erhebung dient (Nummer 3), und durch die Angabe der Stelle, die sie erhoben hat, sofern nicht die Bundespolizei die Daten erhoben hat (Nummer 4) zu kennzeichnen sind. Diese umfassende Kennzeichnung, schafft die Voraussetzung für eine konsistente Anwendung des Grundsatzes der hypothetischen Datenneuerhebung. Nach Absatz 1 Satz 2 kann die Kennzeichnung auch durch die Angabe der Rechtsgrundlage der jeweiligen Mittel der Datenerhebung ergänzt werden.

Zur Vermeidung einer Weiterverarbeitung von Daten, die nicht dem Grundsatz der hypothetischen Datenneuerhebung entspricht, bestimmt Absatz 2, dass personenbezogene Daten, die nicht entsprechend den Anforderungen des Absatzes 1 gekennzeichnet sind, solange nicht weiterverarbeitet werden dürfen, bis eine Kennzeichnung entsprechend den Anforderungen des Absatzes 1 erfolgt ist.

Damit der Grundsatz der hypothetischen Datenneuerhebung auch bei der Weiterverarbeitung von Daten bei anderen Stellen beachtet werden kann, regelt Absatz 3, dass die nach Absatz 1 vorzunehmende Kennzeichnung im Falle der Übermittlung der Daten durch die empfangende Stelle aufrechtzuerhalten ist.

Eine Kennzeichnung von Bild- und Tonaufnahmen, die nach den §§ 26 bis 27c und 41a erstellt wurden, ist aufgrund der Art und dem Umfang der erhobenen Daten erst bei der Übernahme in ein Vorgangs- oder Fallbearbeitungssystem vorzunehmen. Damit wird eine praxisgerechte Ausnahme für die Kennzeichnung von Videoaufzeichnungen der Bundespolizei geschaffen, da bei der Speicherung der Aufnahmen auf den Aufzeichnungsgeräten selbst, die nach Absatz 2 erforderlichen Angaben noch nicht erfasst werden können. Die Kennzeichnung ist jedoch dann vorzunehmen, wenn die Aufnahmen der Gegenstand eines polizeilichen Vorgangs werden und der Bezug zu konkreten Rechtsgütern, Straftaten oder Ordnungswidrigkeiten feststeht.

Es handelt sich bei Absatz 5 um eine Übergangsvorschrift, die § 91 BKAG angeglichen ist. Die Weiterverarbeitung und Übermittlung von personenbezogenen Daten ist bis zum Inkrafttreten der Neufassung des BPolG auch ohne Kennzeichnung zulässig nach den Bestimmungen einer Errichtungsanordnung nach dem bisherigen § 36. Damit soll die Weiterverwendung der nach bisherigem Recht erhobenen „Altdaten“ mit einem für die Bundespolizei vertretbaren Verwaltungsaufwand ermöglicht werden.

**Zu Nummer 16 (§ 31 Absatz 4 Satz 6)**

Es handelt sich um eine redaktionelle Folgeänderung.

**Zu Nummer 17 (§ 31a)**

Der neue § 31a sieht vor, dass die Bundespolizei Ausschreibungen zur polizeilichen Beobachtung oder gezielten Kontrolle im Schengener Informationssystem (SIS) vornehmen kann. Mit der Bezugnahme auf das für die Inbe-

triebnahme des Schengener Informationssystem geltenden Unionsrechts wird die Ausschreibung nach der aktuellen Verordnung (EU) 1987/2006 und dem Beschluss 2007/533/JI sowie zukünftig nach der neuen Verordnung (EU) 2018/1862 ermöglicht.

Im SIS kann die Bundespolizei bisher nur Personen zur Einreiseverweigerung, zur Gewahrsamnahme und zur Aufenthaltsermittlung nach § 30 Absatz 5 ausschreiben. Daneben ergibt sich aus der polizeilichen Praxis die Notwendigkeit, der Bundespolizei die Ausschreibung zur polizeilichen Beobachtung, gezielten Kontrolle oder Ermittlungsanfrage im SIS zu gestatten. Anwendungsfälle ergeben sich insbesondere im Rahmen der Verhinderung der Durchführung von Schleusungsfahrten, wenn polizeiliche Erkenntnisse zu genutzten Fahrzeugen vorliegen.

Mit der Verordnung (EU) 2018/1862 vom 28. November 2018 wird in Artikel 36 Absatz 1 die Ausschreibung im SIS für Ermittlungsanfragen neben der Ausschreibung für verdeckte oder gezielten Kontrollen eingeführt. Damit soll gemäß Erwägungsgrund Nummer 37 eine neue zu ergreifende Maßnahme eingeführt werden, damit eine Person angehalten und befragt werden kann, damit der ausschreibende Mitgliedstaat möglichst detaillierte Informationen erhält. Diese Maßnahme soll für Fälle gelten, in denen eine Person aufgrund eindeutiger Anhaltspunkte verdächtig wird, eine der in Artikel 2 Absätze 1 und 2 des Rahmenbeschlusses 2002/584/JI genannten Straftaten zu planen oder zu begehen, in denen weitere Informationen für die Vollstreckung einer Freiheitsstrafe oder Haftanordnung gegen eine wegen einer der in Artikel 2 Absätze 1 und 2 des Rahmenbeschlusses 2002/584/JI genannten Straftaten verurteilte Person erforderlich sind, oder in denen Grund zu der Annahme besteht, dass sie eine dieser Straftaten begehen wird.

Mit der Ausschreibung zur Ermittlungsanfrage kann die Bundespolizei ergänzende Informationen gewinnen, die über eine reine Kenntnis einer durchgeführten gezielten Kontrolle und der damit in Zusammenhang stehenden Informationen (u. a. Ort, Zeit, Reiseroute, Begleitpersonen) hinausgehen. Anwendungsfälle ergeben sich insbesondere im Rahmen der Verhinderung der Durchführung von Schleusungen (genuines Gefahrenabwehrrecht im Segment der Schadensvertiefung oder der Tatverhinderung), um im weiteren Organisations- und Täterumfeld durch offene Befragungen abstrakte Sachverhaltsbezüge polizeilich bewerten oder Strukturen aufklären zu können. Im diesem Sinne ergänzt die Ermittlungsanfrage die Ausschreibungsoptionen der gezielten und verdeckten Kontrolle.

#### **Zu Nummer 18 (§ 31b)**

Es handelt sich um eine redaktionelle Folgeänderung.

#### **Zu Nummer 19 (§ 32)**

Der neue § 32 (Übermittlung personenbezogener Daten im innerstaatlichen Bereich) Die Gliederung der Vorschriften zur Übermittlung personenbezogener Daten wird neu gefasst. Es erfolgt die Aufteilung der Regelungen zur Übermittlung im innerstaatlichen Bereich, zur Übermittlung an Mitgliedstaaten der Europäischen Union und zur Übermittlung im internationalen Bereich in drei gesonderte Paragraphen. Die Regelungen aus dem bisherigen § 33 werden dabei integriert.

#### **Zu Absatz 1**

Die Ergänzung überträgt die Anforderungen des Bundesverfassungsgerichts aus seinem Urteil vom 20. April 2016 (BVerfG, a. a. O. – Rn. 276f.), den Grundsatz der hypothetischen Datenneuerhebung auf die Datenübermittlung der Bundespolizei an die Polizeien des Bundes und der Länder.

Entgegen § 1 Absatz 4 VwVfG ist der Behördenbegriff nicht organisatorisch, sondern funktional zu verstehen. Vor diesem Hintergrund wurde der bisherige § 32 Absatz 1 Satz 2 gestrichen, da ansonsten bei jeder zwischen Bundespolizeidirektionen stattfindenden Datenübermittlung die personenbezogenen Daten enthält, eine Prüfung der Voraussetzungen des Zweckwechsels obligatorisch wäre. Dabei wurde auch der damit einhergehende nicht unerhebliche Mehraufwand in Betracht gezogen.

#### **Zu den Absätzen 2 und 3**

Absatz 2 entspricht dem bisherigen § 32 Absatz 2 und Absatz 3 entspricht dem bisherigen § 32 Absatz 4; dabei werden aber die Anforderungen des Bundesverfassungsgerichts an den Grundsatz der hypothetischen Datenneuerhebung auf die Datenübermittlung der Bundespolizei an andere inländische öffentliche und an nichtöffentliche Stellen übertragen.

In Absatz 3 Satz 1 wird die Terminologie an das BKAG angepasst.

Absatz 3 wird um einen weiteren Fall („zur Abwehr erheblicher Nachteile für das Gemeinwohl“) ergänzt. Daten der Bundespolizei werden durch die Zentrale Informationsstelle Sporteinsätze an nichtöffentliche Stellen (insbesondere an den Deutschen Fußball Bund) z. B. nach dem Polizeirecht von Nordrhein-Westfalen übermittelt. Laut Schreiben der Datenschutzkonferenz an die Innenministerkonferenz vom 17. Dezember 2018 liegt eine „Umgehung“ bundespolizeilicher Vorschriften vor, soweit die Übermittlung „zur Abwehr erheblicher Nachteile für das Gemeinwohl“ erfolgt. Mit einer entsprechenden Ergänzung von Absatz 3 wird ein Gleichlauf mit nordrhein-westfälischen Vorschriften hergestellt.

#### **Zu Absatz 4**

Absatz 4 entspricht dem bisherigen § 33 Absatz 5.

#### **Zu Absatz 5**

Absatz 5 entspricht dem bisherigen § 33 Absatz 6. Auch der neue Absatz 5 dient der Umsetzung der vom Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 aufgestellten Anforderungen des Grundsatzes der hypothetischen Datenneuerhebung an die weitere Verarbeitung der Daten durch die empfangende Stelle. Auch die empfangende Stelle hat zukünftig die Voraussetzungen des Grundsatzes der hypothetischen Datenneuerhebung zu berücksichtigen, wenn sie die vom Bundeskriminalamt übermittelten Daten zu andern Zwecken, als zu denen die Daten übermittelt wurden, verarbeiten will.

Entscheidend für eine Datenübermittlung an sonstige öffentliche Stellen ist demnach, dass neben konkreten Ermittlungsansätzen für die Aufdeckung von Straftaten oder Gefahren für Rechtsgüter zugleich auch Erkenntnisse zu einer Gefährdung von mindestens gleichwertigen Rechtsgütern vorliegen, die zur Erfüllung der Aufgabe der jeweiligen Behörde bedeutsam sein können.

#### **Zu Absatz 6**

Absatz 6 entspricht dem bisherigen § 33 Absatz 1.

#### **Zu Absatz 7**

Absatz 7 entspricht dem bisherigen § 33 Absatz 2.

#### **Zu Absatz 8**

Absatz 8 entspricht dem bisherigen § 33 Absatz 4.

#### **Zu Absatz 9**

Absatz 9 entspricht dem bisherigen § 33 Absatz 7.

#### **Zu Absatz 10**

Der neue Absatz 10 ermöglicht der Bundespolizei die Teilnahme an einem polizeilichen Datenverbund außerhalb des BKA-Verbunds, die Regelung orientiert sich an § 36e Absatz 4 BremPolG. Ein Beispiel ist die automatisierte Bund-Länder-Datei „PIAS“ (Polizeilicher Informationsaustausch bei Sportveranstaltungen).

#### **Zu Absatz 11**

Absatz 11 übernimmt die Regelung aus dem bisherigen § 32 Absatz 5 auch für den innerstaatlichen Bereich.

#### **Zu Nummer 20 (§§ 32a, 32b und 33)**

##### **Zu § 32a**

Der neue § 32a regelt die Übermittlung personenbezogener Daten durch die Bundespolizei an Mitgliedstaaten der Europäischen Union und Schengen assoziierte Staaten.

Ein effektiver und wirksamer polizeilicher Informationsaustausch zwischen den Sicherheitsbehörden der Mitgliedstaaten der Europäischen Union ist ein Schlüsselement für die Gewährleistung der Sicherheit der Bundesrepublik Deutschland und der Europäischen Union. Nur durch die intensive grenzübergreifende Zusammenarbeit

der europäischen Sicherheitsbehörden bei der Gefahrenabwehr und der Straftatenverhütung und -verfolgung können europaweit Straftaten verhindert, verfolgt und aufgedeckt werden. Vor diesem Hintergrund und der sich stetig vertiefenden europäischen Integration, welche die Europäische Union zu einem gemeinsamen Raum der Freiheit, der Sicherheit und des Rechts gemacht hat, setzt § 53 Absatz 1 den Gleichbehandlungsgrundsatz konsequent um und stellt künftig Datenübermittlung an Mitgliedstaaten der Europäischen Union den inländischen Datenübermittlungen gleich.

Durch Satz 1 Nummer 1 wird die Übermittlung an Behörden, sonstige öffentliche und nichtöffentliche Stellen anderer Mitgliedstaaten der Europäischen Union den Regelungen über Übermittlung an inländische Stellen gleichgestellt. Über Satz 1 Nummer 2 wird klargestellt, dass sich auch Datenübermittlungen an zwischen- und überstaatliche Stellen der Europäischen Union oder deren Mitgliedstaaten, die mit Aufgaben der Verhütung und Verfolgung von Straftaten befasst sind, nach Regelungen über die Übermittlung an Polizeibehörden der Mitgliedstaaten nach Satz 1 Nummer 1 in Verbindung mit § 52 Absatz 1 richten.

Absatz 2 entspricht dem bisherigen § 32a Absatz 6 und Absatz 3 entspricht dem bisherigen § 32 Absatz 5.

### **Zu § 32b**

Der neue § 32b gestaltet die Übermittlung personenbezogener Daten durch die Bundespolizei im internationalen Bereich.

Absatz 1 orientiert sich an § 27 Absatz 1 BKAG und dient über den Verweis auf § 29a der Umsetzung der vom Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 aufgestellten Anforderungen des Grundsatzes der hypothetischen Datenneuerhebung an die Übermittlung von Daten aus besonders eingriffsintensiven Maßnahmen im internationalen Bereich.

Des Weiteren erfolgt ein Hinweis auf die Geltung der im BDSG vorgesehenen Drittstaatenübermittlungsvorschriften.

Absatz 2 orientiert sich an § 27 Absatz 8 BKAG und enthält eine Befugnis zur Datenübermittlung an zwischen- und überstaatliche Stellen, die nicht mit Aufgaben der Verhütung oder Verfolgung von Straftaten befasst sind. Diese Regelung vervollständigt die auf die Verarbeitung bei der Bundespolizei anwendbare Befugnis aus § 81 BDSG, in eng umgrenzten Fällen für die Aufgabenerfüllung Daten an nicht für die Strafverfolgung zuständige Stellen in Drittstaaten zu übermitteln. In Satz 1 wird auf die für die Bundespolizei nach § 81 BDSG bestehende Möglichkeit klarstellend explizit hingewiesen. Durch den Verweis auf § 29a werden die Anforderungen des Grundsatzes der hypothetischen Datenneuerhebung erfüllt.

Absatz 3 legt die Verantwortung für die Übermittlung fest, greift die Regelungen aus dem bisherigen § 33 Absatz 6 Satz 3 und 4 auf und gleicht diese an die Terminologie aus § 27 Absatz 7 BKAG an.

Absatz 4 stellt wie der bisherige § 32 Absatz 5 klar, dass andere Rechtsvorschriften zur Übermittlung personenbezogener Daten unberührt bleiben.

### **Zu § 33**

§ 33 regelt Übermittlungsverbote und Verweigerungsgründe im Rahmen der Datenübermittlung.

Absatz 1 umfasst die Regelungen des bisherigen § 33 Absatz 3 Satz 1. Die Regelungen des bisherigen § 33 Absatz 3 Satz 2 bis 4 entfallen, da über § 32b Absatz 1 die §§ 78, 79 BDSG für die Übermittlung an Drittstaaten anzuwenden sind.

Absatz 2 übernimmt die Regelungen des bisherigen § 33 Absatz 3a Nummer 1 und bisherigen § 33 Absatz 3b Nummer 2.

Ergänzend tragen die neuen Nummern 3 und 4 den vom Bundesverfassungsgericht aufgestellten Anforderungen an die Vergewisserung über das Vorhandensein eines datenschutzrechtlich angemessenen und mit elementaren Menschenrechtsgewährleistungen vereinbaren Umgangs mit den übermittelten Daten im Empfängerstaat und Artikel 38 der Richtlinie (EU) 2016/680 Rechnung.

### **Zu Nummer 21 (§ 33a)**

Der bisherige § 33a zur Umsetzung des „Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden

der Mitgliedstaaten der Europäischen Union“ entfällt aufgrund der neuen Regelungen zur Umsetzung der Richtlinie (EU) 2016/680.

### **Zu Nummer 22 (§ 34a)**

§ 34a sieht die Möglichkeit vor, eine DNA-Referenzdatenbank zu führen, um sogenannte DNA-Trugspuren, die durch Verunreinigungen der betreffenden Spurenträger bei der kriminaltechnischen Untersuchung entstehen können, auszuschließen. Hierdurch können aufwendige Ermittlungsverfahren aufgrund von DNA-Trugspuren verhindert werden.

Die DNA-Analyse nimmt für die Aufklärung von Straftaten mittlerweile eine zentrale Rolle ein. Die Methoden der DNA-Analyse haben sich ständig weiterentwickelt und die für die Analysen notwendige Menge an DNA-Material hat sich beständig verringert. Da mittlerweile bereits in etwa 20 Nanogramm DNA-Material, was der Menge von ca. zwei bis drei DNA-Biomolekülen entspricht, ausreichend ist, um das DNA-Identifizierungsmuster feststellen zu können, können selbst kleinste Verunreinigungen zu so genannten Trugspuren führen. Ein öffentlichkeitswirksames Beispiel für DNA-Trugspuren stellt der Fall des „Phantoms von Heilbronn“ dar. Nachdem am 25. April 2007 in Heilbronn auf der Theresienwiese eine Polizistin getötet wurde und ihr Kollege durch einen Kopfschuss schwerste Verletzungen erlitten hatte, wurde am Tatort ein DNA-Identifizierungsmuster einer weiblichen Unbekannten entdeckt. Bei Abgleichen dieses DNA-Identifizierungsmuster mit den polizeilichen Datenbanken wurde festgestellt, dass in 40 weiteren Fällen übereinstimmende genetische Spuren gefunden wurden. Diese Feststellungen führten zu umfangreichen Ermittlungs- und Fahndungsmaßnahmen in den Jahren 2007 bis 2009 in Süddeutschland, Österreich und Frankreich. Letztendlich stellte sich heraus, dass das fragliche DNA-Identifizierungsmuster von einer Mitarbeiterin der Herstellerfirma der für die Spurensicherung eingesetzten Wattestäbchen stammte und es sich damit um eine DNA-Trugspur handelte.

Eine unter Datenschutzgesichtspunkten weniger belastende anonymisierte Speicherung der DNA-Identifizierungsmuster ist nicht möglich. Denn neben der Feststellung, dass es sich um eine Trugspur handelt, ist es von wesentlicher Bedeutung, zu ermitteln, auf welche Weise das Spurenmaterial verunreinigt wurde. Nur auf diese Weise lässt sich für künftige Fälle das Risiko einer erneuten Verunreinigung minimieren. Mit einer anonymisierten Speicherung ist dies nicht möglich.

Der neue Absatz 1 ermöglicht der Bundespolizei, von ihren Beschäftigten, die Umgang mit Spurenmaterial haben oder die Bereiche in ihren Liegenschaften und Einrichtungen betreten müssen, in denen mit Spurenmaterial umgegangen oder dieses gelagert wird, mittels eines Mundschleimhautabstrichs oder einer hinsichtlich ihrer Eingriffsintensität vergleichbaren Methode Körperzellen zu entnehmen, hieraus das DNA-Identifizierungsmuster festzustellen und dieses mit an Spurenmaterial festgestellten DNA-Identifizierungsmustern automatisiert abzugleichen. Der Abgleich darf nur zu dem Zweck erfolgen, DNA-Trugspuren zu erkennen.

Nach Satz 2 darf die Entnahme der Körperzellen nicht erzwungen werden.

Satz 3 und 4 legen enge Zweckbindungen der Nutzung der Daten fest: Die entnommenen Körperzellen dürfen nur zur Feststellung des DNA-Identifizierungsmuster genutzt werden. Sie sind unverzüglich zu vernichten, sobald sie hierfür nicht mehr erforderlich sind. Andere Feststellungen als diejenigen, die zur Ermittlung des DNA-Identifizierungsmusters erforderlich sind, dürfen bei der Untersuchung des DNA-Identifizierungsmusters nicht getroffen werden.

Der neue Absatz 2 gibt der Bundespolizei die Möglichkeit, unter den Voraussetzungen des Absatzes 1 DNA-Identifizierungsmuster von anderen Personen zum Aufdecken von DNA-Trugspuren zu untersuchen und abzugleichen. Die Untersuchungen und Abgleiche dürfen nur mit dem schriftlichen Einverständnis der betreffenden Person erfolgen.

Nach Absatz 3 Satz 1 sind die DNA-Identifizierungsmuster zu pseudonymisieren und darüber hinaus in einem gesonderten Informationsbestand der Bundespolizei zu speichern. Satz 2 verbietet eine Verwendung der DNA-Identifizierungsmusters zu anderen als den in den Absätzen 1 bis 3 genannten Zwecken. Satz 3 sieht vor, dass die DNA-Identifizierungsmuster unverzüglich zu löschen sind, wenn ihre Verarbeitung für die Zwecke nicht mehr erforderlich ist. Nach Satz 4 hat die Löschung spätestens drei Jahre nach dem letzten Umgang der betreffenden Person mit Spurenmaterial oder dem letzten Zutritt zu einem Bereich, in dem mit Spurenmaterial umgegangen wird, zu erfolgen. Satz 5 sieht vor, dass Betroffene schriftlich über den Zweck und die Verarbeitung der erhobenen Daten zu informieren sind.

**Zu Nummer 23 (§ 35)**

Der neue § 35 (Aussonderungsprüffristen) nimmt die Regelungen aus dem bisherigen § 35 auf und konkretisiert die sich aus § 75 BDSG ergebende Verpflichtung, Lösch- bzw. Aussonderungsprüffristen vorzusehen. Die Regelungen des bisherigen § 35 werden mit dem Ziel der Vereinheitlichung der gesetzlichen Regelungen in den Polizeigesetzen des Bundes in zwei Paragraphen aufgeteilt und in ihrer Struktur an die §§ 77 und 78 BKAG angepasst.

**Zu Nummer 24 (§§ 35a bis 35f)**

Die §§ 35a bis 35f treffen insbesondere Regelungen zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 20. April 2016 und lehnen sich an die vergleichbaren Bestimmungen des BKAG an.

**Zu § 35a**

Der neue § 35a (Löschung von durch Besondere Mittel der Datenerhebung oder vergleichbare Maßnahmen erlangten personenbezogenen Daten) entspricht § 79 BKAG und vollzieht auch die Entscheidung des Bundesverfassungsgerichts vom 20. April 2016 (a. a. O. – Rn. 269 ff.) nach.

**Zu § 35b**

Der neue § 35b (Berichtigung personenbezogener Daten, Einschränkung der Verarbeitung in Akten und Vernichtung von Akten) trifft gesonderte Regelungen für die Berichtigung personenbezogener Daten und die Einschränkung der Verarbeitung in Akten, die bisher ebenfalls im bisherigen § 35 enthalten waren. Der neue § 35b orientiert sich an § 78 BKAG.

**Zu § 35c**

Der neue § 35c (Benachrichtigung bei verdeckten und eingriffsintensiven Maßnahmen) entspricht § 74 BKAG.

Die Vorschrift setzt einerseits die Anforderungen aus dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 (BVerfGE 141, 220 – Rn. 136) an Benachrichtigungspflichten bei verdeckten und sonstigen eingriffsintensiven Maßnahmen um. Andererseits führt sie die bereits bestehenden Benachrichtigungsvorschriften an einer Stelle zusammen.

**Zu § 35d**

Der neue § 35d (Benachrichtigung über die Speicherung personenbezogener Daten von Kindern) entspricht § 75 BKAG und schafft damit einheitliche Regelungen für BKA und Bundespolizei hinsichtlich der Benachrichtigungspflichten über die Speicherung personenbezogener Daten von Kindern.

**Zu § 35e**

Der neue § 35e (Protokollierung) trifft zum BDSG ergänzende Regelungen zur Protokollierung von Verarbeitungsvorgängen. Die Vorschrift ist § 81 BKAG nachgebildet.

Absatz 1 legt über § 76 Absatz 2 BDSG hinausgehend und diesen ergänzend in seiner Nummer 1 fest, dass die Protokolle der oder dem Beauftragten für den Datenschutz und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in elektronisch auswertbarer Form zum Zwecke der Datenschutzkontrolle zur Verfügung stehen müssen, um eine effiziente und IT-gestützte Datenschutzkontrolle zu ermöglichen. Nach Nummer 2 muss die Protokollierung es außerdem ermöglichen, zu überprüfen, ob die Regelungen über Zugriffsberechtigungen eingehalten werden.

Absatz 2 trifft datenschutzfreundliche Regelungen zur Löschung der Protokolldaten.

**Zu § 35f**

Der neue § 35f (Protokollierung bei verdeckten und eingriffsintensiven Maßnahmen) setzt einerseits die Anforderungen aus dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 (BVerfGE 141, 220 – Rn. 141, 267) an eine umfassende Protokollierungspflicht bei verdeckten und sonstigen eingriffsintensiven Maßnahmen um. Andererseits führt sie die bereits bestehenden Protokollierungsvorschriften an einer Stelle zusammen. Die Regelung ist § 82 BKAG nachgebildet.

**Zu Nummer 25 (§§ 36 und 37)****Zu § 36**

Der neue § 36 (Verzeichnis von Verarbeitungstätigkeiten) trifft ergänzend zu § 70 BDSG konkretisierende Regelungen. Anstelle der Errichtungsordnung nach dem bisherigen § 36 ist künftig ein Verzeichnis von Verarbeitungstätigkeiten zu führen, das im Wesentlichen die gleichen Inhalte enthalten werden. Das Verzeichnis von Verarbeitungstätigkeiten ermöglicht die interne und externe Datenschutzkontrolle.

Absatz 1 stellt klar, dass die Bundespolizei zusätzlich zu den Angaben nach § 70 BDSG zu den Zugriffsberechtigungen aufnimmt. Des Weiteren sind zu den betroffenen Verfahren auch Angaben zur Übermittlung im Wege eines eingerichteten automatisierten Abrufverfahrens und zur Auftragsverarbeitung aufzunehmen.

Nach Absatz 2 ist das Verzeichnis von Verarbeitungstätigkeiten zentral beim Bundespolizeipräsidium zu führen. Es ist dort laufend zu aktualisieren. Zur Qualitätssicherung wird durch Satz 2 die Beteiligung der Datenschutzbeauftragten der Bundespolizeibehörden vorgeschrieben.

In Absatz 3 wird bestimmt, dass das Verzeichnis von Verarbeitungstätigkeiten und dessen Aktualisierungen der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur Verfügung zu stellen ist. Insofern wird über § 70 Absatz 4 BDSG hinausgegangen, der eine Zurverfügungstellung lediglich „auf Anfrage“ vorsieht.

**Zu § 37**

Der neue § 37 trifft ergänzende Regelungen zu den Befugnissen der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die datenschutzaufsichtliche Zuständigkeit der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für die Datenverarbeitung sowie Regelungen zur Ausgestaltung seines Amtes und allgemeine Beschreibungen seiner Aufgaben und Befugnisse finden sich im Bundesdatenschutzgesetz. § 37 dient insofern nur der Ergänzung.

Absatz 1 dient der Umsetzung der Anforderungen aus dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 zum BKAG (BVerfG, a. a. O. – Rn. 140 f., 266, 340 und 354) im Hinblick auf die aufsichtliche Kontrolle der Wahrnehmung der Verarbeitungsbefugnisse der Bundespolizei. Hierzu wird angeordnet, dass die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Kontrollen im Hinblick auf die Datenverarbeitung bei Maßnahmen nach § 22a (Erhebung von Telekommunikationsdaten), § 27d (Überwachung der Telekommunikation), § 27e (Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten), § 28 (Besondere Mittel der Datenerhebung) und § 28a (Einsatz technischer Mittel zur Eigensicherung) sowie der Übermittlung nach § 32b (Übermittlung personenbezogener Daten im internationalen Bereich) durchführt. Die Regelungen orientieren sich an § 69 Absatz 1 BKAG.

Absatz 2 bestimmt, dass der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit – auch in Umsetzung von Artikel 47 Absatz 2 der Richtlinie (EU) 2016/680 – die Befugnis hat, gegenüber der Bundespolizei verbindliche Maßnahmen anzuordnen, sofern sie datenschutzrechtliche Verstöße zuvor nach den allgemeinen Regelungen des § 16 Absatz 2 BDSG beanstandet hat. Diese Maßnahmen schließen nicht die Löschung personenbezogener Daten ein und setzen voraus, dass ein erheblicher Verstoß in Rede stehen muss. Die in § 61 BDSG niedergelegten Rechtsschutzmöglichkeiten gegen solche verbindlichen Maßnahmen bleiben unberührt.

**Zu Nummer 26 (Überschrift Abschnitt 2 Unterabschnitt 2 Teil 3)**

Es handelt sich um redaktionelle Anpassungen.

**Zu Nummer 27 (§ 38a)**

Durch die neu in das Bundespolizeigesetz aufgenommene Vorschrift erhält die Bundespolizei die Befugnis, zur Abwehr von Gefahren sowie zur Verhütung von Straftaten Personen zu untersagen, sich an bestimmten Orten aufzuhalten (Aufenthaltsverbot). Dieses Verbot ergänzt den in § 38 geregelten „klassischen“ Platzverweis, der nur eine vorübergehende Entfernung einer Person von einem bestimmten Ort bezweckt. Vergleichbare Regelungen finden sich in nahezu allen Landespolizeigesetzen sowie auch in § 68b Absatz 1 Satz 1 Nummer 1 und 2 StGB.

#### Zu Satz 1

Zweck des Aufenthaltsverbotes ist es, den Aufenthalt an Orten zu verhindern, an denen sich das Risiko der Verwirklichung der abzuwehrenden Gefahr erhöht. Es müssen nachprüfbare Tatsachen vorliegen, die zu der Prognose berechtigen, dass eine Person an einer bestimmten Örtlichkeit eine Straftat im Sinne des § 12 Absatz 1 begehen wird, die für sich genommen oder aufgrund des wiederholenden Charakters erhebliche Bedeutung haben würde (Gefahrenprognose).

So ist die Bundespolizei mit einschlägig wegen schwerer Gewaltdelikte im Kontext des Fußballfanreiseverkehrs in Erscheinung getretenen Personen konfrontiert, die wiederholt versuchen, z. B. anlässlich von Fußballveranstaltungen, Spielorte unter Nutzung von öffentlichen Verkehrsmitteln (§§ 3 oder 4) zu erreichen oder auch gewalttätige Aktionen am Rande der Veranstaltung zu initiieren, zum Beispiel in Form eines Abfangens des „gegnerischen Fanzugs“. Der in seiner örtlichen Ausdehnung stark eingegrenzte Platzverweis ist in diesen Fällen zur Verhinderung der Anreise oder auch der Teilnahme von Personen an gewalttätigen Aktionen am Rande der Veranstaltung ungeeignet.

#### Zu Satz 2

Nach Satz 2 ist die Anordnung zudem auf den zur Abwehr der Gefahr oder zur Straftatenverhütung erforderlichen zeitlichen und örtlichen Umfang zu beschränken. Die Dauer der Maßnahme ist auf höchstens drei Monate zu befristen (vgl. Satz 1).

#### Zu Satz 3

Nach Satz 3 müssen bei der Anordnung eines Aufenthaltsverbots berechnete Interessen der betroffenen Personen berücksichtigt werden, z. B. Wege zur Wohnung, zum Arbeitsplatz oder beruflich bedingte Reisen. Dies kann zu einer veränderten Ausgestaltung des Verbots oder auch zur Unzulässigkeit führen.

#### Zu Satz 4

Die Maßnahme kann nicht bei Versammlungen angeordnet werden. Sie wäre auch als Auflage i. S. d. § 15 Versammlungsgesetz nicht vertretbar, da die Auflage sich nur auf einen bestimmten Versammlungsfall beziehen kann. Satz 4 stellt insoweit klar, dass die Vorschriften des Versammlungsrechts unberührt bleiben.

### **Zu Nummer 28 (§ 41a)**

Im Zuge der bundeseinheitlichen technischen Ertüchtigung von Gewahrsamsräumen ist auch eine mögliche Überwachung mittels Videoanlagen vorgesehen. Die Überwachung kann nur offen, also erkennbar, erfolgen. Eine verdeckte Aufnahme ermöglicht die neue Befugnis nicht.

Zielrichtung ist der Schutz der Gewahrsamsinsassen vor unrechtmäßigen Handlungen der eingesetzten Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten sowie deren Schutz vor Angriffen in gleichem Maße. Eine Unterscheidung zwischen Gewahrsamsräumen, die offen, und solchen, die verschlossen sind, ist nicht vorzunehmen.

Durch eine offene Videoüberwachung soll die Hemmschwelle für Übergriffe auf Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten heraufgesetzt und gleichzeitig das Handeln der Aufsichtspersonen dokumentiert werden. Darüber hinaus ergibt sich für die Aufsichtspersonen eine zusätzliche Möglichkeit, ihrer Kontrollpflicht nachzukommen, sofern Leib oder Leben der festgehaltenen Person gefährdet erscheint.

Auch die Bundesstelle zur Verhütung von Folter kommt in ihrem Jahresbericht 2016 zu dem Schluss, dass der Einsatz von Video- und Tonüberwachung in Gewahrsamsräumen sich positiv zum Schutz aller beteiligten Personen auswirkt.

### **Zu Absatz 1**

Nach Absatz 1 dürfen bei Anwesenheit von Beamtinnen und Beamten im Gewahrsamsraum einer festgehaltenen Person zum Schutz der festgehaltenen Person oder der Polizeibeamtin und des Polizeibeamten Bild- und Tonaufnahmen erstellt werden. Neben Bildaufzeichnungen ist die Nutzung von Tonaufnahmen angezeigt, da tätlichen Auseinandersetzungen häufig verbale Auseinandersetzungen vorausgehen. Entsprechende Aufnahmen sind daher geeignet, eine vollständige Aufklärung der Situation, insbesondere auch in Bezug auf ihre Entstehung, zu ermöglichen.

**Zu Absatz 2**

Nach Absatz 2 sind – ohne Anwesenheit von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten – zum Schutz der Privatsphäre der festgehaltenen Person grundsätzlich nur Bildaufnahmen und diese nur kurzzeitig für einen Zeitraum von einigen Sekunden zulässig, wenn eine Gefahr für Leib oder Leben der Person zu besorgen ist, insbesondere Suizidgefahr besteht. Die Person muss in diesen Fällen durch die Gewahrsamsbeamten kurz in Augenschein genommen werden können, um z. B. etwaige Selbstverletzungshandlungen auszuschließen. Der Maßnahme kann auch abschreckende und damit gefahrenabwehrende Wirkung zukommen, gerade im Falle von denkbaren Fremdgefährdungen. „Soweit“ begrenzt die Maßnahme in zeitlicher Hinsicht auf die Dauer, die zur Erforschung der Gefahr erforderlich ist.

**Zu Absatz 3**

Absatz 3 enthält zum Schutz der Privat- und Intimsphäre der festgehaltenen Person Vorschriften betreffend die Ausgestaltung der Überwachungsmöglichkeit.

**Zu den Absätzen 4 und 5**

Die Absätze 4 und 5 regeln Dokumentationspflichten und über den Verweis auf § 27a Absatz 4 die in Bezug auf die erhobenen personenbezogenen Daten geltenden Aufbewahrungs- und Löschfristen.

**Zu Nummer 29 (§ 43)**

Die Überschrift wird angepasst.

Der neue Absatz 6 orientiert sich an § 36 Hessisches Sicherheits- und Ordnungsgesetz und dient der Eigensicherung von Polizeivollzugsbeamten. Danach können körperliche Eingriffe bei denjenigen Personen vorgenommen werden, die möglicherweise eine Gefahr für andere verursachen. Damit wird die Blutentnahme bei Personen, die möglicherweise HIV-positiv sind und z. B. bei ihrer Festnahme Polizeibeamte verletzt haben, auf eine gesetzliche Grundlage gestellt. Die Maßnahmen dürfen außer bei Gefahr im Verzug nur richterlich angeordnet werden.

**Zu Nummer 30 (§ 62 Absatz 3)**

Bis zum Jahr 1992 zahlte die Bahnpolizei als Teil der Bundesbahn in der Zuständigkeit des Verkehrsministeriums keine Selbstkosten für die Unterbringung.

Die Verkehrsbetreiber (vornehmlich Deutsche Bahn AG – DB AG) entziehen sich vermehrt ihrer gesetzlichen Verpflichtung zur kostengünstigen Bereitstellung zur Wahrnehmung der bundespolizeilichen Aufgaben erforderlichen Diensträume, in dem sie selbst ein Flächenföhl herbeiföhren (z. B. durch Fremdvermietung) oder Liegenschaftsveräußerung und die Unterbringung in Investorenbauten auf ihren Grundstücken anbieten. Während die DB AG nach dem bisherigen § 62 Absatz 3 von der Bundespolizei lediglich ein „gedeckeltes“ Nutzungsentgelt (sog. Selbstkosten) verlangen kann, sind mit der Vermietung von Flächen an Gewerbetreibende höhere Erträge verbunden. Für Investoren, die bahneigene Flächen kaufen/bebauen, besteht keine gesetzliche Verpflichtung, die Bundespolizei unterzubringen bzw. Selbstkosten zu fordern. Die Bundespolizei ist dann zur Entrichtung der marktüblichen Gewerbemiete genötigt oder wird aus den Liegenschaften verdrängt. Dies föhrt zu einer Sicherheitsgeföhrdung und unverhältnismäßigen Belastung der Bundespolizei. Die Aufgabenwahrnehmung der Bundespolizei liegt auch im wesentlichen Interesse der jeweiligen Betreiber von Verkehrsunternehmen, da sie die Sicherheit gewöhrliefert und den reibungslosen Betrieb ermöglicht und insofern Zeit und Kosten spart, die ansonsten für eigene Maßnahmen zur Gewährleistung der Sicherheit an Bahnhöfen sowie Flug- und Seehäfen von den Unternehmen aufgewendet werden müssten. Die Verkehrsunternehmen sparen hohe Personal und Sachmittel, die nur zum geringen Teil durch Investitionen in die bundespolizeiliche Unterbringung abgebildet werden.

Der bisherige § 62 Absatz 3 enthält keine Regelung zur Gestellung von Ersatzflächen. Die Regelungslücke betrifft sowohl Fälle einer erforderlichen Drittanmietung (bislang über die Bundesanstalt für Immobilienaufgaben) als auch Fälle einer Ersatzunterbringung im engeren Sinne (z. B. Auszug der Bundespolizei aufgrund Sanierungsarbeiten im Bahnhof), die nunmehr die Betreiber in die Verantwortung nimmt und zur Kostentragung verpflichtet.

Die nunmehrige Anpassung durch Neufassung des § 62 Absatz 3 zugunsten der Bundespolizei ist insofern sachgerecht, da diese den von den Betreibern eröffneten Verkehr auch in deren Interesse schützt. Ohne die Einrichtung eines entsprechenden Verkehrs durch die Unterstützungspflichtigen, wäre eine Unterbringung auf deren Liegenschaften nicht erforderlich.

**Zu Nummer 31 (§ 69a Absatz 1)**

Es handelt sich um eine redaktionelle Folgeänderung.

**Zu Nummer 32 (§ 71)**

In § 71 (Berichtspflicht) gegenüber dem Deutschen Bundestag werden in Umsetzung der im Urteil des Bundesverfassungsgerichts vom 20. April 2016 (BVerfGE 141, 220 – Rn. 143, 268) enthaltenen Anforderungen turnusmäßige Berichtspflichten der Bundespolizei bzgl. der nach den §§ 26, 27, 27b, 27d, 27e, 28, 28a, 28b, 30 bis 31a enthaltenen Befugnisse eingeführt. Das Bundesverfassungsgericht hatte für verdeckte und eingriffsintensive Überwachungsmaßnahmen eine Berichtspflicht gefordert, da betroffene Personen und die Öffentlichkeit die Maßnahme unmittelbar nicht wahrnehmen und lediglich nachträglichen Rechtsschutz beanspruchen können; durch eine Berichtspflicht soll darüber hinaus eine öffentliche Diskussion über die Ausübung dieser Befugnisse ermöglicht werden.

Dabei wird die Berichtspflicht auch auf die Wahrnehmung der Befugnisse zur Übermittlung personenbezogener Daten im internationalen Bereich (§ 32b) ausgedehnt, soweit die übermittelten Daten im Zusammenhang mit den vorgenannten Maßnahmen erlangt wurden. Die prozedurale Ausgestaltung der Berichtspflicht, d. h. die Berichterstattung des Bundespolizeipräsidiums an das Bundesministerium des Innern, für Bau und Heimat (BMI) und Weiterleitung von dort an die Bundesregierung und den Deutschen Bundestag spiegelt die fachaufsichtliche Rolle des BMI adäquat wider.

**Zu Artikel 2 (Änderung des Gesetzes über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes)**

In § 12 Absatz 2 Satz 1 wird die Einführung des finalen Rettungsschusses zur Schaffung größerer Rechtsklarheit und -sicherheit in Amok-, Geisel- und Piraterielagen vorgenommen (Anpassung an § 41 Absatz 2 Satz 2 MEPolG/Ländergesetze).

Wenn keine anderen geeigneten polizeilichen Mittel gegeben sind, um das Leben Unschuldiger zu retten, muss auch mit dem Ziel geschossen werden können, evtl. zu töten. Mit der Einschränkung, dass der finale Rettungsschuss „das einzige Mittel zur Abwehr einer gegenwärtigen Lebensgefahr oder der gegenwärtigen Gefahr einer schwerwiegenden Verletzung der körperlichen Unversehrtheit ist“, wird Artikel 2 EMRK Rechnung getragen, wonach die Tötung eines Menschen nur dann nicht verboten ist, wenn sie „zur Verteidigung eines Menschen gegenüber rechtswidriger Gewaltanwendung“ vorgenommen wird.

**Zu Artikel 3 (Änderung des Aufenthaltsgesetzes)**

Nach Abschluss der strafprozessualen Maßnahmen nach § 12 Absatz 1 Satz 1 Nummer 2 BPolG ist die Bundespolizei bei vollziehbar ausreisepflichtigen Ausländern sodann zuständig für die aufenthaltsbeendenden Maßnahmen, einschließlich der Beantragung von Haft zur Sicherung der Abschiebung. Als eine Lehre aus dem Anschlag auf den Berliner Weihnachtsmarkt am 19. Dezember 2016 sollten zuständigkeitsbedingte Brüche im Bearbeitungsprozess durch Schnittstellenreduzierung vermieden werden – dem dient die hier vorgenommene Zuständigkeitsarrondierung im bundespolizeilichen Aufgabenbereich. Die legislativen Anpassungen sind nur in dieser Verzahnung repressiver und aufenthaltsrechtlicher Maßnahmen sinnvoll, zumal im Rahmen der Feststellung des unerlaubten Aufenthaltes in der beschriebenen Fallkonstellation die polizeiliche Sachbearbeitung bereits überwiegend in der Hand der Bundespolizei liegt.

Entsprechend der Zuständigkeit für die Verfolgung von Straftaten nach § 13 Absatz 1 Satz 1 Nummer 2 BPolG ist ein neuer Absatz 3a erforderlich, da sich die Zuständigkeitszuweisung des § 71 Absatz 3 ausschließlich auf die mit der polizeilichen Kontrolle des grenzüberschreitenden Verkehrs beauftragten Behörden bezieht.

Der durch die Regelung erfassten Hauptanwendungsfälle betreffen vollziehbar ausreisepflichtige Ausländer ohne Duldung und solche Duldungsinhaber, die die Beschaffung der Heimreisedokumente behindern und insoweit wegen fehlender Passdokumente aus tatsächlichen Gründen geduldet werden (§ 60a Absatz 2 Satz 1 Alternative 1).

Darüber hinaus werden auch andere Fälle der vorübergehenden Aussetzung der Abschiebung erfasst, sofern unter Berücksichtigung des Einzelfalls davon ausgegangen werden kann, dass die Gründe für die Aussetzung der Abschiebung insbesondere bei Ermessensduldungen zwischenzeitlich entfallen sind oder demnächst entfallen und

die Abschiebung des betroffenen Drittstaatsangehörigen innerhalb von sechs Monaten wahrscheinlich ist. Denkbare Anwendungsfälle sind Duldungserteilungen an Drittstaatsangehörige, deren Anwesenheit im Bundesgebiet von der Staatsanwaltschaft oder dem Strafgericht für sachgerecht erachtet wurde (§ 60 Absatz 2 Satz 2) oder Duldungserteilungen aus dringenden persönlichen Gründen, z. B. zur Beendigung einer Drogentherapie, Durchführung einer ärztlichen Behandlung, unmittelbar bevorstehenden Heirat, Betreuung von Familienangehörigen oder Abschluss einer Berufsausbildung (§ 60a Absatz 2 Satz 3), sofern einzelfallbezogen davon ausgegangen werden kann, dass der Duldungsgrund tatsächlich entfallen ist oder in allernächster Zukunft entfällt. Die diesbezügliche Feststellung obliegt der zuständigen Erteilungsbehörde, die von der Bundespolizei unverzüglich in Kenntnis gesetzt wird.

Im Falle der festgestellten Ausreisepflicht prüft die Bundespolizei in eigener Zuständigkeit aufenthaltsbeendende Maßnahmen sowie erforderlichenfalls freiheitsentziehende Maßnahmen zur Vorbereitung oder Sicherung aufenthaltsbeendender Maßnahmen im Zuge des gesetzlichen Befugnisrahmens des § 62 AufenthG in Verbindung mit den Vorschriften nach dem Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG).

Mit dem Beginn der Zuständigkeit übernimmt die Bundespolizei die Fallbearbeitung von der bisher befassten Ausländerbehörde und stimmt sich mit dieser auch im Verlauf des aufenthaltsbeendenden Verfahrens anlassbezogen ab.

Satz 2 legt fest, dass die Zuständigkeit der Bundespolizei auf maximal sechs Monate begrenzt ist. Sie endet, wenn die Abschiebung (z. B. mangels erfolgreicher Passersatzbeschaffung) in diesem Zeitraum nicht gelingt und dies in absehbarer Zeit auch nicht zu erwarten ist oder, wenn nachträglich tatsächliche oder rechtliche Hindernisse auftreten, die der Abschiebung innerhalb von sechs Monaten nach der Feststellung der Drittstaatsangehörigen im Zuständigkeitsbereich der Bundespolizei entgegenstehen. Nach diesem Zeitraum lebt die Zuständigkeit der bisher befassten Aufenthaltsbehörde wieder auf.

#### **Zu Artikel 4 (Inkrafttreten)**

Die Vorschrift regelt das Inkrafttreten.