

## **Gesetzentwurf der Bundesregierung**

### **Entwurf eines Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus**

#### **A. Problem und Ziel**

Bei der Aufklärung des transnational operierenden und vernetzten Terrorismus sind eine Vielzahl von Behörden – national und insbesondere auch international – tätig, deren Erkenntnisse zusammengeführt und übergreifend analysiert werden müssen.

#### **B. Lösung**

Dies wird durch zeitgemäßen IT-Einsatz mit der Einrichtung gemeinsamer Dateien unterstützt. Hierzu erhält das Bundesamt für Verfassungsschutz (BfV) spezielle Befugnisse zur Einrichtung gemeinsamer Dateien mit Partnerdiensten. Zudem sollen bereits auf nationaler Ebene gemeinsame Projektdateien der Sicherheitsbehörden verlängert eingerichtet werden können. Bei der Gelegenheit werden weitere Regelungen zur verbesserten Terrorismusbekämpfung aufgenommen.

#### **C. Alternativen**

Keine.

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

Keine.

#### **E. Erfüllungsaufwand**

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

Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

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

Durch die in Artikel 9 vorgenommene Änderung des Telekommunikationsgesetzes ist eine dauerhafte, zusätzliche Belastung der Telekommunikationsdiensteanbieter zu erwarten, die sich derzeit nicht ermitteln lässt. Eine Bewertung kann gegebenenfalls erst nach Inkrafttreten der gesetzlichen Regelung vorgenommen werden. Eine erste Nacherfassung erfolgt vor Abschluss der parlamentarischen Befassung.

Weitere Belastungen für die Wirtschaft entstehen nicht.

## **E.3 Erfüllungsaufwand für die Verwaltung**

Mit der Einführung gemeinsamer Dateien mit ausländischen Partnerdiensten entstehen dem BfV jährliche Personal- und Sachkosten in Höhe von rund 2,9 Millionen Euro sowie einmalige Sachkosten in Höhe von rund 2,9 Millionen Euro.

Mit der Änderung des Bundespolizeigesetzes entstehen der Bundespolizei jährliche Personal- und Sachkosten in Höhe von rund 1,4 Millionen Euro sowie einmalige Sachkosten in Höhe von rund 700 000 Euro.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat mitgeteilt, insbesondere die Errichtung gemeinsamer Dateien mit ausländischen Nachrichtendiensten sowie die Befugnisweiterungen zugunsten der Bundespolizei führten bei ihr zu einem Mehrbedarf an Personalmitteln verbunden mit jährlichen Personalkosten in Höhe von rund 350 000 Euro.

Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen soll finanziell und stellenmäßig im jeweiligen Einzelplan eingespart werden.

Weiterer Aufwand für die Verwaltung der Länder und Kommunen entsteht nicht.

## **F. Weitere Kosten**

Keine.

# **Entwurf eines Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus**

**Vom ...**

Der Bundestag hat das folgende Gesetz beschlossen:

## **Artikel 1**

### **Änderung des Bundesverfassungsschutzgesetzes**

Das Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch [...] geändert worden ist, wird wie folgt geändert:

1. § 22a Absatz 4 Satz 2 wird wie folgt gefasst:

„Die Frist kann um zwei Jahre und danach um ein weiteres Jahr verlängert werden, wenn das Ziel der projektbezogenen Zusammenarbeit bei Projektende noch nicht erreicht worden ist und die Datei weiterhin für die Erreichung des Ziels erforderlich ist.“

2. Nach § 22a werden die folgenden §§ 22b und 22c eingefügt:

#### **„§ 22b**

**Errichtung gemeinsamer Dateien mit ausländischen Nachrichtendiensten**

(1) Das Bundesamt für Verfassungsschutz kann für die Zusammenarbeit mit ausländischen öffentlichen Stellen, die mit nachrichtendienstlichen Aufgaben betraut sind (ausländische Nachrichtendienste), zur Erforschung von Bestrebungen oder Tätigkeiten, die sich auf bestimmte Ereignisse oder Personenkreise beziehen, gemeinsame Dateien einrichten, wenn

1. die Erforschung von erheblichem Sicherheitsinteresse für die Bundesrepublik Deutschland und den jeweils teilnehmenden Staat ist,
2. in den teilnehmenden Staaten die Einhaltung grundlegender rechtsstaatlicher Prinzipien gewährleistet ist,
3. die Festlegungen und Zusagen nach Absatz 5 Satz 1 verlässlich sind und
4. das Bundesministerium des Innern zugestimmt hat.

(2) Der Nachrichtendienst eines Staates, der weder unmittelbar an die Bundesrepublik Deutschland angrenzt noch Mitgliedstaat der Europäischen Union oder des Nordatlantikvertrages ist, kann darüber hinaus nur teilnehmen, wenn besondere Sicherheitsinteressen dies erfordern. Dies ist der Fall, wenn Bestrebungen

oder Tätigkeiten erforscht werden, die auf die Begehung von schwerwiegenden Straftaten gegen den Bestand oder die Sicherheit eines Staates oder einer internationalen Organisation gerichtet sind. Schwerwiegende Straftaten sind die in § 3 Absatz 1 des Artikel 10-Gesetzes genannten Straftaten. Die Teilnahme eines solchen ausländischen Nachrichtendienstes bedarf der Zustimmung der Bundesministerin oder des Bundesministers des Innern.

(3) Die Datei dient der Feststellung, ob zu Personen, Objekten oder Ereignissen bei einem der beteiligten Nachrichtendienste Informationen vorhanden sind. Hierzu kann die Datei solche personenbezogene Daten enthalten, die zum Auffinden der Informationen und der dazu notwendigen Identifizierung von Personen erforderlich sind. Im Falle eines Treffers wird lediglich derjenige ausländische Nachrichtendienst angezeigt, der die Daten eingegeben hat.

(4) Die Datei kann auch dem Austausch und der gemeinsamen Auswertung von Informationen und Erkenntnissen dienen, wenn dies zur Wahrung besonderer Sicherheitsinteressen (Absatz 2 Satz 2) erforderlich ist. Hierzu kann sie die zur Erforschung und Bewertung solcher Bestrebungen oder Tätigkeiten erforderlichen Daten enthalten und zu diesem Zweck genutzt werden.

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

1. Zweck der Datei,
2. Voraussetzungen der Verwendungen von Daten,
3. Prüfung und erforderlichenfalls unverzügliche Änderung, Berichtigung und Löschung von Daten,
4. Zusage,
  - a) die Daten ohne Zustimmung des eingebenden Nachrichtendienstes nicht für einen anderen Zweck als den nach Nummer 1 zu verwenden oder an Dritte zu übermitteln,
  - b) Auskunft über die Verwendung der Daten zu geben, die vom Auskunft er-bittenden Nachrichtendienst eingegeben worden sind.

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

(6) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten in der gemeinsamen Datei entsprechend § 10 Absatz 1 und 3, § 11 Absatz 1 eingeben, wenn es die Daten allen teilnehmenden ausländischen Nachrichtendiensten übermitteln darf. Für die vom Bundesamt für Verfassungsschutz eingegebenen Daten gilt für die Veränderung und Nutzung § 10 Absatz 1 und § 11 Absatz 1 und für die Überprüfung, Berichtigung, Löschung und Sperrung § 11 Absatz 2 und § 12 Absatz 1 bis 3 entsprechend. Für die Verantwortung des an der Datei teilnehmenden Nachrichtendienstes gilt § 6 Absatz 2 Satz 4 und 5 entsprechend.

(7) Das Bundesamt für Verfassungsschutz trifft für die Dateien die technischen und organisatorischen Maßnahmen nach § 9 des Bundesdatenschutzgesetzes. § 24 des Bundesdatenschutzgesetzes und § 6 Absatz 3 Satz 2 bis 5 gelten nur für die vom Bundesamt für Verfassungsschutz eingegebenen Daten sowie dessen Abrufe. Das Bundesamt für Verfassungsschutz erteilt dem Betroffenen entsprechend § 15 Auskunft nur zu den vom Bundesamt für Verfassungsschutz eingegebenen Daten.

### § 22c

#### Teilnahme an gemeinsamen Dateien mit ausländischen Nachrichtendiensten

Das Bundesamt für Verfassungsschutz darf an gemeinsamen Dateien, die von ausländischen Nachrichtendiensten errichtet sind, teilnehmen. § 22b Absatz 1 bis 4 und 6 gilt entsprechend. Dabei gilt § 22b Absatz 1 Nummer 3 mit der Maßgabe, dass verlässlich zuzusagen ist, dass

1. die vom Bundesamt für Verfassungsschutz eingegebenen Daten ohne dessen Zustimmung nicht an Dritte übermittelt werden dürfen und nur zu dem Zweck verwendet werden dürfen, zu dem sie in die Datei eingegeben wurden, und
2. das Bundesamt für Verfassungsschutz auf Ersuchen Auskunft über die vorgenommene Verwendung der Daten erhält.

Das Bundesamt für Verfassungsschutz erteilt über die von ihm eingegebenen Daten entsprechend § 15 Auskunft.“

## Artikel 2

### Änderung des BND-Gesetzes

Das BND-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch [...] geändert worden ist, wird wie folgt geändert:

1. § 2a wird wie folgt gefasst:

#### „§ 2a Besondere Auskunftsverlangen

(1) Der Bundesnachrichtendienst darf Auskünfte entsprechend den §§ 8a und 8b des Bundesverfassungsschutzgesetzes einholen, soweit dies im Einzelfall erforderlich ist

1. zur Erfüllung seiner Aufgaben nach § 1 Absatz 2 oder
2. zum Schutz seiner Mitarbeiter, Einrichtungen, Gegenstände oder Quellen gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten.

§ 8a Absatz 2 und 2a des Bundesverfassungsschutzgesetzes ist mit der Maßgabe anzuwenden, dass an die Stelle der schwerwiegenden Gefahren für die in § 3 Absatz 1 des Bundesverfassungsschutzgesetzes genannten Schutzgüter

1. im Falle des Satzes 1 Nummer 1 schwerwiegende Gefahren für die in § 5 Absatz 1 Satz 3 Nummer 1 bis 4 und 6 des Artikel 10-Gesetzes genannten Gefahrenbereiche und
  2. im Falle des Satzes 1 Nummer 2 schwerwiegende Gefahren im Sinne des § 3 Absatz 1 Nummer 2 des Bundesverfassungsschutzgesetzes
- treten. § 8b Absatz 1 bis 9 des Bundesverfassungsschutzgesetzes ist mit der Maßgabe anzuwenden, dass an die Stelle des Bundesministeriums des Innern das Bundeskanzleramt tritt.

(2) Anordnungen nach § 8a Absatz 2 und 2a des Bundesverfassungsschutzgesetzes dürfen sich nur gegen Personen richten, bei denen auf Grund tatsächlicher Anhaltspunkte davon auszugehen ist, dass sie an der Schaffung oder Aufrechterhaltung einer in Absatz 1 Satz 2 genannten Gefahr beteiligt sind, sowie gegen die in § 8a Absatz 3 Nummer 2 des Bundesverfassungsschutzgesetzes bezeichneten Personen.

(3) Das Grundrecht des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird insoweit eingeschränkt.“

2. Nach § 2b Satz 1 wird folgender Satz eingefügt:

„§ 8b Absatz 1 Satz 2 ist mit der Maßgabe anzuwenden, dass an die Stelle des Bundesministeriums des Innern das Bundeskanzleramt tritt.“

3. § 9a Absatz 4 Satz 2 wird wie folgt gefasst:

„Die Frist kann um zwei Jahre und danach um ein weiteres Jahr verlängert werden, wenn das Ziel der projektbezogenen Zusammenarbeit bei Projektende noch nicht erreicht worden ist und die Datei weiterhin für die Erreichung des Ziels erforderlich ist.“

### **Artikel 3**

#### **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. § 28 wird wie folgt geändert:

- a) Absatz 2 wird wie folgt geändert:

- aa) In Nummer 2 Buchstabe b wird das Wort „und“ durch ein Komma ersetzt,  
bb) In Nummer 3 wird der Punkt am Ende durch das Wort „und“ ersetzt.  
cc) Folgende Nummer 4 wird angefügt:

„4. der Einsatz von Polizeivollzugsbeamten unter einer ihnen auf Dauer angelegten Legende (Verdeckter Ermittler).“

- b) Nach Absatz 3 wird folgender Absatz 3a eingefügt:

„(3a) Maßnahmen nach Absatz 2 Nummer 4, die sich gegen eine bestimmte Person richten oder bei denen der Verdeckte Ermittler eine Wohnung betritt, die nicht allgemein zugänglich ist, dürfen nur durch das Gericht angeordnet werden. Bei Gefahr im Verzug dürfen Maßnahmen nach Satz 1 durch den Präsidenten des Bundespolizeipräsidiums, seinen Vertreter oder durch den Leiter einer Abteilung des Bundespolizeipräsidiums angeordnet werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit die Anordnung nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ist unter Angabe der maßgeblichen Gründe aktenkundig zu machen und auf höchstens drei Monate zu befristen. Die Verlängerung einer Maßnahme um jeweils einen Mo-

nat ist bei erneuter Anordnung durch ein Gericht möglich. Zuständig ist das Amtsgericht, in dessen Bezirk das Bundespolizeipräsidium seinen Sitz hat. Absatz 3 Satz 6 gilt entsprechend.“

c) Folgende Absätze 6 bis 9 werden angefügt:

„(6) Verdeckte Ermittler dürfen unter einer Legende

1. zur Erfüllung ihres Auftrages am Rechtsverkehr teilnehmen und
2. mit Einverständnis des Berechtigten dessen Wohnung betreten; das Einverständnis darf nicht durch ein über die Nutzung der Legende hinausgehendes Vortäuschen eines Zutrittsrechts herbeigeführt werden.

Soweit es für den Aufbau und die Aufrechterhaltung der Legende von Verdeckten Ermittlern unerlässlich ist, dürfen entsprechende Urkunden hergestellt, verändert oder gebraucht werden.

(7) Über eine Maßnahme nach Absatz 2 Nummer 4 sind zu benachrichtigen

1. die Zielperson,
2. die erheblich mitbetroffenen Personen sowie
3. die Personen, deren nicht allgemein zugängliche Wohnung der Verdeckte Ermittler betreten hat.

Die Benachrichtigung unterbleibt, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen. 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.

(8) Die Benachrichtigung über eine Maßnahme nach Absatz 2 Nummer 4 erfolgt, sobald dies möglich ist ohne Gefährdung

1. des Zwecks der Maßnahme,
2. des Bestandes des Staates,
3. von Leib, Leben oder Freiheit einer Person,
4. von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist oder

5. der Möglichkeit der weiteren Verwendung des Verdeckten Ermittlers.

Wird wegen des zugrunde liegenden Sachverhaltes ein strafrechtliches Ermittlungsverfahren geführt, erfolgt die Benachrichtigung durch die Strafverfolgungsbehörde entsprechend den Vorschriften des Strafverfahrensrechts. Wird die Benachrichtigung aus einem der vorgenannten Gründe zurückgestellt, ist dies aktenkundig zu machen.

(9) Erfolgt die nach Absatz 8 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, jedoch nicht länger als zwölf Monate. Verlängerungen der Zurückstellungsdauer sind zulässig. 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.“

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

„§ 28a

Einsatz technischer Mittel zur Eigensicherung

(1) Werden Verdeckte Ermittler im Rahmen der Gefahrenabwehr nach § 28 Absatz 2 Nummer 4 oder aus Gründen der Strafverfolgung tätig, dürfen, soweit dies zur Abwehr von Gefahren für deren Leib, Leben oder Freiheit unerlässlich ist, ohne Wissen der Betroffenen im Beisein oder in unmittelbarem zeitlichen Zusammenhang mit dem Einsatz des Verdeckten Ermittlers das innerhalb oder außerhalb einer Wohnung nicht öffentlich gesprochene Wort mit technischen Mitteln abgehört, aufgezeichnet und Lichtbilder sowie Bildaufzeichnungen hergestellt werden.

(2) Ist der Kernbereich privater Lebensgestaltung betroffen, ist die Maßnahme unverzüglich zu unterbrechen, sobald dies ohne Gefährdung des Verdeckten Ermittlers möglich ist. Bereits erfasste Daten, 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 ist aktenkundig zu machen. Diese Daten dürfen ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden. Sie sind zu lö-

schen, wenn sie für diese Zwecke nicht mehr erforderlich sind, spätestens jedoch am Ende des zweiten Kalenderjahres, das dem Jahr der Dokumentierung folgt.

(3) Maßnahmen nach Absatz 1 dürfen nur durch den Präsidenten des Bundespolizeipräsidiums, seinen Vertreter oder durch den Leiter einer Abteilung des Bundespolizeipräsidiums angeordnet werden. Bei Gefahr im Verzug dürfen Maßnahmen auch durch Beamte des höheren Dienstes des Bundespolizeipräsidiums angeordnet werden.

(4) Die Zulässigkeit der Verwendung von personenbezogenen Daten, die durch den Einsatz technischer Mittel zur Eigensicherung erlangt werden, richtet sich für Zwecke der Strafverfolgung nach § 161 Absatz 2 und 3 der Strafprozessordnung. Im Übrigen dürfen diese Daten außer für die in Absatz 1 genannten Zwecke nur zur Gefahrenabwehr verwendet werden. Wurden diese Daten in oder aus einer Wohnung erlangt, so ist die Verwendung zur Gefahrenabwehr nur zulässig nach Feststellung der Rechtmäßigkeit der Maßnahme durch das Amtsgericht, in dessen Bezirk das Bundespolizeipräsidium seinen Sitz hat; bei Gefahr im Verzug ist die gerichtliche Entscheidung unverzüglich nachzuholen.

(5) Nach Abschluss der Maßnahme sind die nach Absatz 1 hergestellten Aufzeichnungen unverzüglich zu löschen, es sei denn, sie werden für die in Absatz 4 genannten Zwecke noch benötigt. § 28 Absatz 7 bis 9 gilt entsprechend.“

3. In § 70 Satz 2 wird die Angabe „§§ 45 und 46“ durch die Angabe „§§ 28a, 45 und 46“ ersetzt.

## **Artikel 4**

### **Änderung des VIS-Zugangsgesetzes**

In § 3 Nummer 3a des VIS-Zugangsgesetzes vom 6. Mai 2009 (BGBl I S. 1034; 2013 I S. 3212), das zuletzt durch [...] geändert worden ist, wird die Angabe „§§ 89a, 89b und 91“ durch die Wörter „§§ 89a bis 89c und 91“ ersetzt.

## **Artikel 5**

### **Änderung des Artikel 10-Gesetzes**

In § 15 Absatz 6 des Artikel 10-Gesetzes vom 26. Juni 2001 (BGBl. I S. 1254, 2298), das zuletzt durch [...] geändert worden ist, werden nach Satz 2 folgende Sätze eingefügt:

„Bei Gefahr im Verzug darf am Tag der Beantragung bereits vor der Anordnung der Beschränkungsmaßnahme mit der Datenerhebung begonnen werden. Die bereits erhobenen Daten dürfen erst nach der Anordnung genutzt werden. Erfolgt die Anordnung nicht binnen 24 Stunden nach Beantragung, sind die erhobenen Daten unverzüglich automatisiert und unwiederbringlich zu löschen.“

## **Artikel 6**

### **Änderung des Vereinsgesetzes**

§ 20 Absatz 1 Satz 1 Nummer 3 des Vereinsgesetzes vom 5. August 1964 (BGBl. I S. 593), das zuletzt durch [...] geändert worden ist, wird wie folgt geändert:

1. In Nummer 3 werden nach dem Wort „Art“ die Wörter „oder deren weitere Betätigung“ eingefügt.
2. Das Wort „Gefängnis“ wird durch das Wort „Freiheitsstrafe“ ersetzt.

## **Artikel 7**

### **Änderung des Bundeskriminalamtgesetzes**

§ 9a Absatz 4 Satz 2 des Bundeskriminalamtgesetzes vom 7. Juli 1997 (BGBl. I S. 1650), das zuletzt durch [...] geändert worden ist, wird wie folgt gefasst:

„Die Frist kann um zwei Jahre und danach um ein weiteres Jahr verlängert werden, wenn das Ziel der projektbezogenen Zusammenarbeit bei Projektende noch nicht erreicht worden ist und die Datei weiterhin für die Erreichung des Ziels erforderlich ist.“

## **Artikel 8**

### **Änderung des Strafgesetzbuchs**

Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch [...] geändert worden ist, wird wie folgt geändert:

1. In § 84 Absatz 2 und § 85 Absatz 2 werden nach dem Wort „Zusammenhalt“ jeweils die Wörter „oder ihre weitere Betätigung“ eingefügt.
2. In § 129a Absatz 9 wird die Angabe „1, 2 und 4“ durch die Angabe „1, 2, 4 und 5“ ersetzt.

## **Artikel 9**

### **Änderung des Telekommunikationsgesetzes**

Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch [...] geändert worden ist, wird wie folgt geändert:

1. Nach § 95 Absatz 4 Satz 1 wird folgender Satz eingefügt:  
„Die Pflicht nach § 111 Absatz 1 Satz 3 bleibt unberührt.“
2. § 111 wird wie folgt gefasst:

#### **„§ 111**

##### **Daten für Auskunftersuchen der Sicherheitsbehörden**

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113

1. die Rufnummern und anderen Anschlusskennungen,
2. den Namen und die Anschrift des Anschlussinhabers,
3. bei natürlichen Personen deren Geburtsdatum,
4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,

5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie
6. das Datum des Vertragsbeginns

vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse (§ 104) eingetragen werden. Bei im Voraus bezahlten Mobilfunkdiensten ist die Richtigkeit der nach Satz 1 erhobenen Daten vor der Freischaltung zu überprüfen durch

1. Vorlage eines Ausweises im Sinne des § 2 Absatz 1 des Personalausweisgesetzes,
2. Vorlage eines Passes im Sinne des § 1 Absatz 2 des Passgesetzes,
3. Vorlage eines sonstigen gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, wozu insbesondere auch ein nach ausländerrechtlichen Bestimmungen anerkannter oder zugelassener Pass, Personalausweis oder Pass- oder Ausweisersatz zählt,
4. Vorlage eines Aufenthaltstitels,
5. Vorlage eines Ankunftsnachweises nach § 63a Absatz 1 des Asylgesetzes oder einer Bescheinigung über die Aufenthaltsgestattung nach § 63 Absatz 1 des Asylgesetzes,
6. Vorlage einer Bescheinigung über die Aussetzung der Abschiebung nach § 60a Absatz 4 des Aufenthaltsgesetzes, oder
7. Vorlage eines Auszugs aus dem Handels- oder Genossenschaftsregister oder einem vergleichbaren amtlichen Register oder Verzeichnis, der Gründungsdokumente oder gleichwertiger beweiskräftiger Dokumente oder durch Einsichtnahme in diese Register oder Verzeichnisse und Abgleich mit den darin enthaltenen Daten, sofern es sich bei dem Anschlussinhaber um eine juristische Person oder Personengesellschaft handelt,

soweit die Daten in den vorgelegten Dokumenten oder eingesehenen Registern oder Verzeichnissen enthalten sind. Die Überprüfung kann auch durch andere geeignete Verfahren erfolgen; die Bundesnetzagentur legt nach Anhörung der betroffenen Kreise durch Verfügung im Amtsblatt fest, welche anderen Verfahren

zur Überprüfung geeignet sind, wobei jeweils zum Zwecke der Identifikation vor Freischaltung der vertraglich vereinbarten Mobilfunkdienstleistung ein Dokument im Sinne des Satzes 3 genutzt werden muss. Bei der Überprüfung ist die Art des eingesetzten Verfahrens zu speichern; bei Überprüfung mittels eines Dokumentes im Sinne des Satzes 3 Nummer 1 bis 6 sind ferner Angaben zu Art, Nummer und ausstellender Stelle zu speichern. Für die Identifizierung anhand eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes gilt § 8 Absatz 1 Satz 6 des Geldwäschegesetzes entsprechend. Für das Auskunftsverfahren nach § 113 ist die Form der Datenspeicherung freigestellt.

(2) Die Verpflichtung zur unverzüglichen Speicherung nach Absatz 1 Satz 1 gilt hinsichtlich der Daten nach Absatz 1 Satz 1 Nummer 1 und 2 entsprechend für denjenigen, der geschäftsmäßig einen öffentlich zugänglichen Dienst der elektronischen Post erbringt und dabei Daten nach Absatz 1 Satz 1 Nummer 1 und 2 erhebt, wobei an die Stelle der Daten nach Absatz 1 Satz 1 Nummer 1 die Kennungen der elektronischen Postfächer und an die Stelle des Anschlussinhabers nach Absatz 1 Satz 1 Nummer 2 der Inhaber des elektronischen Postfachs tritt.

(3) Wird dem Verpflichteten nach Absatz 1 Satz 1 oder Absatz 2 eine Änderung bekannt, hat er die Daten unverzüglich zu berichtigen. In diesem Zusammenhang hat der nach Absatz 1 Satz 1 Verpflichtete bisher noch nicht erhobene Daten zu erheben und zu speichern, sofern ihm eine Erhebung der Daten ohne besonderen Aufwand möglich ist.

(4) Bedient sich ein Diensteanbieter zur Erhebung der Daten nach Absatz 1 Satz 1 und Absatz 2 eines Dritten, bleibt er für die Erfüllung der Pflichten nach Absatz 1 Satz 1 und Absatz 2 verantwortlich. Werden dem Dritten im Rahmen des üblichen Geschäftsablaufes Änderungen der Daten nach Absatz 1 Satz 1 und Absatz 2 bekannt, hat er diese dem Diensteanbieter unverzüglich zu übermitteln.

(5) Die Daten nach den Absätzen 1 und 2 sind mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen.

(6) Eine Entschädigung für die Datenerhebung und -speicherung wird nicht gewährt.“

3. § 112 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

- aa) In Satz 1 werden die Wörter „§ 111 Abs. 1 Satz 1, 3 und 4 und Abs. 2“ durch die Wörter „§ 111 Absatz 1 Satz 1, Absatz 2, 3 und 4“ ersetzt.
  - bb) In Satz 3 werden die Wörter „§111 Abs. 1 Satz 4 und Abs. 4“ durch die Wörter „§ 111 Absatz 3 und 5“ ersetzt.
- b) In Absatz 3 Satz 1 Nummer 4 wird die Angabe „§ 111 Abs. 1 Satz 5“ durch die Wörter „§ 111 Absatz 1 Satz 7“ ersetzt.
4. § 115 Absatz 2 wird wie folgt geändert:
- a) In Satz 1 Nummer 3 werden die Wörter „nach § 111 Abs. 1, 2 und 4“ durch die Wörter „nach § 111 Absatz 1, 4 und 5“ ersetzt.
  - b) In Satz 2 werden die Wörter „gegen § 111 Abs. 1, 2 oder Abs. 4“ durch die Wörter „gegen § 111 Absatz 1 bis 5“ ersetzt.
5. § 149 Absatz 1 Nummer 29 bis 30a wird wie folgt gefasst:
- „29. entgegen § 111 Absatz 1 Satz 1, auch in Verbindung mit Absatz 1 Satz 2 oder Absatz 2, oder entgegen § 111 Absatz 1 Satz 3 oder 5 oder Absatz 3 dort genannte Daten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erhebt, nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig speichert oder nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig berichtet oder die Richtigkeit dort genannter Daten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig überprüft.
  - 30. entgegen § 111 Absatz 4 Satz 2 eine Änderung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,
  - 30a. entgegen § 111 Absatz 5 Daten nicht oder nicht rechtzeitig löscht,“
6. Dem § 150 werden die folgenden Absätze 14 und 15 angefügt:
- „(14) Für Vertragsverhältnisse, die am 22. Juni 2004 bereits bestanden, müssen Daten nach § 111 Absatz 1 Satz 1 oder Absatz 2 außer in Fällen des § 111 Absatzes 3 nicht nachträglich erhoben werden.
- (15) Die Bundesnetzagentur veröffentlicht die Verfügung nach § 111 Absatz 1 Satz 4 spätestens am ... [einsetzen: Datum des ersten Tages des sechsten auf die Verkündung des Gesetzes folgenden Monats] im Amtsblatt. Die Pflichten zur

Überprüfung der Richtigkeit der erhobenen Daten nach § 111 Absatz 1 Satz 3 und zur Speicherung der Angaben nach § 111 Absatz 1 Satz 5 sind spätestens ab dem ... [einsetzen: Datum des ersten Tages des achtzehnten auf die Verkündung des Gesetzes folgenden Monats] zu erfüllen.“

## **Artikel 10**

### **Einschränkung eines Grundrechts**

Das Grundrecht des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird nach Maßgabe des Artikels 5 eingeschränkt.

## **Artikel 11**

### **Inkrafttreten**

Dieses Gesetz tritt vorbehaltlich des Satzes 2 am Tag nach der Verkündung in Kraft. Artikel 4 tritt am ...[einsetzen: Datum des ersten Werktages, der kein Samstag ist, des vierten auf die Verkündung folgenden Kalendermonats] in Kraft.

## **Begründung**

### **A. Allgemeiner Teil**

#### **I. Ziel des Gesetzes**

Die jüngsten jihadistischen Anschläge in Europa – am 13. November 2015 in Paris und am 22. März 2016 in Brüssel – haben in Anschlagplanung und -ausführung die transnationale Dimension der terroristischen Bedrohung nochmals unterstrichen. Diese Gefährdungslage gebietet zum gebotenen Schutz der Menschen vor terroristischen Anschlägen dringend eine verbesserte Zusammenarbeit der Sicherheitsbehörden bei der Zusammenführung und Auswertung von Informationen.

Hierzu ist bereits im Vorfeld polizeilicher Maßnahmen eine verbesserte internationale nachrichtendienstliche Zusammenarbeit geboten. In Europa ist dazu die Counter Terrorism Group (CTG) als informeller Zusammenschluss von 30 Nachrichtendiensten eingerichtet. Vertreten sind die Inlandsdienste aller EU-Staaten sowie von Norwegen und der Schweiz. Sie richtet aktuell eine operative „Plattform“ ein. Verbindungsbeamte der CTG-Dienste arbeiten dort zum vereinfachten und beschleunigten Austausch von Erkenntnissen über den islamistischen Terrorismus zusammen. Technisch unterstützt werden soll die Zusammenarbeit auch durch eine gemeinsame Datei. Eine solche Datei könnte derzeit in Deutschland beim Bundesamt für Verfassungsschutz (BfV) nicht geführt werden, da es bislang rechtlich gehindert ist, ausländischen Nachrichtendiensten einen automatisierten Abruf darauf einzurichten. Der Gesetzentwurf soll insoweit die Kooperationsfähigkeit Deutschlands in einem internationalen Analyseverbund zum Schutz der Freiheit und Sicherheit der Menschen verbessern.

Deutschland ist bevorzugtes Ziel- und Transitland illegaler Migration. Schleusernetzwerke sind arbeitsteilig, international organisiert und agieren hoch konspirativ. Gefahren für Leib und Leben der Geschleusten bis hin zum Tod werden teilweise billigend in Kauf genommen, wie der Fund von 71 Leichen in einem Kühllastwagen auf einer österreichischen Autobahn am 27. August 2015 deutlich beweist.

Insbesondere die Schleusungskriminalität ist als Teil der Organisierten Kriminalität zunehmend von einer starken Abschottung und von einem konspirativen Täterverhalten geprägt. Strukturelle Erkenntnisse zu Schleuserorganisationen und valide Informationen zur Verhinderung von menschenverachtenden und teilweise tödlichen Schleusungen sind häufig nur durch verdeckte personelle Maßnahmen im Vorfeld oder in den Strukturen der Organisierten Kriminalität zu gewinnen.

## **II. Wesentlicher Inhalt**

Der Gesetzentwurf enthält spezielle Rechtsgrundlagen für gemeinsame Dateien von BfV mit wichtigen ausländischen Partnerdiensten, insbesondere der Nachbarstaaten und anderer EU- bzw. NATO-Mitgliedstaaten.

Zudem wird bereits national die technische Unterstützung der Informationszusammenführung und -pflege fortentwickelt, indem Projektdaten mit polizeilichen und nachrichtendienstlichen Teilnehmern etwas länger eingerichtet werden können.

Schließlich erfolgen ergänzend abrundende Regelungen zu den Befugnissen der Bundespolizei (präventiver Einsatz Verdeckter Ermittler) und zur Dokumentation der Identität der Nutzer von im Voraus bezahlten Mobilfunkdiensten. Im Übrigen wird eine im VIS-Zugangsgesetz durch überschneidende Gesetzgebungsverfahren versehentlich entstandene Lücke geschlossen.

Zudem werden Strafbarkeitslücken, die bei der Unterstützung der Weiterbetätigung verbotener Vereinigungen bestehen, geschlossen.

## **III. Alternativen, Folgen und Auswirkungen**

### **1. Alternativen**

Keine.

### **2. Folgen und Auswirkungen**

Die Regelungen tragen zum besseren Schutz herausragender öffentlicher Interessen bei.

### **3. Gleichstellungspolitische Gesetzesfolgenabschätzung**

Der Gesetzentwurf hat keine gleichstellungspolitischen Folgen.

## **IV. Gesetzgebungskompetenz des Bundes**

Die Gesetzgebungskompetenz des Bundes für die Änderungen des Bundesverfassungsschutzgesetzes ergibt sich aus Artikel 73 Absatz 1 Nummer 10 Buchstabe b des Grundgesetzes (GG), zur Änderung des BND-Gesetzes aus Artikel 73 Absatz 1 Nummer 1 GG und zur Änderungen des Artikel 10-Gesetzes (G 10) aus Artikel 73 Absatz 1 Nummer 1 und 10 Buchstabe b GG. Sie ergibt sich für die Änderung des Bundespolizeigesetzes aus Artikel 73 Absatz 1 Nummer 5 GG und für die Änderung des VIS-Zugangsgesetzes aus Artikel 73 Absatz 1 Nummer 10 GG (internationale Verbrechensbekämpfung). Die Kompetenz des Bundes zur Änderung des Bundes-

kriminalamtgesetzes folgt aus Artikel 73 Absatz 1 Nummer 10 GG (internationale Verbrechensbekämpfung) sowie Artikel 73 Absatz 1 Nummer 10 Buchstabe a und Buchstabe c GG. Für die Änderung des Strafgesetzbuchs und die Änderung der Strafvorschrift des Vereinsgesetzes beruht die Gesetzgebungskompetenz des Bundes auf Artikel 74 Absatz 1 Nummer 1 GG (Strafrecht). Zur Änderung des Telekommunikationsgesetzes folgt die Gesetzgebungskompetenz des Bundes aus Artikel 73 Absatz 1 Nummer 7 GG (Telekommunikation).

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

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

## **VI. Erfüllungsaufwand**

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

Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

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

Durch die in Artikel 9 vorgenommene Änderung des Telekommunikationsgesetzes (TKG) werden die Erbringer von geschäftsmäßigen Telekommunikationsdiensten sowie daran Mitwirkende verpflichtet, Bestandsdaten der Anschlussinhaber bei im Voraus bezahlten Mobilfunkdiensten auf ihre Richtigkeit hin zu überprüfen. Durch diese Verpflichtung ist eine dauerhafte, zusätzliche Belastung der Telekommunikationsdiensteanbieter zu erwarten, die sich derzeit nicht ermitteln lässt. Eine solche detaillierte Bewertung kann gegebenenfalls erst nach Inkrafttreten der gesetzlichen Regelung und Festlegung der geeigneten Verfahren für die Überprüfung der Angaben nach § 111 Absatz 1 Satz 1 TKG durch die Bundesnetzagentur vorgenommen werden. Eine erste Nacherfassung erfolgt vor Abschluss der parlamentarischen Befassung.

Weitere Belastungen für die Wirtschaft entstehen nicht.

### **3. Erfüllungsaufwand für die Verwaltung**

Mit der Einführung gemeinsamer Dateien mit ausländischen Partnerdiensten entsteht dem BfV ein Mehrbedarf in Höhe von 27 (Plan-) Stellen (3 Stellen höherer Dienst, 13

Stellen gehobener Dienst, 11 Stellen mittlerer Dienst). Die damit verbundenen Personal- und Personalsachkosten betragen insgesamt rund 2,3 Millionen Euro. Der Aufwand berücksichtigt neben dem federführenden Betrieb einer gemeinsamen Datei durch das BfV auch die Bearbeitung der in diesem Zusammenhang erforderlichen nationalen und internationalen Grundsatz- und Rechtsfragen. Darüber hinaus schließt der Personalbedarf die Konzeption, die Entwicklung, die Installation und den Betrieb der IT-Infrastruktur ein. Für die technische Realisierung (Verfahrensentwicklung und Schaffung der Infrastruktur) einer solchen Datei sind darüber hinaus einmalige Sachkosten in Höhe von rund 2,9 Millionen Euro sowie jährlich laufende Kosten von 575 000 Euro zu erwarten. Bei der Einrichtung weiterer gemeinsamer Dateien durch das BfV oder bei Teilnahme des BfV an von anderen Stellen betriebenen gemeinsamen Dateien werden weitere Kosten in jedoch geringerem Umfang anfallen.

Mit der Änderung des Bundespolizeigesetzes entsteht ein Mehrbedarf an Personal- und Sachmitteln bei der Bundespolizei. Der Bedarf beläuft sich auf zwölf (Plan-) Stellen (1 Stelle höherer Dienst, 11 Stellen gehobener Dienst) und damit verbundenen rund 780 000 Euro jährlichen Personal- und Personalnebenkosten sowie rund 600 000 Euro jährliche Sachkosten. Zudem sind einmalig ca. 700 000 Euro für Sachmittel erforderlich.

Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen soll finanziell und stellenmäßig im jeweiligen Einzelplan eingespart werden.

Weiterer Aufwand für die Verwaltung der Länder und Kommunen entsteht nicht.

## **VII. Sonstige Kosten**

Sonstige Kosten sind nicht zu erwarten.

## **VIII. Weitere Gesetzesfolgen**

Auswirkungen auf demographierelevante Belange sind nicht zu erwarten. Nachhaltigkeitsbezogen ist eine weiter verbesserte Verhütung insbesondere terroristischer Straftaten zu erwarten.

## **IX. Evaluierung**

Die Artikel 1 und 3 sowie gegebenenfalls 9 werden spätestens fünf Jahre nach Inkrafttreten evaluiert. Dabei ist zu untersuchen, wie sich der Erfüllungsaufwand entwickelt hat und ob die Entwicklung in einem angemessenen Verhältnis zu den festgestellten Regelungswirkungen steht.

### **B. Besonderer Teil**

#### **Zu Artikel 1 (Änderung des Bundesverfassungsschutzgesetzes)**

##### **Zu Nummer 1 (§ 22a BVerfSchG)**

Mit der Änderung wird die Höchstdauer einer gemeinsamen Projektdatei um ein Jahr auf dann maximal fünf Jahre verlängert. Die allgemeinen Voraussetzungen der gemeinsamen Datenhaltung nach Absatz 2 bleiben davon unberührt. Danach schafft § 22a keine originäre Befugnis zur Dateneingabe, sondern lässt sie nur nach Maßgabe der bestehenden Übermittlungs- und Speicherungsbefugnisse zu. Die Änderung des § 22a erweitert mithin nicht die Befugnisse zum Datenaustausch zwischen den beteiligten Behörden, sondern bezweckt vornehmlich eine technisch vereinfachte Durchführung, die insbesondere auch die Datenpflege erleichtert, dies auch im Interesse Betroffener.

##### **Zu Nummer 2 (§§ 22b und c BVerfSchG)**

###### **Zu § 22b**

§ 22b BVerfSchG schafft eine spezielle Rechtsgrundlage für die Errichtung von gemeinsamen Dateien unter Federführung des BfV mit ausländischen öffentlichen Stellen, die mit nachrichtendienstlichen Aufgaben betraut sind.

In vielen Bereichen ist das BfV zur Erfüllung seiner Aufgaben nach § 3 des Bundesverfassungsschutzgesetzes (BVerfSchG) auf die Kooperation mit ausländischen Nachrichtendiensten angewiesen. Insbesondere mit Partnerdiensten in den Nachbarstaaten und darüber hinaus in der EU und der NATO besteht ein besonderes Zusammenarbeitsbedürfnis und damit auch die Notwendigkeit, relevante Informationen zeitnah zu teilen. Dies gilt gerade auch für den Bereich der Terrorismusbekämpfung.

Bei der Terrorismusabwehr muss beispielsweise besonderes Augenmerk jihadistischen Rückkehrern aus der Krisenregion Syrien/Irak gelten, die aus ihrem dortigen Aufenthalt regelmäßig über eine Vielzahl von Kennbeziehungen verfügen, aus denen nach Rückkehr transnationale Netzwerke in Europa entstehen können, zu deren Aufklärung intensive Zusammenarbeit der befassten Nachrichtendienste geboten ist.

Neben dauerhaft eingerichteten Dateien zur kontinuierlichen Aufklärung gemeinsamer Beobachtungsobjekte werden gegebenenfalls auch gemeinsame Dateien für spezielle Projekte benötigt, etwa zur Aufklärung staatsübergreifend erfolgter elektronischer Angriffe einer fremden Macht.

### **Zu Absatz 1**

Absatz 1 regelt die grundlegenden Voraussetzungen einer Kooperation mit gemeinsamer Datenhaltung. Die bestimmten Bestrebungen oder Tätigkeiten, deren Aufklärung die Datei dient, sind zwischen den teilnehmenden Stellen gemäß Absatz 5 mit der Zweckfestlegung klar zu definieren. Die Beschränkung auf „bestimmte Ereignisse oder Personenkreise“ schließt aus, eine gemeinsame Datei über die gesamte Aufgabenbreite des BfV – gleichermaßen als internationales NADIS – einzurichten. Aufgeklärt werden können hingegen bestimmte Phänomene, etwa jihadistische Bestrebungen mit den zugehörigen Personenzusammenschlüssen oder die Reisen von „Foreign Terrorist Fighters“ und deren weitere Beteiligung an salafistischen Bestrebungen in ihren Heimatstaaten nach Rückkehr aus den Krisenregionen. Ebenso kommen bestimmte Vorgänge bzw. Ereignisse, etwa bestimmte elektronische Angriffe, als gemeinsamer Aufklärungsgenstand in Betracht. Gemeinsam ist immer die Eingrenzung über bestimmte phänomenologische Sachverhalte/Ereignisse bzw. Personenzusammenschlüsse.

Das Erfordernis erheblicher Sicherheitsinteressen (Nummer 1) greift die Schwelle des § 19 Absatz 3 Satz 1 BVerfSchG bei Übermittlungen für Empfängeraufgaben auf. Die Datei dient zwar ebenso der Information der anderen Teilnehmer, dass die Person für das BfV von Interesse ist, und damit – gleichsam als Dauerübermittlungsersuchen – der Gewinnung weiterer Informationen zu dieser Person. Gleichwohl erscheint für diese technisch unterstützte Form informationeller Zusammenarbeit die besondere Schwelle erheblicher Sicherheitsinteressen als generelle Voraussetzung angemessen.

Ebenfalls an dem Grundmodell der Übermittlungsvoraussetzungen ist Nummer 2 orientiert. Das Grundgesetz ist programmatisch auf internationale Zusammenarbeit ausgerichtet und respektiert die Verschiedenartigkeiten der Rechtsordnungen grundsätzlich, setzt der Zusammenarbeit zugleich aber auch Grenzen, wenn eine Verletzung elementarer rechtsstaatlicher Grundsätze zu befürchten ist. Demgemäß ist Voraussetzung, dass ein hinreichend rechtsstaatlicher Umgang mit den vom BfV in die Datei eingestellten Daten im Teilnehmerstaat zu erwarten ist (BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 - Rn. 324 ff.). Dem kommt speziell bei der Teilnahme von Drittstaaten (Absatz 2) besondere Bedeutung zu.

Die Festlegungen nach Absatz 5 haben grundlegende Bedeutung für die Zusammenarbeit und müssen danach effektiv gewährleistet sein. Demgemäß müssen diese Zusagen auch verlässlich sein (Nummer 3). Anders als bei den institutionellen Partnern aus EU und NATO, bei denen das Vertrauen in die Zuverlässigkeit von Zusicherungen grundsätzlich begründet ist, muss dies in Bezug auf die Drittstaaten, zu denen auch im Übrigen qualifizierte Voraussetzungen gelten (Absatz 2), konkret gewürdigt werden. Grundlage dafür sind typischerweise gefestigte Zusammenarbeitserfahrungen.

Fallen Einrichtungsvoraussetzungen nachträglich fort, dann ist die Datei bzw., wenn nur einzelne Teilnehmer (verlässlichkeitsbezogen) betroffen sind, deren Teilnahme zu beenden.

### **Zu Absatz 2**

Absatz 2 regelt qualifizierte materielle und verfahrensmäßige Voraussetzungen für gemeinsame Dateien außerhalb der institutionell oder nachbarschaftlich verfestigten Zusammenarbeitsbeziehungen. Sie ist nur zur Aufklärung besonders gefährlicher Bestrebungen oder Tätigkeiten zulässig, die nämlich auf die Begehung schwerwiegender Straftaten gerichtet sind. Satz 3 definiert dies mit den Staatsschutzdelikten des § 3 Absatz 1 des Artikel 10-Gesetzes (G 10). Gemäß der internationalen Ausrichtung der Zusammenarbeit sind die entsprechenden Delikte im nationalen Recht der Partnerbehörden einbezogen und bei Staatsschutzdelikten auch entsprechende Taten zu Lasten internationaler Organisationen, denen Deutschland angehört, also etwa Angriffe gegen die EU, die NATO oder die Vereinten Nationen.

Gerade in diesen Zusammenarbeitsfällen kommt den Garantien nach Absatz 5 besondere Bedeutung zu.

Zudem kann bei solcher Kooperation mit Drittstaaten neben der abstrakten Datenschutzgewährleistung bei der Dateieinrichtung auch den Voraussetzungen der einzelnen Dateneingabe nach Absatz 6 – im Hinblick auf womöglich entgegenstehende überwiegende schutzwürdige Interessen des Betroffenen – spezielle Bedeutung zukommen.

### **Zu Absatz 3**

Absatz 3 regelt die Basisnutzung als bloße Indexdatei, die lediglich der verbesserten Kontakthanbahnung – zum nachfolgend gezielten Informationsaustausch außerhalb der Datei – dient und in Datenkranz und Nutzung entsprechend beschränkt ist.

#### **Zu Absatz 4**

Die analytische Nutzung nach Absatz 4 ist von höherer Praxisbedeutung wegen des höheren Eingriffsgewichts aber an qualifizierte Voraussetzungen (besondere Sicherheitsinteressen) gebunden.

#### **Zu Absatz 5**

Der Zweck der Datei sowie die Einzelheiten der gemeinsamen Datenhaltung und Datenverwendung sind gemäß Absatz 5 vorab zwischen den teilnehmenden Staaten in einer schriftlichen Erklärung niederzulegen. Im Interesse der Kooperationsoffenheit trifft das Gesetz keine einseitigen Vorgaben zur Formenwahl (etwa als völkerrechtlicher Vertrag). Erforderlich ist aber eine effektive Bindung, die durch verbindliche Zusicherung begründet wird, da das Vertrauen in die Beachtung getroffener Absprachen für nachrichtendienstliche Zusammenarbeit grundlegend ist und ein Verstoß danach gravierende Zusammenarbeitsfolgen – gegebenenfalls über den Ausschluss aus der gemeinsamen Datei hinaus – hätte. Ist dagegen trotz Zusicherung – mangels Verlässlichkeit des Partners – deren tatsächliche Beachtung nicht gewährleistet, scheidet eine Beteiligung dieser Behörde aus (Absatz 1 Nummer 3).

Die Festlegungen müssen insbesondere Garantien zum angemessenen Datenschutz enthalten, entsprechend sind insbesondere angemessene Regelungen zu Eingabe bzw. Speicherung und Abruf bzw. Nutzung sowie zur Löschung von Daten zu treffen, ferner Vorgaben zur Datenpflege, also zur Prüfung, ob Daten zu ändern, zu berichtigen oder löschen sind. Dies fordert keinen der deutschen Rechtsordnung gleichartigen Schutz (denn das Grundgesetz anerkennt die Eigenständigkeit und Verschiedenartigkeit der Rechtsordnungen und respektiert sie grundsätzlich auch im Rahmen des Austauschs von Daten), die Zusicherungen müssen aber sicherstellen, dass der Datenumgang durch die Partnerdienste nicht elementare Anforderungen des menschenrechtlichen Schutzes personenbezogener Daten unterlaufen.

Verbindlich zuzusichern ist dabei auch, die Daten nur zu dem Zweck zu verwenden, zu dem sie in die gemeinsamen Dateien eingestellt wurden. Darüber hinaus müssen die teilnehmenden Stellen sich verpflichten, die eingestellten Daten nicht ohne Zustimmung der eingebenden Stelle an Dritte zu übermitteln. Zudem ist eine Auskunftsregelung vorzusehen, auf deren Grundlage das BfV die Einhaltung der Erklärung in Bezug auf die von ihm eingegebenen Daten begleiten und kontrollieren kann.

Mit der Bindung an den Zweck einer Sachverhaltserforschung, flankiert vom Weitergabeverbot, wird der Eingriffsgehalt der Zusammenarbeit auf die analytische Verwendung der personenbezogenen Daten im Teilnehmerkreis beschränkt. Allerdings können die aus den Informationen gewonnenen Erkenntnisse womöglich auch Fol-

maßnahmen anstoßen. Um auch insofern jedweder Besorgnis etwaiger Verletzungen elementarer menschenrechtlicher oder rechtsstaatlicher Grundsätze vorzubeugen, beschränkt sich das Gesetz nicht darauf, dass mit den Festlegungen ein angemessener Datenschutz zu gewährleisten ist, sondern verlangt ebenso, auch in anderer Hinsicht unangemessene Verwendungen nötigenfalls auszuschließen. Dies betrifft nicht eine gemeinsame Datei mit dem Nachbarstaat Schweiz zur gemeinsamen Aufklärung grenzüberschreitender rechtsextremistischer Verbindungen (spezielle Festlegungen zu rechtsstaatlichen Prinzipien würden bei solcher Zusammenarbeit eher diplomatisch provokativ wirken), kann aber in anderen Zusammenhängen zur verlässlichen Absicherung auch gegen Resteventualitäten angezeigt sein. Beschränkungen von Folgeverwendungen – insbesondere zum Ausschluss der Todesstrafe – entsprechen auch bereits der deutschen Staatspraxis in der internationalen Zusammenarbeit.

Flankierend zur Festlegung zwischen den internationalen Teilnehmern ist für das BfV eine Dateianordnung entsprechend § 14 zu erstellen. Die gemeinsame schriftliche Erklärung nach Satz 1 ist der Dateianordnung beizufügen, da das Gesamtregelwerk der Datei einerseits aus den international getroffenen Regelungen und andererseits den nationalen Festlegungen der Dateianordnung besteht.

### **Zu Absatz 6**

Absatz 6 regelt, unter welchen Voraussetzungen das BfV personenbezogene Daten eingeben und verwenden darf, ferner deren Datenpflege, etwa mit Prüffristen zur weiteren Speichererforderlichkeit. Dabei werden die Voraussetzungen zur nationalen Speicherung und zur Auslandsübermittlung kombiniert. Demgemäß muss eine Eingabe insbesondere unterbleiben, wenn auswärtige Belange der Bundesrepublik Deutschland oder überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen (§ 19 Absatz 3), wobei diese Interessenabwägung mit den – erheblichen – Sicherheitsinteressen zu erfolgen hat, zu deren Wahrung die Datei errichtet ist. Unberührt bleiben dabei auch besondere Zweckbindungen, wie insbesondere § 4 Absatz 4 G 10. Allerdings sind Analysedateien nach § 22b Absatz 4 von vornherein auf die Aufklärung von Bestrebungen oder Tätigkeiten bezogen, bei denen zumindest der Verdacht besteht, dass sie ihre Ziele mit der Begehung der in § 3 Absatz 1 G 10 genannten Straftaten verfolgen.

Jede Stelle trägt die Verantwortung für die von ihr eingegebenen Daten. Für die an der Datei teilnehmenden ausländischen öffentlichen Stellen gilt das jeweils anwendbare nationale Recht der ausländischen öffentlichen Stelle. Für die ausländischen Stellen folgt dies unmittelbar aus ihrem Recht, ohne dass es dazu eines Anwendungsbefehls durch deutsche Gesetzgebung bedürfte. Unabhängig von diesem aus-

ländischen Recht wird mit den Festlegungen nach Absatz 5 ein angemessener Datenschutz gewährleistet.

### **Zu Absatz 7**

Die Regelung stellt zu den technischen und organisatorischen Datenschutzmaßnahmen die Verantwortung des BfV, bei dem die Datei errichtet ist, klar. Kontroll- und Auskunftsrechte beschränken sich auf den Verantwortungsbereich des BfV. Die Auskunft bezieht sich nicht darauf, in welcher Datei die Daten gespeichert sind. Dies ist schon allgemein nicht Gegenstand des § 15 und würde vorliegend speziell § 15 Absatz 3 widersprechen.

### **Zu § 22c**

§ 22c regelt die Teilnahme des BfV an Dateien ausländischer öffentlicher Stellen, die mit nachrichtendienstlichen Aufgaben betraut sind. Insoweit geht es zwar nicht darum, dass das BfV anderen Stellen zu einer eigenen Datei automatisierten Abruf einräumt, gleichwohl erscheint eine dem § 22b entsprechende Regelung angemessen, wenn der Inlandsdienst sich im Ausland an gemeinsamer Datenhaltung beteiligt. Die Vorgaben beziehen sich dabei allein auf das BfV und die von ihm eingegebenen Daten. Ob der federführende ausländische Nachrichtendienst seinerseits eine Dateianordnung erstellt und Festlegungen zwischen den Partnern abspricht, bleibt ihm überlassen. Für die vom BfV eingegebenen Daten müssen aber die Zusagen entsprechend Absatz 5 Satz 1 Nummer 4 erfolgen (vergleiche § 19 Absatz 3 Satz 4 BVerfSchG).

## **Zu Artikel 2 (Änderung des BND-Gesetzes)**

### **Zu Nummer 1 (§ 2a BNDG)**

Mit der Regelung wird der bisherige Wertungswiderspruch ausgeräumt, dass der Bundesnachrichtendienst (BND) zwar gemäß § 3 Absatz 1 Satz 1 Nummer 3 G10 zur Abwehr sicherheitsgefährdender oder geheimdienstlicher Angriffe Beschränkungen nach dem Artikel 10-Gesetz beantragen kann, jedoch nicht zu demselben Zweck das deutlich mildere Eingriffsmittel nach § 2a BNDG einsetzen darf. Die Ergänzung dient auch dazu, einen Gleichklang der Befugnisse von BND und BfV herzustellen.

### **Zu Nummer 2 (§ 2b BNDG)**

Zwischen den besonderen Auskunftsverlangen nach den §§ 2b bzw. 2a BNDG besteht eine formale Diskrepanz. Der nachträglich eingefügte § 2b BNDG sieht (in Verbindung mit § 8d Absatz 1 Satz 2 BVerfSchG) für Anträge des BND eine Anordnung durch das Bundesministerium des Innern vor, während bei besonderen Auskunftsver-

langen nach § 2a BNDG für den Erlass der Anordnung an Stelle des Bundesministerium des Innern das Bundeskanzleramt tritt (§ 2a Satz 4 BNDG). Die Änderung dient der Vereinheitlichung des Anordnungsverfahrens.

### **Zu Nummer 3 (§ 9a Absatz 4 Satz 1 BNDG)**

Die Änderung setzt die Änderung des Artikels 1 Nummer 1 auch im BND-Gesetz um.

## **Zu Artikel 3 (Änderung des Bundespolizeigesetzes)**

### **Zu Nummer 1 (§ 28 BPolG)**

#### **Zu Buchstabe a (§ 28 Absatz 2 BPolG)**

Die Bundespolizei erhält mit der Einfügung der Nummer 4 in § 28 Absatz 2 wie nahezu alle Polizeien der Länder und das Bundeskriminalamt die Befugnis, Verdeckte Ermittler im Rahmen ihrer Zuständigkeit bereits zur Gefahrenabwehr und nicht erst zur Strafverfolgung einzusetzen. Nach der neuen Regelung ist der Einsatz von Polizeivollzugsbeamten unter einer auf Dauer angelegten Legende (Verdeckter Ermittler) zum Zweck der Gefahrenabwehr möglich. Aufgrund der oftmals abgeschotteten Strukturen im Bereich der Schleusungskriminalität ist der Einsatz eines präventiven Verdeckten Ermittlers insbesondere für die Abwehr daraus resultierender Gefahren ein hilfreiches Instrument.

#### **Zu Buchstabe b (§ 28 Absatz 3a BPolG)**

Der neue Absatz 3a trägt dem Erfordernis nach besonderen verfahrensrechtlichen Vorkehrungen Rechnung (so auch BVerfG, Urteil vom 20. April 2016 - 1BvR 966/09 u.a.). Aufgrund der Eingriffsintensität des Einsatzes des Verdeckten Ermittlers darf eine solche Maßnahme, wenn sie sich gegen eine bestimmte Person richtet oder wenn der Verdeckte Ermittler eine Wohnung betritt, nur durch das Gericht angeordnet werden. Somit orientiert sich die Regelung auch an dem Anforderungsniveau für den Einsatz des Verdeckten Ermittlers zum Zwecke der Strafverfolgung nach § 110b Absatz 2 der Strafprozessordnung.

Die Anordnungsbefugnisse bei Gefahr im Verzug obliegen dem Präsidenten des Bundespolizeipräsidiums, seinem Vertreter oder einem Leiter einer Abteilung des Bundespolizeipräsidiums.

Eine Befristung der Einsätze ist aus rechtsstaatlicher Sicht geboten. Im repressiven Bereich erfolgen erfahrungsgemäß vergleichbare Befristungen der Staatsanwaltschaften regelmäßig für einen Zeitraum von bis zu drei Monaten. Der Einsatz eines präventiven Verdeckten Ermittlers setzt den Aufbau einer Vertrauensbasis in der kri-

minellen Szene voraus und erfordert intensive Vorbereitungsmaßnahmen. Dafür ist gerade bei der Erstanordnung ein längerer Zeitraum als ein Monat notwendig.

### **Zu Buchstabe c (§ 28 Absatz 6 bis 9 BPolG)**

#### **Zu Absatz 6**

Die Regelung stellt klar, welche Befugnisse der präventive Verdeckte Ermittler im Falle seiner Legendierung besitzt. Die Regelung entspricht den Vorgaben aus den §§ 110a und 110c der Strafprozessordnung.

#### **Zu den Absätzen 7 bis 9**

Die Absätze 7 bis 9 regeln mit Blick auf das Instrument des Verdeckten Ermittlers die Benachrichtigungspflichten in Anlehnung bereits bestehender Regelungen des Bundeskriminalamtgesetzes, die im Übrigen auch den verfassungsrechtlichen Anforderungen aus der aktuellen Rechtsprechung des Bundesverfassungsgerichts gerecht werden.

#### **Zu Absatz 7**

Beim Einsatz eines Verdeckten Ermittlers sind neben der Person, gegen die sich die Maßnahme konkret richtet (Zielperson) auch die Personen zu benachrichtigen, deren nicht allgemein zugängliche Wohnung der Verdeckte Ermittler betreten hat. Dies trägt dem Umstand der Wohnung als besonders geschützter Raum Rechnung. Erfasst werden zudem erheblich mitbetroffene Personen. Diese Formulierung trägt dem Umstand Rechnung, dass durch die Streubreite einer solchen Maßnahme eine Vielzahl von Personen in jedoch jeweils vergleichsweise unerheblicher Weise mitbetroffen sein kann. Es erscheint weder sachgerecht noch aus verfassungsrechtlichen Gründen geboten, diesen Personenkreis von der Maßnahme zu benachrichtigen. Halten sich jedoch Personen ständig oder für einen längeren Zeitraum im unmittelbaren Umfeld der Zielperson auf und werden deren Handlungen und Äußerungen in erheblichem Umfang im Rahmen der Maßnahme mit erfasst, sind auch diese Personen zu benachrichtigen. Nach Satz 2 hat eine Benachrichtigung zu unterbleiben, wenn überwiegende schutzwürdige Interessen anderer Betroffener der Benachrichtigung entgegenstehen. Dies erfordert eine Abwägung der widerstreitenden Interessen im Einzelfall, die einer weitergehenden gesetzlichen Regelung nicht zugänglich sind. Soweit die zu benachrichtigende Person nicht bekannt ist, enthält Satz 3 Regelungen darüber, wann Nachforschungen zu ihrer Identität geboten sind.

#### **Zu Absatz 8**

Die vorgesehenen Zurückstellungsgründe sind notwendig und hinreichend gewichtig, um eine Beschränkung der Benachrichtigungspflicht zu rechtfertigen. Insbesondere

die Ausbildung Verdeckter Ermittler, die Schaffung der erforderlichen Legende und das – nicht ohne weiteres reproduzierbare – Heranführen und Einschleusen eines Verdeckten Ermittlers in Kreise der Schleusungskriminalität sind mit einem ganz erheblichen zeitlichen, organisatorischen und finanziellen Aufwand verbunden. Zudem ist zu berücksichtigen, dass der Zurückstellungsgrund einer – gegebenenfalls auch wiederholten – gerichtlichen Überprüfung nach Absatz 9 unterliegt und damit der Rechtsschutz Betroffener hinreichend abgesichert ist.

### **Zu Absatz 9**

Absatz 9 trifft Regelungen über eine gerichtliche Kontrolle der Anwendung der in Absatz 8 enthaltenen Zurückstellungsgründe. Diese Kontrolle durch eine unabhängige Stelle hat das Bundesverfassungsgericht als unerlässlich zur Gewährleistung eines effektiven Rechtsschutzes des Betroffenen angesehen. Satz 1 bestimmt daher, dass eine über zwölf Monate hinausgehende Zurückstellung der gerichtlichen Zustimmung bedarf. Satz 4 sieht die Möglichkeit vor, fünf Jahre nach Beendigung der Maßnahme unter den dort genannten Voraussetzungen mit gerichtlicher Zustimmung endgültig von einer Benachrichtigung abzusehen. Bei sorgfältiger Prüfung dieser Voraussetzungen, insbesondere der Prognose, dass die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch zukünftig nicht eintreten werden, wird die Regelung in der praktischen Anwendung voraussichtlich keinen breiten Anwendungsbereich haben. Sie ist gleichwohl aufgenommen worden, um bei Vorliegen eines solchen Ausnahmefalles die Bundespolizei und die Gerichte nicht mit fortwährenden Prüfungen weiterer Zurückstellungen zu belasten, wenn absehbar ist, dass eine Benachrichtigung ohnehin auch in Zukunft nicht wird erfolgen können.

### **Zu Nummer 2 (§ 28a BPolG)**

#### **Zu Absatz 1**

Die Norm ist eine notwendige Ergänzung zur Eigensicherung der eingesetzten Polizeibeamtinnen und -beamten. Nahezu alle Polizeigesetze der Länder und das Bundeskriminalamtgesetz enthalten eine derartige Norm im Sachzusammenhang.

Insbesondere die Bekämpfung der Schleusungskriminalität ist eine wesentliche Aufgabe der Bundespolizei. Diese ist als Teil der Organisierten Kriminalität zunehmend von einer starken Abschottung und von einem konspirativen Täterverhalten geprägt. Schleuserorganisationen gehen dabei mit menschenverachtenden Modi Operandi vor und nehmen Gefahren für Leib und Leben der Geschleusten bis hin zum Tod billigend in Kauf, wie der Fund von 71 Leichen in einem luftdicht verschlossenen Kühl-lastwagen auf einer österreichischen Autobahn am 27. August 2015 verdeutlicht. Die

organisierte Schleusungskriminalität unterliegt aufgrund der immensen Gewinne („high-profit“-Kriminalität) einer erhöhten Gewaltbereitschaft. Kriminelle Schleuserbanden schrecken auch nicht vor der Anwendung von Gewalt – bis hin zum Schusswaffengebrauch – zurück. Die erhöhte Gewaltbereitschaft richtet sich nicht nur gegen Geschleuste, sondern auch gegen Konkurrenten oder „Verräter“. Verdeckte Ermittler müssen sich in diesem hoch gefährlichen Täterumfeld orientieren und zunächst eine Vertrauensbasis zur kriminellen Szene aufbauen.

Mit dem Eindringen in das Zentrum einer Schleuserorganisation erhöht sich zwangsläufig die Gefährdung des Verdeckten Ermittlers. Alleine aus Gründen der Fürsorge des Dienstherrn müssen die Polizeibehörden alle technischen Möglichkeiten nutzen, um das Leben und die Gesundheit sowie die Freiheit des eingesetzten verdeckt agierenden Polizeibeamten zu schützen. Der Einsatz des präventiven Verdeckten Ermittlers ohne (verdeckte) technische Absicherung ist nicht zu verantworten, weil die Möglichkeit eines sofortigen (Not-) Zugriffs und der Schutz der in Rede stehenden Rechtsgüter (Leib, Leben, Freiheit) den Polizeibehörden entzogen ist.

## **Zu Absatz 2**

Die Eigensicherungsmaßnahme nach Absatz 1 dient ausschließlich dem Schutz des Verdeckten Ermittlers und soll die Möglichkeit einer umgehenden Reaktion (Rettungszugriff) ermöglichen. Es handelt sich damit im Unterschied zu einer akustischen Überwachung zur Strafverfolgung oder zur Gefahrenabwehr nicht um ein Instrument, welches den Primärzweck verfolgt, Informationen zu erheben und unter bestimmten Umständen weiter zu verwenden. Grundsätzlich ist davon auszugehen, dass beim Einsatz eines Verdeckten Ermittlers in einer Wohnung dieser erheblichen Einfluss auf den Inhalt und den Verlauf des Gesprächs nehmen wird, so dass im Regelfall in derartigen Gesprächen nicht der Kernbereich privater Lebensgestaltung betroffen wird. Sollte dieser dennoch betroffen sein, regelt Satz 1, dass die Eigensicherungsmaßnahmen innerhalb von Wohnungen zu unterbrechen sind. Mit dem Zusatz „sobald dies ohne Gefährdung des Verdeckten Ermittlers möglich ist“ wird verdeutlicht, dass die Unterbrechung situationsangepasst und -angemessen erfolgen soll, insbesondere unter Berücksichtigung der Möglichkeit eines Rettungszugriffs. Andere Gründe dürfen zur Verzögerung der Unterbrechung nicht herangezogen werden. Satz 2 stellt sicher, dass Aufzeichnungen, die den Kernbereich privater Lebensgestaltung betreffen, unverzüglich zu löschen sind. Erkenntnisse über solche Vorgänge dürfen nicht verwertet werden, auch nicht unter den Voraussetzungen des Absatzes 4. Die Tatsache der Erfassung der Daten und ihrer Löschung sind in jedem Fall aktenkundig zu machen. Diese über den Löschvorgang angefallenen Daten dürfen zu Zwecken der Datenschutzkontrolle verwendet werden und sind zu löschen, wenn sie für diese

Zwecke nicht mehr erforderlich sind, spätestens am Ende des zweiten Kalenderjahres, das dem Jahr der Dokumentierung folgt.

### **Zu Absatz 3**

Die Anordnung von Maßnahmen nach Absatz 1 obliegt dem Präsidenten des Bundespolizeipräsidiums, seinem Vertreter oder einem Leiter einer Abteilung des Bundespolizeipräsidiums. Dies entspricht der verfassungsrechtlichen Maßgabe des Artikels 13 Absatz 5 GG. Bei Gefahr im Verzug kann die Maßnahmen auch durch einen Beamten des höheren Dienstes des Bundespolizeipräsidiums angeordnet werden. Hierbei handelt es sich um Angehörige des höheren Polizeivollzugsdienstes, die auch über entsprechende beurteilungsrelevante Kenntnisse verfügen, die an der Deutschen Hochschule der Polizei oder im Rahmen eines juristischen Studiums vermittelt wurden.

### **Zu Absatz 4**

Satz 1 stellt klar, dass sich die Zulässigkeit der Verwendung der nach Absatz 1 gewonnenen Daten für Zwecke der Strafverfolgung nach der Strafprozessordnung richtet. Ansonsten darf die Bundespolizei die Daten auch über den Zweck der Eigensicherung hinaus zur Gefahrenabwehr verwenden. Besondere Anforderungen gelten jedoch dann, wenn diese Daten in oder aus einer Wohnung erlangt wurden. In diesem Fall bedarf es einer gerichtlichen Rechtmäßigkeitskontrolle vor Verwendung der Daten zur Gefahrenabwehr. Die Formulierung entspricht den verfassungsrechtlichen Anforderungen nach Artikel 13 Absatz 5 GG.

### **Zu Absatz 5**

Sofern es sich bei den aufgezeichneten Daten um solche handelt, die den Kernbereich privater Lebensgestaltung betreffen, ist für ihre datenschutzrechtliche Behandlung vorrangig die Regelung nach Absatz 2 maßgeblich. Sofern der Kernbereich nicht betroffen ist, gilt Satz 1. Demnach sind die Aufzeichnungen nach Abschluss der Maßnahme unverzüglich zu löschen, es sei denn, eine Verwendung nach Absatz 4 kommt in Betracht. Satz 2 stellt durch Verweisung den Anspruch auf Benachrichtigung sicher.

### **Zu Nummer 3 (§ 70 Satz 2 BPolG)**

Folgeänderung zur Erfüllung des grundgesetzlichen Zitiergebots.

### **Zu Artikel 4 (Änderung des VIS-Zugangsgesetzes)**

Die Änderung schließt eine versehentlich durch überschneidende Gesetzgebungsverfahren entstandene Lücke. Die neue Nummer 3a des § 3 VIS-Zugangsgesetzes

(VISZG) war mit dem Entwurf eines Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes im März 2015 (Bundratsdrucksache 123/15) in das Gesetzgebungsverfahren eingebracht worden, also vor Inkrafttreten des GVVG-Änderungsgesetzes vom 12. Juni 2015 (BGBl I S. 926) am 20. Juni 2015. Zum Zeitpunkt der Einbringung existierte der erst mit dem GVVG-Änderungsgesetz eingeführte, die Terrorismusfinanzierung nunmehr zusammenfassend regelnde § 89c StGB mithin noch nicht, vielmehr war eine spezielle Strafbestimmung zur Terrorismusfinanzierung noch im damaligen § 89a Absatz 2 Nummer 4 StGB enthalten, der zum damaligen Zeitpunkt vom vorgesehenen § 3 Nummer 3a VISZG umfasst war, nachfolgend aber in § 89c StGB eingegangen ist. Letzteres ist im parlamentarischen Verfahren des Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes jedoch versehentlich unberücksichtigt geblieben. Die damit in § 3 Nummer 3a VISZG entstandene Lücke wird mit der Änderung gefüllt, indem der neue § 89c StGB in den Katalog aufgenommen wird.

#### **Zu Artikel 5 (Änderung des Artikel 10-Gesetzes)**

Die Regelung betrifft die Befugnis zur Datenerhebung, begründet jedoch keine Mitwirkungspflichten nach § 2. Sie hat mithin praktische Bedeutung in dem Fall, dass nicht der Diensteanbieter auf Anordnung erst Daten ausleitet, sondern in dem der überwachende Nachrichtendienst selbst aus einem Datenstrom die mit dem Antrag bezeichnete Filterung vornimmt. Im Ergebnis betrifft dies mithin Maßnahmen des BND und den Fall, dass bereits der Überwachung unterliegende Fernmeldeverkehrsbeziehungen nach zusätzlichen Telekommunikationsmerkmalen gefiltert werden sollen. Bei Gefahr in Verzug kann mit der Erfassung nicht bis zur Anordnung zugewartet werden. Die Nutzung der Daten darf jedoch erst nach Anordnung erfolgen, d.h. zunächst erfolgt eine rein technische Erfassung ohne jede menschliche Kenntnisnahme, die für sich noch kein Eingriff in Artikel 10 GG darstellt. Die Regelung schreibt im Weiteren vor, dass erhobene Daten zu löschen sind, sollte die beantragte Beschränkungsmaßnahme nicht binnen 24 Stunden nach Beantragung angeordnet werden. Einzelheiten sind in einer Dienstvorschrift zu regeln.

#### **Zu Artikel 6 (Änderung des Vereinsgesetzes)**

Mit der Änderung werden Zuwiderhandlungen gegen das Vereinsverbot umfassender unter Strafe gestellt. Künftig ist nicht mehr lediglich die Unterstützung des organisatorischen Zusammenhalts erfasst, sondern jegliche Unterstützung der Vereinigung, da

dies gleichermaßen den Tatunwert eines Verstoßes gegen das Vereinigungsverbot verwirklicht.

### **Zu Artikel 7 (Änderung des Bundeskriminalamtgesetzes)**

Die Änderung setzt die Änderung des Artikels 1 Nummer 1 auch im Bundeskriminalamtgesetz um.

### **Zu Artikel 8 (Änderung des Strafgesetzbuches)**

#### **Zu Nummer 1 (§ 84 Absatz 2 und § 85 Absatz 2 StGB)**

Die Änderung setzt die Änderung des Artikels 6 ebenso im Strafgesetzbuch (StGB) um.

#### **Zu Nummer 2 (§ 129a Absatz 9 StGB)**

Durch die Änderung kann auch in den Fällen des § 129 Absatz 5 StGB das Gericht Führungsaufsicht anordnen, wenn der Täter zu einer Freiheitsstrafe von mindestens sechs Monaten verurteilt wird und die Gefahr besteht, dass er weitere Straftaten begehen wird (§ 68 Absatz 1 StGB). Täter nach § 129a StGB sind nicht nur in der mitgliedschaftlichen, sondern auch in der unterstützenden Begehungsform oftmals von verfestigten Einstellungen motiviert, so dass auch insofern besonderer Bedarf besteht, etwaigen Wiederholungstaten im Wege von Weisungen nach § 68b StGB, die ihrerseits nach § 145a StGB sanktionsbewehrt sind, begegnen zu können. Die Weisungen dienen dabei nicht nur zur Überwachung, sondern auch zur Betreuung mit dem Ziel weiterer Resozialisierungshilfe. Die neue Möglichkeit zur Führungsaufsicht kraft richterlicher Anordnung ist wegen der obligatorischen Führungsaufsicht nach § 68f Absatz 1 StGB insbesondere für Freiheitsstrafen unter zwei Jahren bedeutsam, die in den Fällen des § 129a Absatz 5 StGB strafrahmenbedingt sogar näher liegen, als bei den bisher in § 129a Absatz 9 StGB genannten Fällen.

### **Zu Artikel 9 (Änderung des Telekommunikationsgesetzes)**

#### **Zu Nummer 1 (§ 95 Absatz 4 Satz 2 TKG)**

Mit der Ergänzung wird das Verhältnis von § 95 Absatz 4 TKG und dem neuen § 111 Absatz 1 Satz 3 TKG klargestellt.

## **Zu Nummer 2 (§ 111 TKG)**

§ 111 regelt, welche Daten von den geschäftsmäßigen Erbringern von Telekommunikationsdiensten bzw. Anbietern von Diensten der elektronischen Post zu erheben, zu verifizieren und zu speichern sind und stellt die Verantwortlichkeit bei der Einschaltung von Dritten durch einen Diensteanbieter klar. Zur besseren Lesbarkeit der Vorschrift wurden die Regelungen des bisherigen § 111 Absatz 1 in mehrere Absätze aufgeteilt, wobei die Pflicht zur Identifizierung von Kunden von im Voraus bezahlten Mobilfunkdiensten ergänzt wurde. Der neue Absatz 1 regelt jetzt die Pflichten der geschäftsmäßigen Erbringer von Telekommunikationsdiensten, Absatz 2 regelt die Pflichten von Erbringern von Diensten der elektronischen Post. Absatz 3 regelt, welche Pflichten die Diensteanbieter treffen, wenn ihnen Änderungen bekannt werden. Absatz 4 regelt die Verantwortlichkeit bei der Einschaltung von Dritten. Die Absätze 5 und 6 enthalten die Regelungen der bisherigen Absätze 4 und 5.

Die Regelung im neuen Absatz 1 Satz 3 verpflichtet die geschäftsmäßigen Erbringer von Telekommunikationsdiensten sowie daran Mitwirkende bei im Voraus bezahlten Mobilfunkdiensten dazu, die nach § 111 Absatz 1 Satz 1 zu erhebenden Bestandsdaten der Anschlussinhaber auf ihre Richtigkeit hin zu überprüfen. Die Erweiterung der nach § 111 Absatz 1 bereits bestehenden Pflicht zur Erhebung und Speicherung der Daten ist geboten, um eine belastbare Datenlage für die Auskunftsverfahren nach den §§ 112, 113 TKG in den Kundendateien zu erhalten. In seiner Entscheidung vom 24. Januar 2012 (1 BvR 1299/05, Rz. 132 ff.) hat das Bundesverfassungsgericht festgestellt, dass § 111 dazu dient, eine verlässliche Datenbasis für Auskünfte nach den §§ 112, 113 TKG vorzuhalten, die es bestimmten Behörden erlaubt, als Anknüpfungspunkt für weitere Ermittlungen Telekommunikationsnummern individuellen Anschlussinhabern zuzuordnen.

In den vergangenen Jahren hat sich gezeigt, dass der Datenerhebungspflicht aus § 111 Absatz 1 Satz 1 nicht im gebotenen Umfang nachgekommen wurde. Teilweise wird seitens der Anbieter die Rechtsauffassung vertreten, dass keine gesetzliche Verpflichtung des jeweiligen Diensteanbieters zur Verifikation der erhobenen Bestandsdaten bestehe. Stichprobenuntersuchungen der Bundesnetzagentur haben im Segment der im Voraus bezahlten Mobilfunkdienste eine enorme Anzahl offensichtlich fehlerhafter Datensätze in Kundendatenbanken von Anbietern von Telekommunikationsdiensten ergeben. Es liegen zahlreiche Hinweise auf automatische und händisch eingetragene systematische Generierungen von fiktiven Angaben vor. Da es sich hierbei nicht um Einzelfälle, sondern um Erscheinungen mit Massencharakter handelt, sind die auf Grundlage von § 111 Absatz 1 derzeit erhobenen Daten quanti-

tativ und qualitativ unbefriedigend. Die Auskunftsverfahren der Behörden nach den §§ 112, 113 TKG führen daher in vielen Verfahren zu keinen brauchbaren Informationen bzw. liefern keinen Anknüpfungspunkt für weitere Ermittlungen. In diesem Zusammenhang besteht auch die Gefahr, dass Unschuldige, deren Daten von Kriminellen missbraucht werden, in strafrechtliche Ermittlungen hineingezogen werden.

Die Überprüfung der Richtigkeit der Daten hat durch Verfahren zu erfolgen, die für die Identifikation geeignet sind. Hierzu zählt insbesondere die Identifizierung durch Vorlage eines gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird. Außerdem kommen von deutschen Behörden ausgestellte Ersatzpapiere für Ausländer in Betracht, die über keine amtlichen Ausweispapiere ihres Heimatlandes verfügen (z. B. Ankunfts-nachweis und Bescheinigung über die Aufenthaltsgestattung). Soweit sich aus solchen ausgestellten Ersatzpapieren keine eigene Anschrift des Anschlussinhabers ergibt, sondern in den Papieren lediglich die Anschrift der ausstellenden Behörde oder der Aufnahmeeinrichtung angegeben ist, genügt auch die Erhebung und Speicherung dieser Anschrift den Vorgaben des § 111 Absatz 1 Satz 1 Nummer 2. Ebenso möglich sind ausländische amtliche Identitätsdokumente, also ausländische Reisepässe oder Personalausweise. Die Angaben nach § 111 Absatz 1 Satz 1, die mittels eines solchen Identitätsdokumentes verifizierbar sind, müssen durch dieses verifiziert werden. Bei juristischen Personen oder Personengesellschaften kann die Überprüfung durch Vorlage eines Auszugs aus dem Handels- oder Genossenschaftsregister oder einem vergleichbaren amtlichen Register oder Verzeichnis, der Gründungsdokumente oder gleichwertiger beweiskräftiger Dokumente oder durch Einsichtnahme in diese Register oder Verzeichnisse und Abgleich mit den Register- oder Verzeichnisdaten erfolgen.

Der neue Absatz 1 Satz 4 legt fest, dass von der Bundesnetzagentur weitere, zur Erreichung des Zieles einer Identifikation des Anschlussinhabers gleichermaßen geeignete Verfahren zur Überprüfung der Angaben nach § 111 Absatz 1 Satz 1 zugelassen werden. Falls bei Erwerb des im Voraus bezahlten Mobilfunkdienstes aufgrund des gewählten Vertriebsweges eine Überprüfung anhand eines vorgelegten gültigen amtlichen Ausweises ausscheidet, kann diese durch andere geeignete Verfahren durchgeführt werden, wie beispielsweise eine Überprüfung des Identitätsnachweises durch Web-Ident oder Post-Ident-Verfahren. Dabei ist entscheidend, dass eine unmittelbare Identifikation anhand eines Identitätsdokumentes zu einem Zeitpunkt vor der Freischaltung der vertraglich vereinbarten Mobilfunkdienstleistungen stattgefunden hat. Die Überprüfung kann auch durch Nutzung des erworbenen Mobilfunkdienstes selbst geschehen, z. B. kann eine erworbene SIM-Karte für ein digitales Überprüfungsverfahren verwendet werden. Eine Identifikation ohne Über-

prüfung eines Identitätsdokuments scheidet hingegen aus. Bei der vorgesehenen Anhörung der betroffenen Kreise sind sowohl die betroffenen Anbieter von Telekommunikationsdiensten bzw. deren Verbände als auch die zur Abfrage nach den §§ 112 und 113 TKG berechtigten Stellen zu beteiligen.

Die im neuen Absatz 1 Satz 5 vorgesehene Speicherung von Angaben zu dem Überprüfungsvorgang dient dem Zweck, den Behörden einen Anknüpfungspunkt für weitere Ermittlungen zur Feststellung des Anschlussinhabers zu ermöglichen. Bei Identifikation durch Vorlage eines Identitätsdokumentes sind Bezeichnung, Nummer und die ausstellende Behörde des Identitätsdokumentes zu speichern. Darüber hinaus ist die Art des zur Überprüfung eingesetzten Verfahrens zu speichern.

Der neue Satz 6 stellt durch den Verweis auf § 8 Absatz 1 Satz 6 des Geldwäschegesetzes klar, welche Angaben bei Identifizierung anhand eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes oder § 78 Absatz 5 des Aufenthaltsgesetzes zu speichern sind.

Mit der Änderung des bisherigen Absatzes 2 und Einführung des neuen Absatzes 3 wird die eigene öffentlich-rechtliche Pflicht des Vertriebspartners zur Datenerhebung aufgehoben. Um eine zutreffende Datenlage in der Kundendatei zu gewährleisten, trifft die Pflicht zur Datenerhebung daher zukünftig nur noch den Diensteanbieter gemäß § 111 Absatz 1 Satz 1 und Absatz 2. Von der bisher geltenden Möglichkeit der Delegation der Datenerhebungspflicht an Vertriebspartner wird in der Praxis häufig Gebrauch gemacht. Dabei hat sich allerdings gezeigt, dass die bisherigen vertraglichen Verpflichtungen der Vertriebspartner gegenüber den Diensteanbietern nicht ausreichen, um die Erhebung korrekter Kundendaten zu gewährleisten. Der weit überwiegende Anteil an Falschangaben ist auf dem Vertriebsweg des stationären Fachhandels durch Vertriebspartner zu verzeichnen. In Anbetracht der großen Anzahl lokaler Verkaufsstellen und der daneben bestehenden alternativen Vertriebswege kann die Richtigkeit des Datenbestands daher effektiv und nachhaltig nur mittels eines zentralen Systems zur Verifikation durch den Diensteanbieter sichergestellt werden.

Die Regelung stellt klar, dass es dem Diensteanbieter weiterhin frei steht, seine Pflicht zur Datenerhebung im Rahmen der Vorgaben des § 11 des Bundesdatenschutzgesetzes (BDSG) auf vertraglichem Wege insgesamt oder in Teilen auf Dritte zu delegieren. Er bleibt als Auftraggeber aber Hauptverantwortlicher mit allen Kontroll- und Überwachungspflichten.

In dem neuen Absatz 3 Satz 2 bleibt die Pflicht des bisherigen Vertriebspartners zur Übermittlung von im Rahmen der üblichen Geschäftsabwicklung bekannt werdenden Änderungen der Daten in sprachlich angepasster Form erhalten.

### **Zu Nummer 3 (§ 112 TKG)**

Die Änderung der Verweise in § 112 ist eine Folgeänderung zur Änderung des neuen § 111 Absatz 1 Satz 3 ff. TKG.

### **Zu Nummer 4 (§ 115 TKG)**

Die Änderung der Verweise in § 115 ist eine Folgeänderung zur Änderung des neuen § 111 Absatz 1 Satz 3 ff. TKG.

### **Zu Nummer 5 (§ 149 TKG)**

Die Änderung der Verweise und Erweiterung des Ordnungswidrigkeitstatbestandes in § 149 Absatz 1 Nummer 29 um die nicht, nicht richtige, nicht vollständige oder nicht rechtzeitig durchgeführte Überprüfung der Richtigkeit der erhobenen Daten sind Folgeänderungen zur Neufassung von § 111 Absatz 1 TKG.

Die Änderung in § 149 Absatz 1 Nummer 30 ist eine Folgeänderung zur Änderung des neuen § 111 Absatz 4 Satz 2 TKG. Dieser verpflichtet Dritte dazu, Änderungen der Daten nach § 111 Absatz 1 Satz 1 und Absatz 2 TKG, die im Rahmen des üblichen Geschäftsablaufes bekannt werden, dem Diensteanbieter unverzüglich zu übermitteln.

Die Änderung des Verweises in § 149 Nummer 30a ist eine Folgeänderung zur Verschiebung der Pflicht zur Löschung der Daten mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres aus § 111 Absatz 4 TKG in § 111 Absatz 6 TKG.

### **Zu Nummer 6 (§ 150 TKG)**

#### **Zu § 150 Absatz 14**

Absatz 14 enthält die bisher in § 111 Absatz 3 TKG enthaltene Regelung. Zur besseren Verständlichkeit ist das seinerzeitige Datum des Inkrafttretens konkret bezeichnet worden.

#### **Zu § 150 Absatz 15**

Mit der Neuregelung in § 111 Absatz 1 Satz 3 TKG wird der Diensteanbieter dazu verpflichtet, die Richtigkeit der nach § 111 Absatz 1 Satz 1 TKG erhobenen Daten durch geeignete Verfahren zu überprüfen und mit der Neuregelung in § 111 Absatz 1 Satz 5 TKG wird er dazu verpflichtet, Angaben zu dem Überprüfungsvorgang zu speichern. Die neue Regelung in § 150 Nummer 14 stellt klar, dass beide Verpflichtungen nur diejenigen Vertragsverhältnisse erfassen, die nach Ablauf der Übergangsfrist geschlossen werden. Vertragsverhältnisse, die bereits vor diesem Zeitpunkt bestehen, sind weder von der Überprüfungs- noch der Speicherpflicht erfasst.

Zur Umsetzung dieser Regelungen bedarf es der Vorgabe geeigneter Überprüfungsverfahren durch die Bundesnetzagentur. Mit der Übergangsfrist wird der Bundesnetzagentur ein angemessener zeitlicher Rahmen für die Entwicklung der Vorgaben eingeräumt und den Telekommunikationsanbietern wird die Implementierung erforderlicher organisatorischer und technischer Maßnahmen ermöglicht, wie beispielsweise die Anpassung laufender Verträge mit Vertriebspartnern und die Einführung neuer oder Änderung bereits eingeführter IT-gestützter Prozesse.

### **Zu Artikel 10 (Einschränkung eines Grundrechts)**

Durch Artikel 5 werden die Regelungen in § 15 Absatz 6 des Artikel 10-Gesetzes geändert, die Eingriffe in das Grundrecht nach Artikel 10 GG vorsehen.

### **Zu Artikel 11 (Inkrafttreten)**

Die Vorschrift regelt das Inkrafttreten. Satz 2 trägt dem Umstand Rechnung, dass mit Blick auf Artikel 4 (Änderung des VIS-Zugangsgesetzes) entsprechende technische Anpassungen erforderlich sind.

Dokumentenname: 160531 Kabinettfassung\_final.doc

Ersteller: BMI

Stand: 30.05.2016 12:45

...