

# **Gesetzentwurf**

## **der Staatsregierung**

### **zur Änderung des Bayerischen Verfassungsschutzgesetzes**

#### **A. Problem**

1. Das novellierte Bayerische Verfassungsschutzgesetz (BayVSG) vom 12. Juli 2016 (GVBl. S. 145) ist am 1. August 2016 in Kraft getreten. Während des laufenden Gesetzgebungsverfahrens verkündete das Bundesverfassungsgericht (BVerfG) das Urteil zum Bundeskriminalamtgesetz (BKAG) (BVerfGE 141, 220 ff.). Inwieweit dieses zum Polizeirecht ergangene Urteil auch für das Recht der Nachrichtendienste bedeutsam ist, konnte in der Kürze der Zeit nicht beurteilt werden. Die Novelle von 2016 hat daher nur erste Konsequenzen aus dem neuen Urteil gezogen, weitere Änderungen der gebotenen eingehenden Prüfung vorbehalten.
2. Die Ständige Konferenz der Innenminister und –senatoren der Länder (IMK) hat in ihrer Herbstsitzung am 7./8. Dezember 2017 Bund und Ländern empfohlen, den von einer Arbeitsgruppe unter Federführung des Bundesministeriums des Innern entwickelten „harmonisierten Rechtsrahmen“ in Überlegungen zur Novellierung ihrer Verfassungsschutzgesetze einzubeziehen.

#### **B. Lösung**

Soweit das Urteil des BVerfG verallgemeinerungsfähige Aussagen enthält, die für das Recht der Nachrichtendienste als Leitlinien zu verstehen sind, wird das Bayerische Verfassungsschutzgesetz weiter entwickelt. Gleichzeitig werden Regelungsideen des harmonisierten Rechtsrahmens der IMK aufgegriffen.

#### **C. Alternativen**

Keine.

#### **D. Kosten und Nutzen**

Es handelt sich weder im staatlichen noch im kommunalen oder privaten Bereich um originär kostenbegründende Anforderungen, sondern im Wesentlichen um die Normierung haushaltsneutraler behördlicher Befugnisse und ihrer rechtlichen Schranken.

**Gesetzentwurf**  
**zur Änderung des**  
**Bayerisches Verfassungsschutzgesetzes**

**§ 1**

**Änderung des Bayerischen Verfassungsschutzgesetzes**

Das Bayerische Verfassungsschutzgesetz (BayVSG) vom 12. Juli 2016 (GVBl. S. 145, BayRS 12-1-I), das durch Art. 39b Abs. 1 des Gesetzes vom [...] [...] 2018 (GVBl. S. [...])<sup>1</sup> geändert worden ist, wird wie folgt geändert:

1. Art. 7 Abs. 2 Satz 2 wird wie folgt gefasst:

„<sup>2</sup>Sie sind nach Abschluss der Kontrolle nach Art. 28 Abs. 2, spätestens nach drei Jahren zu löschen, es sei denn, dass besondere Gründe der Geheimhaltung oder des Geheimschutzes eine längere Aufbewahrung gebieten.“

2. In Art. 8 Abs. 2 Satz 1 werden die Wörter „und den Schutz des Kernbereichs privater Lebensgestaltung gewährleistet“ gestrichen.
3. Nach Art. 8 werden folgende Art. 8a und 8b eingefügt:

„Art. 8a

Schutz des Kernbereichs privater Lebensgestaltung und der  
Berufsgeheimnisträger

(1) <sup>1</sup>Die Anwendung nachrichtendienstlicher Mittel ist unzulässig, soweit tatsächliche Anhaltspunkte dafür vorliegen, dass durch sie allein Erkenntnisse gewonnen werden würden

1. aus dem Kernbereich privater Lebensgestaltung oder

---

<sup>1</sup> Es handelt sich um das noch im Gesetzgebungsverfahren befindliche neue Bayerische Datenschutzgesetz.

2. bei einem Rechtsanwalt, einem Kammerrechtsbeistand, einem der in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder Nr. 4 der Strafprozeßordnung (StPO) genannten Berufsheimnisträger oder einer diesen nach § 53a Abs. 1 Satz 1 StPO gleich stehenden Person, über die der Berufsheimnisträger das Zeugnis verweigern dürfte.

<sup>2</sup>Ergeben sich während der Anwendung nachrichtendienstlicher Mittel tatsächliche Anhaltspunkte im Sinne von Satz 1, ist die Maßnahme zu unterbrechen, sobald dies ohne Gefährdung eingesetzter Personen möglich ist und solange die Anhaltspunkte bestehen. <sup>3</sup>Soweit bei der Anwendung nachrichtendienstlicher Mittel Erkenntnisse im Sinne von Satz 1 gewonnen wurden, dürfen sie nicht verarbeitet werden. <sup>4</sup>Aufzeichnungen solcher Erkenntnisse sind zu löschen. <sup>5</sup>Beim Einsatz technischer Mittel findet § 3a Satz 3 bis 7 des Artikel 10-Gesetzes (G 10) entsprechende Anwendung.

(2) Erfolgen Maßnahmen bei einem der in § 53 Abs. 1 Satz 1 Nr. 3 bis 3b oder Nr. 5 StPO genannten Berufsheimnisträger oder einer diesen nach § 53a Abs. 1 Satz 1 gleich stehenden Person nicht zur Aufklärung von deren eigenen Bestrebungen oder Tätigkeiten, sind das öffentliche Interesse an den von dem Berufsheimnisträger wahrgenommenen Aufgaben und das Interesse an der Geheimhaltung der diesem anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen.

#### Art. 8b

##### Zweckbindung

(1) <sup>1</sup>Das Landesamt darf personenbezogene Daten, die es für einen bestimmten Zweck erhoben hat, für andere in Art. 5 Abs. 1 Satz 1 genannte Zwecke weiterverarbeiten, wenn sich tatsächliche Anhaltspunkte erkennen lassen, dass die Daten als konkreter Ansatz zur Erfüllung des geänderten Zwecks geeignet sind. <sup>2</sup>Soweit die Erhebung der Daten nur zum Schutz bestimmter Rechtsgüter zulässig ist, dürfen die erhobenen Daten nur weiterverarbeitet werden, wenn sich tatsächliche Anhaltspunkte erkennen

lassen, dass die Zweckänderung dem Schutz eines mindestens vergleichbar bedeutsamen Rechtsguts dient.

(2) <sup>1</sup>Personenbezogene Daten, die durch einen verdeckten Einsatz technischer Mittel zur Wohnraumüberwachung oder einen verdeckten Zugriff auf informationstechnische Systeme erlangt wurden, dürfen nur weiterverarbeitet werden,

1. wenn die sachlichen Voraussetzungen des Art. 9 Abs. 1 Satz 1 vorliegen,
2. wenn tatsächliche Anhaltspunkte für die dringende Gefahr der Begehung von Straftaten im Sinne von § 100b Abs. 2 StPO vorliegen oder
3. zur Verfolgung von Straftaten, sofern die Daten der Verfolgung von Straftaten dienen, zu deren Aufklärung eine solche Maßnahme nach den entsprechenden Befugnissen der Strafprozeßordnung angeordnet werden könnte.

<sup>2</sup>Personenbezogene Daten aus Maßnahmen nach Art. 9, die durch Herstellung von Lichtbildern oder Bildaufzeichnungen erlangt wurden, dürfen nicht zu Strafverfolgungszwecken weiterverarbeitet werden.

(3) Personenbezogene Daten, die durch Maßnahmen nach Art. 15 Abs. 2 und 3 sowie Art. 16 erlangt wurden, dürfen nur unter entsprechender Anwendung des § 4 G 10 weiterverarbeitet werden.“

4. Art. 9 wird wie folgt geändert:

a) Der Wortlaut wird Abs. 1 und wird wie folgt geändert:

aa) Satz 1 wird wie folgt geändert:

aaa) Im Satzteil vor Nr. 1 werden nach dem Wort „einsetzen“ die Wörter „ , um das nichtöffentlich gesprochene Wort abzuhören und aufzuzeichnen sowie Lichtbilder und Bildaufzeichnungen herzustellen“ eingefügt.

bbb) Nr. 3 wird wie folgt gefasst:

„3. Sachen, deren Erhaltung im besonderen öffentlichen Interesse geboten ist.“

bb) Satz 2 wird durch die folgenden Sätze 2 und 3 ersetzt:

„<sup>2</sup>Zur Vorbereitung und Durchführung der Maßnahme darf die Wohnung auch ohne Wissen des Inhabers und der Bewohner betreten werden, wenn dies ausdrücklich angeordnet wurde. <sup>3</sup>§ 3 Abs. 2 Satz 1 G 10 gilt entsprechend.“

b) Es wird folgender Abs. 2 angefügt:

„(2) <sup>1</sup>Die Maßnahme darf sich nur gegen eine Person richten, von der auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass sie für die Gefahr verantwortlich ist (Zielperson), und nur in deren Wohnung durchgeführt werden. <sup>2</sup>In der Wohnung einer anderen Person ist die Maßnahme zulässig, wenn tatsächliche Anhaltspunkte vorliegen, dass

1. die Zielperson sich dort zur Zeit der Maßnahme aufhält,
2. sich dort für die Erforschung des Sachverhalts relevante Informationen ergeben werden und
3. eine Maßnahme in der Räumlichkeit der Zielperson allein nicht zur Erforschung des Sachverhalts ausreicht.“

5. Art. 10 wird wie folgt geändert:

a) In Abs. 1 wird nach der Angabe „Art. 9“ die Angabe „Abs. 1“ eingefügt.

b) Abs. 2 wird wie folgt geändert:

aa) Satz 1 wird wie folgt geändert:

aaa) In Nr. 1 wird das Wort „und“ gestrichen.

bbb) In Nr. 2 wird der Punkt am Ende durch das Wort „und“ ersetzt.

ccc) Es wird folgende Nr. 3 angefügt:

„3. Daten, die den Kernbereich privater Lebensgestaltung betreffen, soweit technisch möglich nicht erhoben werden.“

bb) In Satz 3 wird das Wort „Kopierte“ durch das Wort „Erhobene“ ersetzt.

c) Es wird folgender Abs. 3 angefügt:

„(3) <sup>1</sup>Die Maßnahme darf sich nur gegen die Zielperson richten und nur durch Zugriff auf deren informationstechnisches System durchgeführt werden. <sup>2</sup>Auf informationstechnische Systeme, die räumlich von der Zielperson getrennt sind, darf die Maßnahme erstreckt werden, soweit von dem informationstechnischen System der Zielperson darauf zugegriffen werden kann. <sup>3</sup>Der Zugriff auf informationstechnische Systeme anderer ist zulässig, wenn tatsächliche Anhaltspunkte vorliegen, dass

1. die Zielperson deren informationstechnisches System benutzt oder benutzt hat,
2. sich dadurch für die Abwehr der Gefahr relevante Informationen ergeben werden und
3. ein Zugriff auf das informationstechnische System der Zielperson allein nicht zur Erforschung des Sachverhalts ausreicht.“

6. Art. 11 wird wie folgt geändert:

a) Abs. 3 wird aufgehoben.

b) Der bisherige Abs. 4 wird Abs. 3 und in Satz 2 Halbsatz 1 wird die Angabe „Art. 9 Satz 1“ durch die Angabe „Art. 9 Abs. 1 Satz 1“ ersetzt.

c) Der bisherige Abs. 5 wird Abs. und in Satz 1 Halbsatz 1 wird die Angabe „Abs. 1 bis 4“ durch die Angabe „Abs. 1 bis 3“ ersetzt.

7. Art. 13 wird wie folgt geändert:

a) Abs. 1 wird wie folgt geändert:

aa) Der Wortlaut wird Satz 1 und wird wie folgt geändert:

aaa) Im Satzteil vor Nr. 1 werden die Wörter „unter den Voraussetzungen des § 3 G 10“ gestrichen.

bbb) Der Nr. 1 wird folgende Nr. 1 vorangestellt:

„1. eine Telekommunikationsüberwachung bereits angeordnet wurde oder zeitgleich angeordnet wird,“.

ccc) Die bisherigen Nrn. 1 und 2 werden die Nrn. 2 und 3.

bb) Es wird folgender Satz 2 angefügt:

„<sup>2</sup>Zur Vorbereitung und Durchführung der Maßnahme darf die Wohnung des Betroffenen auch ohne Wissen des Inhabers und der Bewohner betreten werden, wenn dies zuvor ausdrücklich angeordnet wurde.“

b) In Abs. 2 werden die Wörter „§§ 2, 3a bis 4, 9 bis 13, 17 bis 20 G 10 sowie Art. 2“ durch die Wörter „§§ 2, 9 bis 13, 17 bis 20 G 10 sowie Art. 2“ ersetzt.

8. Art. 15 wird wie folgt geändert:

a) Abs. 2 wird wie folgt geändert:

aa) In Satz 1 wird die Satznummerierung gestrichen.

bb) Satz 2 wird aufgehoben.

b) Abs. 3 wird wie folgt geändert:

aa) In Satz 1 wird die Satznummerierung gestrichen.

bb) Satz 2 wird aufgehoben.

9. Art. 17 wird wie folgt geändert:

a) In Abs. 2 Satz 1 wird die Angabe „ 4,“ gestrichen.

b) In Abs. 3 Satz 1 und 2 wird jeweils nach der Angabe „Art. 15 Abs. 2“ die Angabe „Satz 1“ gestrichen.

10. Art. 20 wird wie folgt geändert:



- a) Abs. 1 Satz 1 Nr. 2 wird wie folgt geändert:
  - aa) In Buchst. a wird das Wort „und“ am Ende durch ein Komma ersetzt.
  - bb) In Buchst. b wird der Punkt am Ende durch das Wort „und“ ersetzt.
  - cc) Es wird folgender Buchst. c angefügt:
    - „c) Übermittlungen nach Art. 25 Abs. 3 Satz 1 Nr. 1 und 2, soweit sie der Verfügungsberechtigung des Landesamts unterliegen.“
- b) In Abs. 2 Halbsatz 1 wird nach der Angabe „Art. 15 Abs. 2“ die Angabe „Satz 1“ gestrichen.

11. Art. 21 Abs. 1 Satz 2 wird wie folgt gefasst:

„<sup>2</sup>Bei schriftlichen und elektronischen Akten erfolgt die Löschung erst, wenn die Voraussetzungen des Satzes 1 für den gesamten Akt gegeben sind.“

12. Art. 23 Abs. 1 Satz 3 wird wie folgt geändert:

- a) In Nr. 1 wird das Wort „und“ am Ende durch ein Komma ersetzt.
- b) In Nr. 2 wird der Punkt am Ende durch das Wort „und“ ersetzt.
- c) Es wird folgende Nr. 3 angefügt:
  - „3. solche Daten, die im Falle des Art. 21 Abs. 1 Satz 2 zur Erfüllung der Aufgaben nicht mehr erforderlich sind und die ausschließlich für eine zukünftige Übergabe an ein staatliches Archiv gespeichert sind; durch technische und organisatorische Vorgaben ist sicherzustellen, dass diese Daten nicht mehr für die in Art. 5 Abs. 1 genannten Zwecke verwendet werden.“

13. Art. 25 wird wie folgt geändert:

- a) Abs. 1 wird wie folgt geändert:
  - aa) Im Satzteil vor Nr. 1 werden nach den Wörtern „übermitteln, wenn“ die Wörter „sich tatsächliche Anhaltspunkte erkennen lassen, dass“ eingefügt.
  - bb) Nr. 1 wird durch die folgenden Nrn. 1 und 2 ersetzt:

- „1. zum Schutz der von Art. 3 umfassten Rechtsgüter oder sonst für Zwecke der öffentlichen Sicherheit,
2. für Zwecke der Strafverfolgung, der Strafvollstreckung, des Strafvollzugs und der Gnadenverfahren oder“.

dd) Die bisherige Nr. 2 wird Nr. 3.

b) Nach Abs. 1 wird folgender Abs. 1a eingefügt:

„(1a) Abs. 1 gilt entsprechend für die Übermittlung von Informationen an

1. öffentliche und nicht-öffentliche Stellen in Mitgliedstaaten der Europäischen Union,
2. zwischen- und überstaatliche Stellen der Europäischen Union oder deren Mitgliedstaaten und
3. öffentliche Stellen von Staaten, welche die Bestimmungen des Schengen-Besitzstandes auf Grund eines Assoziierungsübereinkommens mit der Europäischen Union über die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes anwenden.“

c) Abs. 2 Satz 1 wird wie folgt geändert:

aa) Dem Satzteil vor Nr. 1 werden die Wörter „ , wenn sich tatsächliche Anhaltspunkte erkennen lassen, dass der Empfänger die Informationen benötigt“ angefügt.

bb) Nr. 1 wird wie folgt gefasst:

- „1. zum Schutz des Bestands oder der Sicherheit des Bundes oder eines Landes oder von Leib, Leben, Gesundheit, Freiheit oder sexueller Selbstbestimmung einer Person oder Sachen, deren Erhaltung im besonderen öffentlichen Interesse geboten ist,“ .

d) Abs. 3 wird wie folgt geändert:

aa) Der Wortlaut wird Satz 1 und wird wie folgt geändert:

aaa) In Nr. 2 werden nach dem Wort „wenn“ die Wörter „sich tatsächliche Anhaltspunkte erkennen lassen, dass“ eingefügt.

bbb) In Nr. 3 werden nach dem Wort „wenn“ die Wörter „tatsächliche Anhaltspunkte dafür bestehen, dass“ eingefügt.

bb) Es wird folgender Satz 2 angefügt:

„<sup>2</sup>Die Übermittlung hat zu unterbleiben, wenn im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist.“

e) Abs. 4 Satz 1 wird wie folgt gefasst:

„<sup>1</sup>Art. 8b Abs. 2 und 3 bleibt unberührt.“

14. In Art. 27 Abs. 2 Satz 1 Nr. 1 werden die Wörter „von bedeutendem Wert“ gestrichen.

## **§ 2**

### **Einschränkung von Grundrechten**

Durch § 1 werden die Grundrechte der Versammlungsfreiheit, auf Unverletzlichkeit der Wohnung und das Brief-, Post- und Fernmeldegeheimnis (Art. 8 Abs. 1, Art. 10 und 13 des Grundgesetzes, Art. 106 Abs. 3, Art. 112 und 113 der Verfassung) eingeschränkt.

## **§ 3**

### **Inkrafttreten**

Dieses Gesetz tritt am \_\_\_\_\_ in Kraft.

## **Begründung:**

### **A. Allgemeines**

#### ***I. Anlass und Zielsetzung***

1. Die Novelle des Bayerischen Verfassungsschutzgesetzes (BayVSG) vom 12. Juli 2016 (GVBl. S. 145) ist am 1. August 2016 in Kraft getreten. Am 20. April 2016, während des laufenden Gesetzgebungsverfahrens und kurz vor der von den Ausschüssen für Kommunale Fragen, Innere Sicherheit und Sport und für Verfassung, Recht und Parlamentsfragen des Bayerischen Landtags am 27. April 2016 gemeinsam zur Novelle durchgeführten Anhörung von Sachverständigen, verkündete das Bundesverfassungsgericht (BVerfG) das Urteil zum Bundeskriminalamtgesetz (BKAG), in welchem der Erste Senat über die Verfassungsmäßigkeit der im Jahre 2009 in das BKAG eingefügten polizeilichen Befugnisse des Bundeskriminalamts zum Einsatz von heimlichen Überwachungsmaßnahmen für die Abwehr von Gefahren des internationalen Terrorismus entschied und eine lange Rechtsprechung zu einzelnen Fragen dieses Themenkomplexes zusammenführte (BVerfGE 141, 220 ff.).
  - a) In diesem Urteil befand der Erste Senat, dass die Ermächtigung des Bundeskriminalamts zum Einsatz von heimlichen Überwachungsmaßnahmen zwar im Grundsatz mit den Grundrechten des Grundgesetzes vereinbar sei, die konkrete gesetzliche Ausgestaltung der Befugnisse genüge aber in verschiedener Hinsicht nicht dem Verhältnismäßigkeitsgrundsatz. Der Erste Senat beanstandete sowohl die Voraussetzungen für die Durchführung solcher Maßnahmen als auch die Frage der Übermittlung der Daten zu anderen Zwecken an dritte Behörden sowie die Weiterleitung von Daten an ausländische Behörden. Die Voraussetzungen für die Durchführung der Maßnahmen seien teilweise zu unbestimmt und zu weit formuliert, es fehle zum Teil an flankierenden rechtsstaatlichen Absicherungen, vor allem zum Schutz des Kernbereichs privater Lebensgestaltung oder zur Gewährleistung von Transparenz, individuellem Rechtsschutz und aufsichtlicher Kontrolle.

Besonders strenge Anforderungen formulierte der Erste Senat für die Befugnisse zur verdeckten Wohnraumüberwachung und zur Online-Durchsuchung, da diese besonders tief in die Privatsphäre eindringen.

- b) Ob und inwieweit die im BKAG-Urteil formulierten verfassungsgerichtlichen Anforderungen an heimliche Überwachungsmaßnahmen unmodifiziert auf die Nachrichtendienste übertragbar sind, konnte seitens der zur Novelle 2016 angehörten Sachverständigen in der Kürze der damals zwischen Urteilsverkündung und Anhörung verbleibenden Zeit nicht abschließend geprüft werden. Es bestand allerdings Einigkeit, dass das BKAG-Urteil auf die Tätigkeit des BKA als Polizeibehörde zugeschnitten sei und daher nicht ohne Weiteres auf das Recht der Nachrichtendienste übertragen werden könne (vgl. auch die Gutachten der Sachverständigen Prof. Dr. Lindner vom 18. April 2016, S. 1 f.; Dr. Löffelmann vom 22. April 2016, S. 1; Prof. Dr. Wollenschläger vom 25. April 2016, S. 5). Da aber der Erste Senat mit dem BKAG-Urteil erkennbar den Ansatz einer systembildenden Leitentscheidung verfolgte, mit der vorausgegangene Rechtsprechung teils ausdrücklich korrigiert und insgesamt konsolidiert wurde (vgl. BVerfGE 141, 220 Rn. 292), war bereits damals erkennbar, dass gewisse Vorgaben, die das BVerfG im BKAG-Urteil aus dem Verhältnismäßigkeitsgrundsatz für den Gesetzgeber im Bereich des Polizeirechts abgeleitet hatte, für das Recht der Nachrichtendienste nicht ohne Bedeutung bleiben können. Welche Vorgaben dies im konkreten sind, in welchem Umfang und in welcher Form diese übertragbar sind, bedurfte jedoch noch näherer rechtlicher Prüfung. Auf Grund der Zielsetzung der Novelle von 2016, im Interesse einer effektiven und engen Zusammenarbeit der Sicherheitsbehörden von Bund und Ländern möglichst einheitliche Rechtsstandards zu etablieren und das bayerische Verfassungsschutzrecht stärker mit Bundesrecht zu synchronisieren, war zunächst beabsichtigt, abzuwarten, welche Änderungen der Bundesgesetzgeber vornehmen würde. Zudem würden Änderungen des Bundesrechts aufgrund der zahlreichen dynamischen Verweisungen hierauf in der Novelle von 2016 unmittelbare

Geltung im bayerischen Landesrecht entfalten, ohne dass es eines eigenen Änderungsgesetzes seitens des Landesgesetzgebers bedürfte.

Der im Nachgang zur Sachverständigenanhörung von der CSU-Landtagsfraktion am 1. Juni 2016 eingebrachte Änderungsantrag (LT-Drs. 17/11609) beschränkte sich daher zunächst – neben dem Aufgreifen von Verbesserungsvorschlägen der Sachverständigen – ausdrücklich auf punktuelle Änderungen bezüglich einzelner Aussagen des BKAG-Urteils, die bereits damals als allgemeingültig angesehen wurden.

- c) Die Bedeutung der im BKAG-Urteil formulierten verfassungsgerichtlichen Anforderungen für das Recht der Nachrichtendienste ist bis heute höchststrichterlich nicht geklärt und auch in der Literatur umstritten (vgl. Gärditz, in: Menzel/Müller-Terpitz (Hrsg.), Verfassungsrechtsprechung, 3. Aufl. 2017, S. 988 ff.; Siems, NWVBl. 2018, 1 ff.). Das BVerfG selbst hat in dem die verfassungsrechtlichen Anforderungen an Befugnisnormen zur heimlichen Überwachung betreffenden Teil des BKAG-Urteils zwar über den konkreten Streitgegenstand, die präventiv-polizeilichen Befugnisse des Bundeskriminalamts zur Terrorismusbekämpfung, hinaus von „Polizeibehörden“, an keiner Stelle aber von „Nachrichtendiensten“ gesprochen.

Der wesentliche und für die Frage der uneingeschränkten Übertragung der im BKAG-Urteil aufgestellten Grundsätze auf Nachrichtendienste entscheidende Unterschied zwischen Polizei und Nachrichtendiensten besteht darin, dass den Nachrichtendiensten in Deutschland keine Befugnisse zu exekutiv-polizeilichem Tätigwerden zustehen (§ 8 Abs. 3 BVerfSchG; § 4 Abs. 2 MADG; § 2 Abs. 3 BNDG; in Bayern Art. 5 Abs. 2 BayVSG). Ähnlich wie der britische Inlandsnachrichtendienst MI 5 (Military Intelligence Section 5; heute Security Service), dem der deutsche Verfassungsschutz nach dem Zweiten Weltkrieg nachgebildet wurde, werden die Verfassungsschutzbehörden als analytische Informationsdienstleister für gefahrenintervenierende Sicherheitsbehörden wie die Polizei tätig. Ihnen obliegt es, Erkenntnisse über Bestrebungen und

Tätigkeiten, die gegen die Existenzgrundlagen des Staates gerichtet sind, unabhängig von konkreten Gefahren im Vorfeld zu sammeln, zu analysieren und so zu verdichten, dass sie schließlich an die Polizei oder andere mit exekutiven Befugnissen ausgestattete Behörden übermittelt werden können, damit diese die erforderlichen Maßnahmen zur Intervention ergreifen und die Realisierung der konkretisierten Gefahr verhindern können. Die Verfassungsschutzbehörden als Inlandsnachrichtendienste sind damit Ausdruck der Grundentscheidung des Grundgesetzes für eine wehrhafte Demokratie, des Selbstbehauptungswillens des Rechtsstaates und folglich Bestandteil des Sicherheitssystems der Bundesrepublik Deutschland (BVerfG, Beschluss vom 13. Juni 2017 – 2 BvE 1/15 – Rn. 110; Beschluss vom 13. Oktober 2016 – 2 BvE 2/15 – Rn. 126).

Demgegenüber vereinen Polizeibehörden in sich informationelle und operativ-polizeiliche Eingriffsbefugnisse. Sie können aufgrund der erhobenen Informationen somit unmittelbar Folgeeingriffe durchführen. Aufgrund des unmittelbaren Risikos von Folgemaßnahmen gegen die jeweiligen Betroffenen sind an die grundrechtliche Rechtfertigung polizeilicher Befugnisse zur Datenerhebung höhere und damit andere Anforderungen zu stellen als dies bei Nachrichtendiensten der Fall ist (vgl. BVerfGE 130, 151/206; 100, 313/383). Die Kumulation von Datenerhebung und operativ-polizeilicher Zugriffsmöglichkeit in derselben Behörde verleiht der Datenerhebung eine erhöhte Eingriffsintensität, da mit den – zumal verdeckt erhobenen – Informationen zugleich und unmittelbar die Möglichkeit eines operativ-polizeilichen Zugriffs im Raum steht, etwa in der Modalität einer Durchsuchung, Beschlagnahme oder Ingewahrsamnahme. Bei den Verfassungsschutzbehörden verhält es sich grundlegend anders. Diese verfügen gerade nicht über operativ-polizeiliche Befugnisse – das kumulierte Grundrechtsgefährdungspotential besteht mithin nicht. Folgeeingriffe können erst nach der an eigene materielle Voraussetzungen geknüpften Übermittlung und damit nach einem eigenständigen Verfahrensschritt aufgrund einer selbständigen Entscheidung durch die empfangende (Polizei-)Behörde

erfolgen. Aus diesem Grund ist es sachlich nicht gerechtfertigt, das BKAG-Urteil des BVerfG vollumfänglich und undifferenziert auf das Bayerische Verfassungsschutzgesetz zu übertragen.

Dieser Logik folgend hat das BVerfG in seinem Urteil zum Antiterrordateigesetz (ATDG) aus dem Jahr 2013 ausführlich dargelegt, dass die Rechtsordnung zwischen einer grundsätzlich offen arbeitenden Polizei, die auf eine operative Aufgabenwahrnehmung ausgerichtet und von detaillierten Rechtsgrundlagen angeleitet sei, und den grundsätzlich verdeckt arbeitenden Nachrichtendiensten unterscheide, die auf die Beobachtung und Aufklärung im Vorfeld beschränkt seien und sich deswegen auf weniger ausdifferenzierte Rechtsgrundlagen stützen können (BVerfGE 133, 277 Rn. 122).

- d) Ausgehend von diesen Prämissen spricht viel dafür, dem Urteil lediglich systemübergreifende Leitlinien zu entnehmen, die als verfassungsrechtliche Richtungsvorgaben bei der Gesetzgebung zu berücksichtigen sind, und die Vorgaben des BKAG-Urteils nicht unmodifiziert auf das Recht der Nachrichtendienste zu übertragen. Daraus ergeben sich folgende Konsequenzen:
- Auch im nachrichtendienstlichen Tätigkeitsbereich beansprucht der Kernbereich privater Lebensgestaltung gegenüber allen Überwachungsmaßnahmen Beachtung und bedarf jedenfalls bei Befugnissen, die typischerweise zur Erhebung kernbereichsrelevanter Daten führen, einer normenklaren Gewährleistung durch den Gesetzgeber (vgl. BVerfGE 141, 220 Rn. 123).
  - Differenzierungen hinsichtlich des Kreises besonders geschützter Berufsheimnisträger sind nach ähnlichen Grundsätzen wie bei polizeilichen Informationserhebungen vorzunehmen (vgl. BVerfGE 141, 220 Rn. 131 ff.).
  - Ebenso wie die Verarbeitung personenbezogener Daten durch die Polizei richten sich auch die weitere Nutzung und Übermittlung der von Nachrichtendiensten erhobenen Informationen nach dem Grundsatz der



Zweckbindung (vgl. BVerfGE 141, 220 Rn. 276 ff.). Eine Nutzung von personenbezogenen Daten über den konkreten Anlass und rechtfertigenden Grund einer Datenerhebung hinaus bedürfen einer gesetzlichen Rechtsgrundlage (vgl. BVerfGE 141, 220 Rn. 277). Die Zulassung von Zweckänderungen muss sich am Kriterium der hypothetischen Datenneuerhebung orientieren, d.h. der ursprüngliche und der geänderte Verwendungszweck müssen verfassungsrechtlich ein vergleichbares Gewicht aufweisen, ohne dass allerdings die Gefahrenlage bzw. der Tatverdacht hinsichtlich des Konkretisierungsgrades identisch sein muss – ausreichend ist bereits ein konkreter Ermittlungsansatz (vgl. BVerfGE 141, 220 Rn. 286 ff.). Weiter reicht die Zweckbindung nur für Daten aus Wohnraumüberwachungen und Online-Datenerhebungen, deren weitere Nutzung stets einen mit den Erhebungsvoraussetzungen vergleichbaren Gefahrengrad erfordern (vgl. BVerfGE 141, 220 Rn. 283).

- Nicht in jeder Hinsicht vergleichbar sind jedenfalls die Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle (vgl. BVerfGE 141, 220 Rn. 134 ff.). Die Arbeit der Nachrichtendienste erfolgt naturgemäß grundsätzlich verdeckt und unterliegt besonderen Regeln, etwa der in der Zusammenarbeit mit ausländischen Diensten einzuhaltenden Third-Party-Rule, nach der ausgetauschte Informationen ohne Zustimmung des Informationsgebers nicht an Dritte weitergegeben oder für andere Zwecke verwendet werden dürfen (vgl. BVerfGE 143, 101 Rn. 162 ff.). Das nachrichtenspezifische Geheimhaltungsinteresse hat Verfassungsrang und wird in Art. 10 Abs. 2 Satz 2 und Art. 45d GG ausdrücklich anerkannt. Daher kann es beispielsweise verfassungsrechtlich gerechtfertigt sein, dass sogar dem zur Geheimhaltung verpflichteten Parlamentarischen Kontrollgremium bestimmte Informationen vorenthalten werden (vgl. BVerfG NVwZ 2017, 1364 Rn. 119 ff.). Im Übrigen nimmt das BVerfG im BKAG-Urteil Bezug auf die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates 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 und zur Aufhebung des Rahmenbeschlusses 2008/977/JI (ABl. L 119 vom 4. Mai 2016, S. 89) (vgl. BVerfGE 141, 220 Rn. 134, 138). Diese Richtlinie findet jedoch keine Anwendung auf das Recht der Nachrichtendienste, da die nationale Sicherheit in der alleinigen Verantwortung der Mitgliedstaaten verblieben ist (Art. 4 Abs. 2 Satz 3 EU-Vertrag, Art. 2 Abs. 3 Buchst. a Richtlinie (EU) 2016/680). Eine Transformation unionsrechtlich vorgegebener Standards in das nationale Recht der Nachrichtendienste ist deshalb nicht geboten.

2. Die Ständige Konferenz der Innenminister und –senatoren der Länder (IMK) hat in ihrer 207. Sitzung am 7./8. Dezember 2017 über einen „harmonisierten Rechtsrahmen mit wirksamen Befugnissen“, der zuvor von der Arbeitsgruppe des AK IV „Harmonisierung wirksamer Verfassungsschutzbefugnisse in Bund und Ländern“ unter Federführung des Bundesministeriums des Innern entwickelt worden ist, Beschluss gefasst (TOP 29). Danach zeigt der dem Beschluss zugrunde liegende Bericht des Bundes und der Länder gesetzgeberische Optionen für den Bereich der Aufklärung extremistischer und terroristischer Bestrebungen auf. Die IMK empfiehlt Bund und Ländern, den Bericht in Überlegungen zur Novellierung ihrer Verfassungsschutzgesetze einzubeziehen.

## **II. Wesentlicher Inhalt des Gesetzentwurfs**

Über die bereits im Änderungsantrag vom 1. Juni 2016 (LT-Drs. 17/11609) gezogenen Konsequenzen hinaus nimmt der Gesetzentwurf nach den o.g. Leitlinien weitere Anpassungen vor. Gleichzeitig greift er Regelungsideen des harmonisierten Rechtsrahmens der IMK auf. Im Einzelnen:

- Im Hinblick auf die Gewährleistung einer datenschutzrechtlichen Kontrolle werden die in Art. 7 Abs. 2 enthaltenen Fristen so angepasst, dass ihre Verfügbarkeit im Rahmen der datenschutzrechtlichen Kontrolle, die alle zwei Jahre stattfindet, gewährleistet ist.

- Im neuen Art. 8a wird eine allgemein und grundsätzlich für alle nachrichtendienstlichen Mittel geltende Regelung zum Kernbereichs- und Berufsgeheimnisträgerschutz geschaffen. Dabei werden Rechtsanwälte und Kammerrechtsbeistände den Strafverteidigern gleichgestellt.
- Ferner wird als neuer Art. 8b der allgemeine Grundsatz der Zweckbindung gesetzlich normiert, der prinzipiell bei jeder zweckändernden Weiterverarbeitung von Daten, die mit nachrichtendienstlichen Mitteln gewonnen wurden, durch das Landesamt für Verfassungsschutz zu beachten ist. Bereits existierende besondere Zweckbindungen hinsichtlich personenbezogener Daten aus Wohnraumüberwachungen, Online-Datenerhebungen und den Auskunftersuchen gemäß Art. 15 Abs. 2 und 3 sowie Art. 16 werden im Interesse einer normenklaren Systematik in Art. 8b an einer zentralen Stelle zusammengezogen.
- Die gesetzliche Befugnis zur Wohnraumüberwachung wird in mehrfacher Hinsicht modifiziert: So erfolgt eine ausdrückliche Differenzierung zwischen akustischer und optischer Wohnraumüberwachung. Aufgenommen wird auch ein – die vorherige richterliche Anordnung voraussetzendes – Betretungsrecht zur Vorbereitung und Durchführung der Maßnahme. Außerdem erfolgt eine maßnahmespezifische Konkretisierung des Adressatenkreises dahingehend, dass die Maßnahme primär in der Wohnung der Zielperson zu erfolgen hat und in Wohnungen anderer Personen nur subsidiär unter erhöhten Anforderungen durchgeführt werden darf.
- Aufgrund des im Gesetz angelegten Gleichlaufs gelten die Eingriffsvoraussetzungen der Wohnraumüberwachung auch für die Online-Datenerhebung. Der Adressatenkreis bedarf allerdings einer maßnahmespezifischen Ausgestaltung.
- Die in Art. 15 Abs. 2 Satz 2 für Auskunftersuchen im Schutzbereich von Art. 10 GG und Art. 112 BV normierte erhöhte Eingriffsschwelle ist

verfassungsrechtlich nicht geboten und wird im Einklang mit dem harmonisierten Rechtsrahmen der IMK gestrichen.

- Die Übermittlungsvorschriften werden mit Blick auf den Grundsatz der hypothetischen Datenneuerhebung dahingehend konkretisiert, dass jeweils für die in der Übermittlung liegende Zweckänderung tatsächliche Anhaltspunkte im Sinne eines konkreten Spurenansatzes vorliegen müssen. Ferner wird sichergestellt, dass bei Übermittlungen ins Ausland ein hinreichender rechtsstaatlicher Umgang mit den Daten im Empfängerstaat zu erwarten ist. Über Auslandsübermittlungen an Drittstaaten ist zudem künftig dem Parlamentarischen Kontrollgremium jährlich zu berichten.

## **B. Zwingende Notwendigkeit einer normativen Regelung**

Soweit der Gesetzentwurf Leitlinien aus der Rechtsprechung des BVerfG umsetzt, handelt es sich um zwingende Vorgaben aus höherrangigem Recht. Das gleichzeitige Aufgreifen von Regelungsimpulsen des harmonisierten Rechtsrahmens der IMK ist im Interesse einer stärkeren Vereinheitlichung der gesetzlichen Grundlagen von Bund und Ländern im Verfassungsschutzverbund zweckmäßig. Die stärkere Harmonisierung mit Bundesrecht gehörte zu den zentralen Zielen der Novelle des Bayerischen Verfassungsschutzgesetzes von 2016 (vgl. LT-Drs. 17/10014 S. 14; 17/11609 S. 18 f.). Anhand dieser Zielsetzung ist das Gesetz konsequent weiterzuentwickeln. Der von der IMK entwickelte harmonisierte Rechtsrahmen enthält insoweit wesentliche Richtungsvorgaben, die innerhalb des Verfassungsschutzverbundes weitestgehend konsensfähig sind.

## **C. Zu den Vorschriften im Einzelnen**

### ***Zu § 1 (Änderung des Bayerischen Verfassungsschutzgesetzes)***

#### Zu Nr. 1 (Art. 7 Abs. 2 Satz 2)

Nach der Rechtsprechung des BVerfG setzt die Verhältnismäßigkeit von heimlichen Überwachungsmaßnahmen voraus, dass der Gesetzgeber eine effektive aufsichtliche Kontrolle gewährleistet (BVerfGE 141, 220 Rn. 140 f., 205, 246, 272). Dazu gehöre es, die Frist zur Aufbewahrung derjenigen Daten, die der aufsichtlichen Kontrolle dienen, so lange zu bemessen, dass sie im Rahmen der nächsten anstehenden Kontrolle durch den Landesbeauftragten für Datenschutz noch vorliegen. Demgemäß wird in Art. 7 Abs. 2 Satz 2 nun eine Höchstfrist für die Aufbewahrung von drei Jahren festgelegt. Eine Löschung erfolgt dadurch nicht vor Abschluss der nach Art. 28 Abs. 2 (in der Fassung des derzeit im Gesetzgebungsverfahren befindlichen neuen Bayerischen Datenschutzgesetzes) im zweijährigen Turnus durchzuführenden Datenschutzkontrolle. Nach Abschluss der Kontrolle sind die Daten zu löschen, es sei denn dass besondere Gründe der Geheimhaltung oder des Geheimschutzes eine längere Frist gebieten. Letzteres entspricht der geltenden Rechtslage.

#### Zu Nr. 2 (Art. 8)

Die Streichung in Abs. 2 ist eine Folgeänderung zum neuen Art. 8a. Da der Kernbereichsschutz nach Art. 8a des Entwurfs künftig allgemein gelten soll, bedarf es der in Abs. 2 verpflichtend vorgegebenen näheren Regelung in der Dienstvorschrift über nachrichtendienstliche Mittel nicht mehr.

#### Zu Nr. 3 (Art. 8a und Art. 8b)

Der neu eingefügte Art. 8a enthält eine allgemeine Regelung zum Schutz des Kernbereichs privater Lebensführung und der Berufsgeheimnisträger im Rahmen des Einsatzes nachrichtendienstlicher Mittel. Der harmonisierte Rechtsrahmen der IMK sieht gleichfalls eine allgemein gültige Klausel für den Kernbereichs- und Berufsgeheimnisträgerschutz vor.

Nach der Rechtsprechung des BVerfG beansprucht der Kernbereich privater Lebensgestaltung gegenüber allen Überwachungsmaßnahmen Beachtung, weshalb der Gesetzgeber Regelungen schaffen müsse, die einen wirksamen Schutz normenklar gewährleisten (BVerfGE 141, 220 Rn. 123 m.w.N.). Auch wenn das BVerfG im BKAG-Urteil eine eigene gesetzliche Regelung nur für „verletzungsgeneigte Befugnisse“ gefordert hat, die „typischerweise zur Erhebung kernbereichsrelevanter Daten führen“, und die Maßstäbe des BKAG-Urteils nicht unmittelbar auf das Recht der Nachrichtendienste übertragbar sind, soll nun in Abs. 1 eine allgemeine Regelung für alle nachrichtendienstlichen Mittel geschaffen werden. Diese gilt für die allgemeinen nachrichtendienstlichen Mittel i.S.v. Art. 8 Abs. 1 Satz 1 ebenso wie für die besonderen nachrichtendienstlichen Mittel gemäß Art. 9 bis 19, soweit nicht spezielle Regelungen getroffen sind. Solche vorrangigen Regelungen sind bei der Online-Datenerhebung in Art. 10 Abs. 2 Nr. 3, der Telekommunikationsüberwachung in § 4 Abs. 4 G 10 sowie bei Auskunftersuchen nach Art. 15 Abs. 2 und 3 und Art. 16 durch den Verweis im neuen Art. 8b Abs. 3 (derzeit Art. 17 Abs. 2 Satz 1) auf § 4 Abs. 4 G 10 vorgesehen.

Der Gesetzgeber ist nach Ansicht des BVerfG nicht verpflichtet, bestimmte Personengruppen von Überwachungsmaßnahmen von vornherein auszunehmen (BVerfGE 141, 220 Rn. 132). Gleichwohl wird nun in Abs. 1 Satz 1 Nr. 2 und Abs. 2 auch eine allgemeine Regelung zum Schutz von Berufsgeheimnisträgern eingeführt, die bei allen nachrichtendienstlichen Mitteln zu beachten ist. Schon im Rahmen des Gesetzgebungsverfahrens zur Novellierung des Bayerischen Verfassungsschutzgesetzes 2016 war darauf hingewiesen worden (LT-Drs. 17/11609 S. 19), dass die in § 3b G 10 vorgenommene Differenzierung zwischen Strafverteidigern und sonstigen Rechtsanwälten, die im Wege der dynamischen Verweisung zugrunde gelegt wurde, nicht sachgerecht ist. Angesichts dessen, dass eine bundesgesetzliche Änderung derzeit noch nicht absehbar ist, erfolgt nun eine eigene landesrechtliche Regelung, durch die Rechtsanwälte und Kammerrechtsbeistände den Strafverteidigern gleichgestellt werden.

Bei technischen Maßnahmen gilt nach Abs. 1 Satz 5 die Regelung in § 3a Satz 3 bis 7 des Artikel 10-Gesetzes (G10) entsprechend. Zu den technischen Maßnahmen

gehören insbesondere die Wohnraumüberwachung (Art. 9) und die Online-Datenerhebung (Art. 10). Soweit durch den Verweis auf § 3a Satz 4 bis 6 G 10 eine Entscheidung der G 10-Kommission über die Verwertbarkeit der erhobenen personenbezogenen Daten herbeizuführen ist, ergibt sich bereits aus dem klaren Wortlaut, der insoweit keine Einschränkung vornimmt, dass die Daten vollständig vorzulegen sind. Aus § 3a Satz 3 G 10 folgt zudem eindeutig („nur“), dass die Daten nach Möglichkeit ohne vorherige Kenntnisnahme der G 10-Kommission vorzulegen sind. Aus der Verweisung ausgenommen sind die Regelungen zur Dokumentation und Löschung gemäß § 3a Satz 9 bis 12 G 10, da insoweit bereits in Art. 7 dem Erfordernis einer effektiven datenschutzrechtlichen Kontrolle entsprechende allgemeine Regelungen vorgesehen sind.

Der neue Art. 8b stellt den zentralen Grundsatz der Zweckbindung als allgemeine Norm voran, die für jede Verarbeitung von personenbezogenen Daten, die mit nachrichtendienstlichen Mitteln gewonnen wurden, zu beachten ist. Das BVerfG hat insoweit ausgeführt (vgl. BVerfGE 141, 220 Rn. 281 ff.), dass es nicht von vornherein dem Gebot einer dem ursprünglichen Erhebungszweck entsprechenden Verwendung widerspreche, wenn die weitere Nutzung solcher Daten bei Wahrnehmung derselben Aufgabe auch unabhängig von weiteren gesetzlichen Voraussetzungen als bloßer Spurenansatz erlaubt wird. Es komme demnach darauf an, dass die erhebungsberechtigte Behörde die Daten im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutzt, wie es die jeweilige Datenerhebungsvorschrift erlaubt. Hinsichtlich der Nutzung der Daten zu anderen Zwecken als denen der ursprünglichen Datenerhebung komme es darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben neu auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln erhoben werden dürften (Kriterium der hypothetischen Datenneuerhebung). Dies gelte allerdings nicht schematisch abschließend und schließe die Berücksichtigung weiterer Gesichtspunkte nicht aus. So stehe die Tatsache, dass die Zielbehörde bestimmte Datenerhebungen, zu denen die Ausgangsbehörde berechtigt ist, ihrerseits wegen ihres Aufgabenspektrums nicht vornehmen darf,

einem Datenaustausch nicht prinzipiell entgegen. Auch könnten Gesichtspunkte der Vereinfachung und der Praktikabilität bei der Schaffung von Übermittlungsvorschriften es rechtfertigen, dass nicht alle Einzelanforderungen, die für die Datenerhebung erforderlich sind, in gleicher Detailliertheit für die Übermittlung der Daten gelten. Nicht in jedem Fall identisch seien die Voraussetzungen einer Zweckänderung mit denen einer Datenerhebung hinsichtlich des erforderlichen Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts.

Verfassungsrechtlich geboten, aber regelmäßig auch ausreichend, sei insoweit, dass sich aus den Daten – sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde – ein konkreter Ermittlungsansatz ergibt.

Abs. 1 überträgt diese Grundsätze auf den Aufgabenbereich des Verfassungsschutzes. Sämtliche der in Art. 5 Abs. 1 Satz 1 genannten Zwecke liegen nach Art. 3 im selben Aufgabenspektrum und haben verfassungsrechtlich ein vergleichbares Gewicht. Innerhalb der in Art. 5 Abs. 1 Satz 1 genannten Zwecke sind daher Zweckänderungen ohne Weiteres möglich; für die zweckändernde Weiterverarbeitung genügen tatsächliche Anhaltspunkte dafür, dass die Daten für den neuen Zweck geeignet sind. Auf die in der jeweiligen Erhebungsbefugnis vorausgesetzte Gefahrenlage kommt es nicht an. Demgemäß können gemäß Satz 1 personenbezogene Daten, die für einen bestimmten Erhebungszweck im Sinne von Art. 5 Abs. 1 Satz 1 erhoben wurden, für jeden anderen der in Art. 5 Abs. 1 Satz 1 genannten Zwecke als Spurenansatz weiterverarbeitet werden. Beispielsweise dürfen auf dieser Grundlage die im Rahmen der zulässigen Ortung eines Mobilfunkendgeräts nach Art. 12 gewonnenen Daten zum Schutz sämtlicher von Art. 3 umfassten Rechtsgüter weiterverarbeitet werden, ohne dass es darauf ankäme, dass die in Art. 12 Abs. 1 vorausgesetzte „schwerwiegende Gefahr“ vorliegt.

Im Ergebnis können daher sämtliche Informationen, die zum Schutz der von Art. 3 umfassten Rechtsgüter erhoben wurden, für die Aufgabenerfüllung im Rahmen des Verfassungsschutzverbunds weiterverarbeitet werden; Besonderheiten gelten lediglich für personenbezogene Daten, die aufgrund von Befugnisnormen erhoben wurden, die an qualifizierte Eingriffsschwellen anknüpfen. Insoweit ist sicherzustellen, dass der geänderte Verarbeitungszweck mindestens dem Schutz eines vergleichbar



gewichtigen Rechtsguts dient. Diesen Grundsatz bringt Satz 2 in allgemeiner Form zum Ausdruck. Für die zweckändernde Übermittlung an andere Stellen gelten die Regelungen des Art. 25, die insoweit dem allgemeinen Grundsatz des Art. 8b Abs. 1 als *lex specialis* vorgehen.

Für die Maßnahmen der Wohnraumüberwachung, der Online-Datenerhebung, der Telekommunikationsüberwachung und der Auskunftersuchen im Schutzbereich des Brief-, Post- und Fernmeldegeheimnisses, die an erhöhte Eingriffsschwellen gebunden sind, findet der allgemeine Grundsatz des Abs. 1 Satz 2 eine spezielle Ausprägung in den Abs. 2 und 3 sowie in § 4 G 10. Diese besonderen Zweckbindungen sind nach dem neu gefassten Art. 25 Abs. 4 Satz 1 auch bei der Übermittlung an andere Stellen zu beachten.

Besonderheiten gelten vor allem für personenbezogene Daten, die mittels Wohnraumüberwachung (Art. 9) oder Online-Datenerhebung (Art. 10) gewonnen wurden. Hier hat das BVerfG gesteigerte Voraussetzungen an die zweckändernde Weiterverarbeitung gestellt (BVerfGE 141, 220 Rn. 283), denen bereits die bisherige Regelung des Art. 11 Abs. 3 im Wesentlichen Rechnung trägt. Auch diese Regelung wird nun aus systematischen Gründen als Abs. 2 mit den allgemeinen Grundsätzen in einer Vorschrift zusammengezogen. Satz 1 entspricht inhaltlich weitgehend dem bisherigen Art. 11 Abs. 3. Allerdings wird in Nr. 2 künftig mit dem Erfordernis tatsächlicher Anhaltspunkte für eine dringende Gefahr eine der Nr. 1 entsprechende qualifizierte Gefahrenlage vorausgesetzt. In Nr. 3 wird die Weiterverarbeitung von Daten zur Verfolgung von Straftaten geregelt. Sollen Daten zu Zwecken der Strafverfolgung weiterverarbeitet werden, ist dies im Hinblick auf den Grundsatz der hypothetischen Datenneuerhebung nur zulässig, wenn die Daten auch mit den entsprechenden strafprozessualen Befugnissen erlangt werden könnten (vgl. BVerfGE 141, 220 Rn. 291 und 316). Die nunmehrige Formulierung orientiert sich an § 100e Abs. 6 Nr. 3 StPO. Dadurch werden die Vorschriften über die Weiterverarbeitung zu repressiven Zwecken auf Bundes- und Landesebene weiter vereinheitlicht.

Wurde die Maßnahme nach Art. 9 oder 10 nur zur Eigensicherung auf Anordnung der Behördenleitung durchgeführt (Art. 11 Abs. 4 Satz 1), dürfen dabei gewonnene Erkenntnisse nach der Verfahrensvorschrift des Art. 11 Abs. 4 Satz 2 grundsätzlich nur weiterverarbeitet werden, wenn zuvor der Richter festgestellt hat, dass die Maßnahme rechtmäßig ist und die Voraussetzungen des Art. 9 Abs. 1 Satz 1 vorliegen. In Eilfällen hat die Behördenleitung eine vorläufige Entscheidung zu treffen (Art. 11 Abs. 1 Satz 2, Abs. 4 Satz 2 Halbsatz 2).

Ferner wird als neuer Satz 2 die Vorgabe des BVerfG aus dem BKAG-Urteil umgesetzt, dass Lichtbilder und Bildaufzeichnungen nicht zu Strafverfolgungszwecken weiterverarbeitet werden dürfen (BVerfGE 141, 220 Rn. 317). Da diese Vorgabe unmittelbar daraus hergeleitet wurde, dass Art. 13 Abs. 3 GG für die Strafverfolgung nur den Einsatz der akustischen Wohnraumüberwachung erlaubt, beansprucht sie unterschiedslos für Polizeibehörden und Nachrichtendienste Geltung.

Für Maßnahmen im Schutzbereich des Art. 10 GG und Art. 112 BV besteht in § 4 G 10 eine bundeseinheitliche Spezialvorschrift, die entsprechend für Auskunftersuchen nach Art. 15 Abs. 2 und 3 sowie Art. 16 gilt. Die entsprechende Verweisung im bisherigen Art. 17 Abs. 2 Satz 1 wird zur Verdeutlichung der Systematik als Abs. 3 vorangestellt.

#### Zu Nr. 4 (Art. 9)

Die Befugnis zum verdeckten Einsatz technischer Mittel in Wohnungen wird nach folgenden Maßgaben neu gefasst:

In Abs. 1 Satz 1 werden die akustische und die optische Wohnraumüberwachung, wie vom BVerfG für den Polizeibereich gefordert (BVerfGE 141, 220 Rn. 185), als eigene und damit auch eigens zu prüfende Überwachungsmaßnahmen ausgestaltet. Dadurch wird sichergestellt, dass das größere Eingriffsgewicht, das einer Verbindung von akustischer und optischer Wohnraumüberwachung zukommt, im Rahmen der Verhältnismäßigkeitsprüfung hinreichend berücksichtigt wird.

Nr. 3 sieht nun vor, dass es nicht mehr auf den bedeutenden Wert der Sache ankommt, sondern darauf, ob die Erhaltung der Sache im besonderen öffentlichen Interesse liegt. Sachen, die im besonderen öffentlichen Interesse liegen, sind nicht zwangsläufig mit einem besonderen monetären Wert verbunden. Ein solcher kann freilich ein Indiz für ein besonderes öffentliches Interesse darstellen.

In Satz 2 wird aus Gründen der Rechtssicherheit das als Annexkompetenz vom parlamentarischen Gesetzgeber (vgl. LT-Drs. 15/10313 S. 25) anerkannte (und bis zum 31. Juli 2009 in Art. 6g enthaltene) Betretungsrecht zur Vorbereitung und Durchführung der Maßnahme einer neuerlichen gesetzlichen Regelung zugeführt. Ein solches ist auch im harmonisierten Rechtsrahmen der IMK vorgesehen. Durch entsprechende Geltung des § 3 Abs. 2 Satz 1 G 10 wird dem Verhältnismäßigkeitsgrundsatz Rechnung getragen.

Die Streichung des bisherigen Satzes 2 ist eine Folgeänderung: der Kernbereichs- und Berufsgeheimnisträgerschutz ist in den neuen Art. 8a vorgezogen. Der Verweis auf § 3 Abs. 2 Satz 2 bis 4 G 10 entfällt, da die Adressatenregelung in Abs. 2 spezifisch gefasst ist. Der Verweis auf § 3 Abs. 2 Satz 1 G 10 wird als Satz 3 des Abs. 1 beibehalten.

Abs. 2 legt im Einzelnen den Adressatenkreis der Maßnahme fest. Der harmonisierte Rechtsrahmen der IMK trifft ebenso bei der Wohnraumüberwachung eine spezifische Adressatenregelung.

Nach Satz 1 darf sich die Maßnahme nur gegen die Zielperson, also diejenige Person, die für die Gefahr verantwortlich ist, richten und nur in deren Wohnung durchgeführt werden (vgl. BVerfGE 141, 220 Rn. 115, 187).

Satz 2 trägt den strengen Vorgaben des BVerfG für den verdeckten Einsatz technischer Mittel in Wohnungen anderer Personen Rechnung. Danach bedarf es eines konkretisierten Verdachts, dass sich die Zielperson zur Zeit der Maßnahme in der Wohnung des Dritten aufhält (vgl. BVerfGE 141, 220 Rn. 115, 188). Dies ist gegebenenfalls durch andere Maßnahmen, wie eine Observation, sicherzustellen. Nicht auf konkrete Anhaltspunkte gestützte Vermutungen für die Anwesenheit der Zielperson in der Wohnung des Dritten reichen für den Beginn der Maßnahme nicht

aus. Darüber hinaus muss eine hinreichende Wahrscheinlichkeit bestehen, hierbei verfahrensrelevante Informationen zu gewinnen. Erforderlich sind auch insoweit tatsächliche Anhaltspunkte dafür, dass die Zielperson in den zu überwachenden Räumlichkeiten im Überwachungszeitraum verfahrensrelevante und im weiteren Verfahren verwertbare Gespräche führen wird.

#### Zu Nr. 5 (Art. 10)

- a) Über den umfassenden Rechtsgrundverweis in Abs. 1 auf Art. 9 Abs. 1 („nach Maßgabe“) gelten die dort genannten Regelungen auch bei der Online-Datenerhebung. Dies gilt insbesondere auch für das in Art. 9 Abs. 1 Satz 2 normierte Betretungsrecht von Wohnungen zur Vorbereitung und Durchführung der Maßnahme. Wie das BVerfG im BKAG-Urteil ausgeführt hat, ist der Gesetzgeber nicht gehindert, die maßgebliche Schwelle für den Rechtsgüterschutz bei der Wohnraumüberwachung und bei der Online-Datenerhebung einheitlich zu bestimmen (BVerfGE 141, 220 Rn. 108).
- b) In Abs. 2 wird eine neue Nr. 3 angefügt, die dem Schutz des Kernbereichs privater Lebensführung bereits auf der Erhebungsebene dient. Sie sieht vor, dass durch technische Maßnahmen, soweit möglich, sicherzustellen ist, dass Daten aus dem Kernbereich privater Lebensgestaltung bereits nicht erhoben werden. Ein entsprechender Regelungsvorschlag findet sich auch im harmonisierten Rechtsrahmen der IMK.
- c) Der Adressatenkreis wird im neuen Abs. 3 in Parallele zur Wohnraumüberwachung (Art. 9 Abs. 2) maßnahmespezifisch gefasst. Der harmonisierte Rechtsrahmen der IMK sieht bei der Online-Datenerhebung ebenfalls eine spezifische Adressatenregelung vor.

Die Online-Datenerhebung ist nur gegen die Zielperson zulässig und darf nur durch Zugriff auf deren informationstechnisches System durchgeführt werden. Der Zugriff auf informationstechnische Systeme anderer ist nur unter erhöhten Anforderungen zulässig. Erforderlich sind tatsächliche Anhaltspunkte dafür, dass die Zielperson dort ermittlungsrelevante Informationen speichert und ein

auf ihre eigenen informationstechnischen Systeme beschränkter Zugriff zur Erreichung des Ermittlungsziels nicht ausreicht (vgl. BVerfGE 141, 220 Rn. 115).

#### Zu Nr. 6 (Art. 11)

- a) Die Streichung des Abs. 3 ist eine Folgeänderung zum neuen Art. 8b Abs. 3.
- b) Die Änderung des Art. 9 macht eine Folgeänderung im bisherigen Abs. 4 notwendig, der nun zu Abs. 3 wird.
- c) Der bisherige Abs. 5 wird infolge der Streichung des Abs. 3 zu Abs. 4.

#### Zu Nr. 7 (Art. 13 Abs. 1 und 2)

- a) Durch die Änderung von Abs. 1 Satz 1 wird klargestellt, dass Maßnahmen der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) nicht ihrerseits über eine dynamische Verweisung an die Tatbestandsvoraussetzungen des § 3 G 10 genknüpft sind, vielmehr die Quellen-TKÜ als Vorbereitungsmaßnahme zur eigentlichen Telekommunikationsüberwachung, die nach den Vorschriften des Artikel 10-Gesetzes durchzuführen und dort bundeseinheitlich geregelt ist, akzessorisch ist. Die Quellen-TKÜ ist nur bei einer nach dem Artikel 10-Gesetz angeordneten oder zeitgleich mit einer angeordneten Telekommunikationsüberwachung zulässig.

Wie in Art. 9 Abs. 1 Satz 2 wird auch hier in Satz 2 ein Betretungsrecht zur Vorbereitung und Durchführung der Maßnahme einer klaren gesetzlichen Regelung zugeführt.

- b) In Abs. 2 werden die Verweise auf die §§ 3a und 3b G 10 gestrichen, da der Kernbereichs- und Berufsgeheimnisträgerschutz in den allgemeinen Teil in den neuen Art. 8a vorgezogen werden. Die Streichung des § 4 G 10 bereinigt ein Redaktionsversehen. § 4 G 10 betrifft die Verarbeitung erhobener Daten, Art. 13 stellt jedoch nur eine Vorbereitungsmaßnahme der Telekommunikationsüberwachung dar, sodass eine Verarbeitungsregelung entbehrlich ist.

Zu Nr. 8 (Art. 15 Abs. 2 und 3)

- a) Die erhöhten Eingriffsvoraussetzungen in Abs. 2 Satz 2 sind verfassungsrechtlich nicht geboten. Das BVerfG hat in seiner Entscheidung zur Online-Durchsuchung (BVerfGE 120, 274/348 f.) ausgeführt, dass das Erfordernis tatsächlicher Anhaltspunkte für eine schwerwiegende Gefahr hinreichend sicherstelle, dass nicht jeder vage Verdacht, bestimmte Gruppierungen könnten sich gegen die freiheitliche demokratische Grundordnung richten, zu einer Erhebung von Kontoinhalten und Kontobewegungen ausreiche. Die Aussage des BVerfG bezog sich unmittelbar auf Auskunftersuchen gegenüber Kreditinstituten über Kontoinhalte und Kontobewegungen wie sie in Art. 16 Abs. 1 Nr. 2 geregelt sind. Wie allerdings die Evaluierung der entsprechenden Befugnisse in § 8a Abs. 2 Satz 1 BVerfSchG gezeigt hat, ist die Eingriffswirkung bei Auskunftersuchen gegenüber Luftfahrtunternehmen und Kreditinstituten mit derjenigen bei Anfragen zu Verkehrsdaten gegenüber Telekommunikations- und Telemediendienstleistern vergleichbar, weshalb der Bundesgesetzgeber insoweit auch einheitliche rechtliche Anforderungen festgelegt hat (vgl. BT-Drs. 17/6925 S. 15). Deshalb ist es gerechtfertigt, den vom BVerfG formulierten verfassungsrechtlichen Maßstab auf alle Auskunftersuchen von Art. 15 und 16 zu erstrecken. Der harmonisierte Rechtsrahmen der IMK sieht ebenfalls keine erhöhte Eingriffsschwelle vor.

Die in Abs. 2 Satz 2 enthaltene Eingriffsschwelle für Auskunftersuchen bei Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben, ist folglich verfassungsrechtlich nicht geboten und wird gestrichen

- b) Der Verweis in Abs. 3 Satz 2 auf § 3b G 10 ist entbehrlich, da der Berufsgeheimnisträgerschutz die allgemeine Bestimmung des Art. 8a vorgezogen wurde.

Zu Nr. 9 (Art. 17 Abs. 2 Satz 1)

- a) Folgeänderung zum neuen Art. 8b Abs. 3.
- b) Folgeänderung zur Streichung des Satzes 2 in Art. 15 Abs. 2.

Zu Nr. 10 (Art. 20 Abs. 1 Nr. 2)

Die parlamentarische Kontrolle wird auf Datenübermittlungen an Drittstaaten (Art. 25 Abs. 3 Satz 1 Nr. 1 und 2) erstreckt, soweit sie der Verfügungsberechtigung des Landesamts unterliegen (vgl. BVerfGE 141, 220 Rn. 354). Die Berichtspflicht gilt nur für Übermittlungen durch das Landesamt für Verfassungsschutz an ausländische Stellen. Übermittlungen aus dem Ausland an das Landesamt für Verfassungsschutz sind demgegenüber nicht berichtspflichtig, da diese regelmäßig der Third-Party-Rule unterliegen. Im Normtext wird dies dadurch deutlich, dass die Berichtspflicht nur für Übermittlungen gilt, die der Verfügungsberechtigung des Landesamts unterliegen. Dies entspricht der in Art. 6 Abs. 1 PKGG enthaltenen Rechtslage. Nach der Third-Party-Rule dürfen ausgetauschte Informationen ohne Zustimmung des Informationsgebers nicht an Dritte weitergegeben oder für andere Zwecke verwendet werden. Dieser Grundsatz gilt regelmäßig auch gegenüber Kontrollorganen des Parlaments und selbst gegenüber Aufsichtsbehörden (Wills/Born in Born/Leigh/Wills, *International Intelligence Cooperation and Accountability*, 2011, 277/283; a.A. Gärditz DVBl 2015, DVBl. 2015, 903/907). Es handelt sich um eine auch vom BVerfG anerkannte Verhaltensregel der internationalen Kooperation im Sicherheits- und Nachrichtendienstbereich (BVerfGE 143, 101 Rn. 165), die in Art. 4 Buchst. d und Art. 5 Buchst. b des Abkommens zwischen der Europäischen Union und der Nordatlantikvertrags-Organisation über den Geheimschutz vom 14. März 2003 (ABl. L 80, 36 ff.) ausdrücklich erwähnt ist.

Die Berichterstattung erfolgt wie bei den in Art. 20 Abs. 1 Satz 1 Nr. 2 Buchst. a und b genannten Maßnahmen in Form eines Lageberichts. Auch insoweit ist selbstverständlich die Third-Party-Rule einzuhalten. Ging der Übermittlung durch das Landesamt für Verfassungsschutz an eine ausländische Stelle eine Anfrage derselben voraus, kann die Third-Party-Rule einer Berichterstattung entgegenstehen.

Zu Nr. 11 (Art. 21 Abs. 1 Satz 2)

Es handelt sich um eine Klarstellung der Formulierung ohne materielle Änderung.

Zu Nr. 12 (Art. 23 Abs. 1 Satz 3)

Die Änderung ist eine notwendige Konsequenz der Änderung des Art. 21 Abs. 1 Satz 2 für solche Unterlagen, die durch eine entsprechende technische Zugriffsbeschränkung dem Zugriff der Facharbeit entzogen sind und ausschließlich noch für das Hauptstaatsarchiv aufbewahrt werden.

Zu Nr. 13 (Art. 25)

- a) Nach den Ausführungen des BVerfG im BKAG-Urteil muss die in der Übermittlung von personenbezogenen Daten an andere Behörden liegende Zweckänderung den Anforderungen des Grundsatzes der hypothetischen Datenneuerhebung genügen (BVerfGE 141, 220 Rn. 304 ff.). Erforderlich ist insbesondere das Vorliegen eines konkreten Ermittlungsansatzes im Aufgabenbereich des Empfängers (vgl. BVerfGE 141, 320 Rn. 320). Dem trägt die Ergänzung des Erfordernisses „tatsächliche Anhaltspunkte“ in Abs. 1 Rechnung.

Durch die neu eingefügte Nr. 2 werden repressive Zwecke systematisch klar von den in Nr. 1 geregelten präventiven Übermittlungszwecken getrennt. Gleichzeitig wird klargestellt, dass der repressive Übermittlungszweck sich nicht auf die Strafverfolgung im engeren Sinn, also das strafrechtliche Ermittlungsverfahren beschränkt, sondern auch die an eine Verurteilung anschließenden Verfahrensabschnitte der Strafvollstreckung, des Strafvollzugs und des Gnadenverfahrens umfasst.

- b) Der neue Abs. 1a regelt die Auslandsübermittlung an Stellen in Mitgliedstaaten der Europäischen Union und an öffentliche Stellen von Staaten, die die Bestimmungen des Schengen-Besitzstandes anwenden. Hierfür gelten die gleichen Voraussetzungen wie bei der Inlandsübermittlung.



- c) Der Grundsatz der hypothetischen Datenneuerhebung gilt bei der Übermittlung an sämtliche öffentliche Stellen und damit auch für die Übermittlung zwischen Nachrichtendiensten und Polizei.

Im BKAG-Urteil hat der Erste Senat des BVerfG „eine konkretisierende Konsolidierung einer langen Rechtsprechung beider Senate des BVerfG“ vorgenommen und dabei ausweislich der hierzu zitierten Entscheidungen auch das ATDG-Urteil vom 24. April 2013 (BVerfGE 133, 277) einbezogen (BVerfGE 141, 220 Rn. 292). Während im ATDG-Urteil vorrangig die unterschiedlichen Aufgaben von Polizei und Nachrichtendiensten in den Blick genommen wurden, stellt das BKAG-Urteil in seinen Ausführungen zur hypothetischen Datenneuerhebung allein auf das verfassungsrechtliche Gewicht des geänderten Nutzungszwecks und das Vorliegen eines konkreten Ermittlungsansatzes ab. Den Ausführungen zur Übermittlungsbefugnis des BKA an die Verfassungsschutzbehörden und den Militärischen Abschirmdienst (BVerfGE 141, 220 Rn. 320) ist zu entnehmen, dass diese Kriterien auch für den Austausch von Daten zwischen Polizei und Nachrichtendiensten anzuwenden sind. Soweit im BKAG-Urteil „für die Datenübermittlung von Nachrichtendiensten an das Bundeskriminalamt“ auf das ATDG-Urteil hingewiesen wird (BVerfGE 133, 277 Rn. 123), bezieht sich dies eindeutig auf das zuvor genannte Erfordernis konkreter „Erkenntnisse zu einer Gefährdung hochrangiger Rechtsgüter“. Andernfalls wäre nicht verständlich, warum der entsprechende Einschub mitten im Satz an der entsprechenden Stelle zum Gewicht der Rechtsgüter erfolgt und nicht am Ende des gesamten Satzes. Folglich kommt es bei Übermittlungen an Polizeibehörden zum Zwecke der Gefahrenabwehr ebenfalls auf das Vorliegen entsprechender tatsächlicher Anhaltspunkte an. Dem trägt die Änderung von Abs. 2 Satz 1 Rechnung. Zur Klarstellung wird in der in Nr. 1 enthaltenen Aufzählung bedeutender Rechtsgüter die sexuelle Selbstbestimmung ergänzt. Dadurch wird insoweit ein Gleichlauf mit dem Polizeiaufgabengesetz (PAG) sichergestellt (vgl. Art. 11 Abs. 3 Satz 2 Nr. 3 PAG und die Entwurfsfassung des Art. 60 Abs. 3 PAG des

derzeit im Gesetzgebungsverfahren befindlichen PAG-Neuordnungsgesetzes). Wie im Rahmen von Art. 9 wird zudem hinsichtlich des Schutzes von Sachwerten das Erfordernis des erheblichen Werts durch den umfassenderen Begriff des „besonderen öffentlichen Interesses“ ersetzt (vgl. die Begründung zu Art. 9 Abs. 1 Satz 1 Nr. 3).

- d) In Abs. 3 werden die Übermittlungsvoraussetzungen an Dienststellen der Stationierungstreitkräfte, an andere ausländische öffentliche und an weitere Stellen sowie an nicht-öffentliche Stellen geregelt. Nach Ansicht des BVerfG gelten für die Übermittlung ins Ausland mit Blick auf die Achtung fremder Rechtsordnungen und -anschauungen eigene verfassungsrechtliche Bedingungen (vgl. BVerfGE 141, 220 Rn 324 ff., 329 ff.). Die Übermittlung von Daten ins Ausland setze eine Begrenzung auf hinreichend gewichtige Zwecke, für die die Daten übermittelt und genutzt werden dürfen, sowie die Vergewisserung über einen rechtsstaatlichen Umgang mit diesen Daten im Empfängerland voraus. Ferner sei eine wirksame inländische Kontrolle sicherzustellen.

Durch das in Nr. 2 und 3 aufgenommene Erfordernis der tatsächlichen Anhaltspunkte wird dem Erfordernis eines konkreten Ermittlungsansatzes für die Übermittlung Rechnung getragen.

Satz 2 schließt die Datenübermittlungen aus, wenn im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist oder sonst überwiegende schutzwürdige Interessen einer betroffenen Person entgegenstehen. Die Vorschrift entspricht inhaltlich § 78 Abs. 2 BDSG. In der Regel kann von der Zulässigkeit der Datenübermittlung ausgegangen werden, wenn die Europäische Kommission gemäß Art. 36 Abs. 3 der Richtlinie (EU) 2016/680 einen Angemessenheitsbeschluss gefasst hat. Die Nachrichtendienste fallen zwar nicht in den Anwendungsbereich dieser Richtlinie. Es gibt jedoch keinen Grund, der in Fällen, in denen die Europäische Kommission im Rahmen des Anwendungsbereichs der Richtlinie

die Angemessenheit festgestellt hat, für den nachrichtendienstlichen Bereich eine andere Bewertung rechtfertigen würde. Trotz Vorliegens eines Angemessenheitsbeschlusses bedarf es indes stets noch der Prüfung im Einzelfall, ob ausnahmsweise ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist. Dabei ist maßgeblich zu berücksichtigen, ob der Empfänger im Einzelfall einen angemessenen Schutz der übermittelten Daten garantiert. Im Übrigen gelten die Übermittlungsverbote des Art. 27, weshalb auch die schutzwürdigen Interessen des Betroffenen der Übermittlung im Einzelfall entgegenstehen können.

Der gesetzlichen Anordnung einer eigenen Dokumentationspflicht, wie sie in § 79 Abs. 2 BDSG geregelt ist, bedarf es angesichts des umfassend und damit auch für jede Informationsübermittlung geltenden Grundsatzes der Nachvollziehbarkeit gemäß Art. 7 nicht.

- e) Der bislang in Abs. 4 Satz 1 enthaltene Richtervorbehalt entfällt, da er verfassungsrechtlich nicht geboten ist. Die neue Fassung stellt klar, dass die besonderen Zweckbindungen nach Art. 8b Abs. 2 und 3 auch bei Übermittlungen an andere Stellen zu beachten sind.

#### Zu Nr. 14 (Art. 27 Abs. 2 Satz 1 Nr. 1)

Wie bei Art. 9 Abs. 1 Satz 1 Nr. 3 und Art. 25 Abs. 2 Satz 1 Nr. 1 wird künftig auch im Rahmen der für die Annahme eines Übermittlungsverbots i.S.v. Art. 27 Abs. 1 Nr. 1 und 2 maßgeblichen Interessenabwägung, soweit eine gegenwärtige Gefahr für Sachwerte im Raum steht, entscheidend darauf abgestellt, ob die Erhaltung der Sachen im besonderen öffentlichen Interesse geboten ist (vgl. die Begründung zu Art. 9 Abs. 1 Satz 1 Nr. 3).

#### **Zu § 2 (Einschränkung von Grundrechten)**

Das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG gilt nach der Rechtsprechung des BVerfG auch für die Änderung eines Gesetzes, die zu neuen Grundrechtseinschränkungen führt (BVerfGE 113, 348/366).

**Zu § 3 (Inkrafttreten)**

Gemäß Art. 76 Abs. 2 der Verfassung muss in jedem Gesetz der Tag bestimmt werden, an dem es in Kraft tritt.