



## **Gesetzentwurf**

der Landesregierung

**Entwurf eines Gesetzes zur Änderung des Landesverwaltungsgesetzes und des Landesverfassungsschutzgesetzes - Anpassung des manuellen Abrufs der Bestandsdaten nach dem Telekommunikationsgesetz an die verfassungsrechtlichen Vorgaben**

**Federführend ist das Innenministerium**

**Gesetzentwurf der Landesregierung**  
**Entwurf eines Gesetzes zur Änderung des Landesverwaltungsgesetzes und**  
**des Landesverfassungsschutzgesetzes - Anpassung des manuellen Abrufs der**  
**Bestandsdaten nach dem Telekommunikationsgesetz**  
**an die verfassungsrechtlichen Vorgaben**

**A. Problem**

Das Bundesverfassungsgericht (BVerfG) hat mit Beschluss vom 24. Januar 2012 (1 BvR 1299/05) eine Verfassungsbeschwerde gegen die gesetzlichen Bestimmungen des Telekommunikationsgesetzes (TKG) über die Verpflichtung geschäftsmäßiger Anbieter von Telekommunikationsdiensten zur Speicherung (§ 111 TKG) und Verwendung von Kundendaten (Bestandsdaten), insbesondere zu ihrer Beauskunftung im Wege des automatisierten oder manuellen Auskunftsverfahrens (§§ 112, 113 TKG) im Wesentlichen zurückgewiesen. Es hat jedoch festgestellt, dass die beschwerten Regelungen, soweit sie den verfassungsrechtlichen Vorgaben nicht entsprechen, übergangsweise bis längstens Ende Juni 2013 angewendet werden dürfen. Bis dahin müssen der Bundesgesetzgeber für seinen und die Landesgesetzgeber für ihren Kompetenzbereich die vom BVerfG kritisierten Normen und angemahnten Neuregelung den verfassungsrechtlichen Vorgaben anpassen.

Das automatisierte Auskunftsverfahren nach § 112 TKG hat das BVerfG nicht bemängelt. Hingegen hat es zum manuellen Auskunftsverfahren nach § 113 TKG drei Änderungen gefordert.

Erstens: Nach dem „Doppeltürenmodell“ kann der Bundesgesetzgeber im TKG nur die Befugnis bzw. Verpflichtung der Telekommunikationsdiensteanbieter, die Auskunft über die Bestandsdaten zu erteilen, normieren. Die Voraussetzungen für die Strafverfolgungs- und Sicherheitsbehörden, auf diese Daten zuzugreifen und von den Telekommunikationsdiensteanbietern darüber Auskunft zu verlangen, müssen im jeweiligen Fachgesetz vom jeweiligen Fachgesetzgeber geregelt werden.

Zweitens: Eine Auskunft über Daten, mittels derer der Zugriff auf Endgeräte oder Speichereinrichtungen durch Zugangssicherungs\_codes wie Passwörter, PIN und PUK geschützt wird, ist nur zulässig, wenn auch die gesetzlichen Voraussetzungen für die Nutzung der auf den Endgeräten gespeicherten Daten gegeben sind.

Drittens: Die Auskunft der Diensteanbieter über die namentliche Zuordnung dynamischer Internetprotokoll-Adressen (IP-Adresse) erfordert eine normenklare Regelung, dass es sich hierbei um einen Eingriff in Artikel 10 Absatz 1 des Grundgesetzes handelt. Denn die Bestandsdaten zu Name und Anschrift kann der Diensteanbieter nur anhand der bei ihm gespeicherten Telekommunikationsverkehrsdaten feststellen. Solche Feststellungen unterliegen dem Schutz des Fernmeldegeheimnisses aus Artikel 10 des Grundgesetzes. Das löst das Zitiergebot auch dann aus, wenn die staatliche Stelle selbst keine Verkehrsdaten erhält.

## B. Lösung

Das Gesetz schafft für die bisher möglichen und für die Gefahrenabwehrarbeit der Landespolizei und für den Aufgabenbereich des Landesverfassungsschutzes unverzichtbaren Bestandsdatenauskünfte eine den Anforderungen des Bundesverfassungsgerichts mehr als genügende neue normative Grundlage. Für die polizeiliche Gefahrenabwehr sind Bestandsdatenauskünfte vor allem zur Verhinderung von angedrohten Suiziden, zum Auffinden von vermissten und hilflosen Personen oder Verhinderung von angedrohten Straftaten gegen Leben, Gesundheit und Freiheit (Amoklagen) von großer Bedeutung. Der Landesgesetzgeber regelt das Ob und Wie des Zugriffs auf die auf die nach Bundesrecht (TKG) gespeicherten Bestandsdaten. Neue Befugnisse für die Landespolizei oder den Landesverfassungsschutz werden nicht geschaffen. Landespolizei und Landesverfassungsschutz sollen nach dem 30. Juni 2013 für ihre jeweilige Aufgabenerfüllung Bestandsdaten bei den Diensteanbietern abrufen dürfen.

Die Voraussetzungen manueller Bestandsdatenauskünfte staffelt das Gesetz für Polizei und Verfassungsschutz den unterschiedlichen Eingriffstiefen entsprechend aufsteigend, gefolgt von einem ebenso gestaffelten Anordnungsverfahren. Es berücksichtigt, dass der Zugriff auf die durch Sicherungscodes (PIN und PUK) geschützten Endgeräte oder Speichereinrichtungen und die den Schutzbereich des Artikel 10 des Grundgesetzes tangierende Bestandsdatenauskunft anhand zu bestimmter Zeit zugewiesener Internetprotokoll-Adresse (dynamische IP-Adresse) gegenüber der einfachen Bestandsdatenauskunft von gesteigerten Anforderungen und Verfahrenssicherungen abhängig zu machen ist. Der Gesetzesvorschlag berücksichtigt auch teilweise über die Vorgaben des Bundesverfassungsgerichtes hinausgehende Forderungen des Schleswig-Holsteinischen Landtages zum Schutz der Vertraulichkeit und Anonymität der Telekommunikation (Beschluss vom 12.12.12, Annahme des Antrages gem. Drucksache 18/311 in der Fassung der Drucksache 18/370), greift Anregungen des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD SH) sowie aus dem parlamentarischen Bereich des Schleswig-Holsteinischen Landtages, anderer Länderparlamente und des Bundestages auf.

Der Entwurf übernimmt das vom Bundesverfassungsgericht für das Vorhalten und für die Abfrage von Bestandsdaten nach dem Telekommunikationsgesetz entwickelte, die Grundrechte sichernde Doppeltürenmodell klarstellend auch für das Auskunftsverlangen nach den Bestandsdaten gemäß § 14 Abs. 2 des Telemediengesetzes. Das ist konsequent. Die Abrufnormen für Bestands- und Nutzungsdaten nach dem Telemediengesetz (§§ 14, 15 TMG) stellen den Datenabruf einzig auf die im jeweiligen Fachgesetz nicht weiter eingegrenzte Erforderlichkeit für Strafverfolgung, Gefahrenabwehr und nachrichtendienstliche Aufgabenerfüllung ab. Das gerade kritisiert das Bundesverfassungsgericht in Bezug auf die Bestandsdaten des Telekommunikationsgesetzes abrufenden Fachgesetze. Deshalb bringt Schleswig-Holstein eine Konkretisierung nun auch im anderen Fachgesetz. Auch in den - je nach Nutzung unter der Herrschaft des Telekommunikationsgesetzes oder des Telemediengesetzes stehenden - sozialen Netzwerken werden Amoktaten, Suizide oder polizeilich

relevante Rechts-Rock-Konzerte angekündigt, die es rechtssicher zu verhindern gilt. Das aktuelle Gesetzesvorhaben der Landesregierung in Nordrhein-Westfalen zum dortigen Polizeigesetz sieht Entsprechendes vor (NW-Landtagsdrucksache 16/2256, § 20 a PolG-E NW).

Das geltende Landesrecht hat den Zugriff auf die Telemedien-Bestandsdaten als ein „besonderes Auskunftsverlangen“ (§ 8 a Abs. 1 Satz 1, Abs. 2 Nr. 5 LVerfSchG) dem Verfassungsschutz bereits zur Verfügung gestellt.

### **C. Alternativen**

Keine.

### **D. Direkte Kosten und Verwaltungsaufwand**

#### 1. Kosten

Die Entschädigung der betroffenen Telekommunikationsanbieter nach § 23 JVEG wird aus dem Haushalt des Innenministeriums bestritten.

#### 2. Verwaltungsaufwand

Ein Erfüllungsaufwand für die Verwaltung entsteht nicht.

#### 3. Auswirkungen auf die private Wirtschaft

Auswirkungen auf die private Wirtschaft werden durch dieses Gesetz nicht verursacht. Der Aufwand für die Auskunftserteilung wird den betroffenen Telekommunikationsanbietern nach § 23 JVEG entschädigt.

### **E. Information des Landtages nach Art. 22 der Landesverfassung**

Der Präsident des Schleswig-Holsteinischen Landtages wurde mit Schreiben vom 6. März 2013 zeitgleich mit den Verbänden von dem Gesetzesvorhaben unterrichtet

### **F. Federführung**

Innenministerium

## Entwurf

**Gesetz zur Änderung des Landesverwaltungsgesetzes und des Landesverfassungsschutzgesetzes - Anpassung des manuellen Abrufs der Bestandsdaten nach dem Telekommunikationsgesetz an die verfassungsrechtlichen Vorgaben**

Vom

Der Landtag hat das folgende Gesetz beschlossen:

**Artikel 1****Gesetz zur Änderung des Landesverwaltungsgesetzes**

Das Landesverwaltungsgesetz in der Fassung der Bekanntmachung vom 2. Juni 1992 (GVOBl. Schl.-H. S. 243, ber. S. 534), zuletzt geändert durch Artikel 1 des Gesetzes vom 17. Dezember 2012 (GVOBl. Schl.-H. S. 749), wird wie folgt geändert:

**1. Das Inhaltsverzeichnis wird wie folgt geändert:**

Im Inhaltsverzeichnis werden nach den Worten „§ 180 Befragung und Auskunftspflicht, polizeiliche Anhalte- und Sichtkontrollen“ folgende Worte eingefügt:

- a) „§ 180 a Bestandsdatenauskunft“
- b) „§ 180 b Verfahren zur Bestandsdatenauskunft“

**2. Nach § 180 werden §§ 180 a und 180 b eingefügt:**

## a) „§ 180 a Bestandsdatenauskunft

(1) Die Polizei darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), Auskunft über die nach §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten verlangen (§ 113 Abs. 1 Satz 1 des Telekommunikationsgesetzes), soweit dies zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für die öffentliche Sicherheit erforderlich ist. Das vom Telekommunikationsgesetz zum Inhalt und zur Übermittlung des Auskunftsverlangens an die Diensteanbieter vorgegebene Verfahren findet Anwendung (§ 113 Abs. 2 des Telekommunikationsgesetzes).

(2) Bezieht sich das Auskunftsverlangen nach Absatz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Abs. 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen

1. zur Überwachung der Telekommunikation nach § 185 a oder
2. zur Sicherstellung von nicht mehr dem Schutz des Artikel 10 des Grundgesetzes unterliegenden in Endeinrichtungen oder auf Speichereinrichtungen abgelegten Daten nach § 210.

Die Auskunft über die nach §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten nach Satz 1 und Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Abs. 1 Satz 3 des Telekommunikationsgesetzes). Satz 2 gilt bei fest zugewiesenen Internetprotokoll-Adressen sinngemäß.

(3) Aufgrund eines Auskunftsverlangens nach Absatz 1 bis 2 hat der Diensteanbieter die zur Auskunftserteilung erforderlichen Daten unverzüglich und vollständig zu übermitteln. Für seine Entschädigung ist § 23 des Justizvergütungs- und –entschädigungsgesetzes entsprechend anzuwenden.

(4) Absatz 1 bis 3 gilt bei an die Telemedien-Diensteanbieter gerichteten Auskunftsverlangen auf Bestandsdaten nach § 14 des Telemediengesetzes sowie auf die Identifikation der Nutzer und auf das Datum und die Uhrzeit des Beginns und Endes der Nutzung beschränkte Daten im Sinne des § 15 des Telemediengesetzes entsprechend.“

b) „§ 180 b Verfahren zur Bestandsdatenauskunft

(1) Auskunftsverlangen nach § 180 a Abs. 2 dürfen nur auf Antrag der Polizei durch das nach § 186 Abs. 2 Satz 1 zuständige Gericht angeordnet werden. Für das Verfahren findet das Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechende Anwendung. Der Anhörung der betroffenen Person durch das Gericht bedarf es nicht. Bei Gefahr im Verzuge kann die Polizei die Anordnung treffen. In diesem Fall gelten die § 186 Abs. 1 Satz 3 bis 5, § 186 a Abs. 6 entsprechend. Satz 1 bis 4 findet keine Anwendung, wenn der Betroffene vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird. Das Vorliegen der Voraussetzungen nach Satz 6 ist aktenkundig zu machen. Nach Abschluss der Maßnahmen nach § 180 a Abs. 2 ist die betroffene Person von der Polizei zu unterrichten und auf die Möglichkeit nachträglichen Rechtsschutzes hinzuweisen. Die Unterrichtung erfolgt, soweit und sobald der Zweck der Auskunft nicht vereitelt wird. Die Unterrichtung nach Satz 8 unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Unterrichtung nach Satz 9 zurückgestellt oder nach Satz 10 von ihr abgesehen, gilt § 186 Abs. 4 Satz 5 bis 9 entsprechend.

(2) Absatz 1 gilt bei Auskunftsverlangen nach § 180 a Abs. 4 entsprechend.“

## Artikel 2

### Gesetz zur Änderung des Landesverfassungsschutzgesetzes

Das Landesverfassungsschutzgesetz vom 23. März 1991 (GVObI. Schl.-H. S. 203), zuletzt geändert durch Artikel 2 des Gesetzes vom 11. Januar 2012 (GVObI. Schl.-H. S. 78), wird wie folgt geändert:

#### 1. § 8 a wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Die Verfassungsschutzbehörde darf im Einzelfall bei denjenigen, die geschäftsmäßig Postdienstleistungen oder Telemedien erbringen oder daran mitwirken, Auskunft über Daten einholen, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Postdienstleistungen oder Telemedien (Bestandsdaten) gespeichert worden sind, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Bei denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, darf die Verfas-

sungsschutzbehörde im Einzelfall Auskunft über die nach den §§ 95 und 111 Telekommunikationsgesetz erhobenen Daten verlangen (§ 113 Abs. 1 Satz 1 des Telekommunikationsgesetzes), soweit dies zu ihrer Aufgabenerfüllung erforderlich ist. Bezieht sich das Auskunftsverlangen nach Satz 2 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Abs. 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. Die Auskunft darf auch anhand einer zu bestimmten Zeitpunkten zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Abs. 1 Satz 3 des Telekommunikationsgesetzes). Aufgrund eines Auskunftsverlangens nach den Sätzen 2 bis 4 haben diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, die zur Auskunft erforderlichen Daten unverzüglich, vollständig und richtig zu übermitteln.“

b) In Absatz 7 Satz 1 werden dem Wort „Telekommunikationsverkehrsdaten“ ein Komma und die Worte „zu Telekommunikationsbestandsdaten nach Absatz 1 Satz 3 und 4“ eingefügt.

c) Nach Absatz 8 wird folgender Absatz 9 angefügt:

„(9) Für die Erteilung von Auskünften nach Absatz 1 Satz 2 bis 4 hat der Verpflichtete Anspruch auf eine Entschädigung entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes.“

## **2. § 26 a Abs. 1 Nr. 2 erhält folgende Fassung:**

„2. bei der Anordnung von Auskunftspflichten zu Telekommunikationsbestandsdaten (§ 8 a Abs. 1 Satz 3 und 4), zu Post- und Telekommunikationsverkehrsdaten (§ 8 a Abs. 2 Nr. 3 und 4) sowie zu Nutzungsdaten von Telemedien (§ 8 a Abs. 2 Nr. 5)“

### **Artikel 3 Einschränkung von Grundrechten**

Durch die Artikel 1 und 2 dieses Gesetzes wird das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) beschränkt.

### **Artikel 4 Inkrafttreten**

Dieses Gesetz tritt am 1. Juli 2013 in Kraft.

Das vorstehende Gesetz wird hiermit ausgefertigt und ist zu verkünden.

Kiel, TT. MM. 2013

Torsten Albig  
Ministerpräsident

Andreas Breitner  
Innenminister

## Begründung

### I. Allgemeines

Das Bundesverfassungsgericht – BVerfG – hat eine Verfassungsbeschwerde gegen die gesetzlichen Bestimmungen des Telekommunikationsgesetzes (TKG) zur Speicherung bestimmter Bestandsdaten (§ 111 TKG) sowie zur Verwendung dieser Daten im Wege des automatisierten (§ 112 TKG) oder manuellen Auskunftsverfahrens (§ 113 TKG) im Wesentlichen zurückgewiesen (Beschluss vom 24. Januar 2012, 1 BvR 1299/05). Es beurteilt die Erhebung und Speicherung von Telekommunikationsdaten nach § 111 TKG sowie deren Verwendung im automatisierten Auskunftsverfahren (§ 112 TKG) ohne Einschränkung als verfassungsgemäß. Hingegen genügten die manuellen Auskunftsverfahren (§ 113 TKG) nicht voll den verfassungsrechtlichen Anforderungen. Hier hat das Bundesverfassungsgericht vom Gesetzgeber in Bund und Ländern folgende Nachbesserungen bis zum 30.06.2013 verlangt:

1. In der Zuordnung von Telekommunikationsnummern zu ihren Anschluss-inhabern liegt ein Eingriff in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG (Grundrecht auf informationelle Selbstbestimmung). Demgegenüber liegt in der Zuordnung von dynamischen IP-Adressen ein Eingriff in Art. 10 Abs. 1 GG (Fernmeldegeheimnis).
2. Der Gesetzgeber muss nach dem vom BVerfG entwickelten sog. Doppeltürenmodell im manuellen Auskunftsverfahren (§§ 113 Abs. 1, 111, 95 Abs. 1 TKG) sowohl belastbare Rechtsgrundlagen für die (unmittelbare wie mittelbare) Übermittlung von Bestandsdaten<sup>3</sup> durch die TK-Anbieter (§ 113 TKG, Norm für die Datenübermittlung = 1. Tür) an die Sicherheitsbehörden für deren repressive, präventive und nachrichtendienstliche Aufgabenerledigung als auch für den Abruf dieser Daten durch die Sicherheitsbehörden bei den TK-Anbietern schaffen (Normen für den Datenabruf = 2. Tür). Für den Abruf der Daten bei den TK-Anbietern bedürfe es qualifizierter Rechtsgrundlagen in den jeweiligen Bedarfsträgergesetzen (StPO, Polizeigesetze des Bundes und der Länder, Verfassungsschutzgesetze), die selbst eine Auskunftspflicht der Telekommunikationsunternehmen normenklar begründen müssen. Allgemeine Datenerhebungsregelungen reichen dort nicht (mehr) aus.
3. Die Sicherheitsbehörden dürfen Auskünfte über Zugangssicherungs\_codes wie Passwörter, PIN und PUK (§ 113 Abs. 1 TKG) nur dann verlangen, wenn die ge-

---

<sup>3</sup> **Bestandsdaten** sind Name, Anschrift, Bankverbindung, Anschlussnummer (Rufnummer), Passwörter, PIN und PUK. Das sind Daten, die während eines Vertragsverhältnisses mit einem Telekommunikationsunternehmen normalerweise gleich bleiben. (**Legaldefinition in § 3 Nr. 3 TKG**: "Bestandsdaten": Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden.")

Dem gegenüber sind **Verkehrsdaten** beispielsweise die Nummer / Kennung beteiligter Anschlüsse (anrufender und angerufener Kommunikationsteilnehmer), Beginn und Ende der jeweiligen Verbindung als auch sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation notwendige Verkehrsdaten (**Legaldefinition in § 3 Nr. 30 TKG**: "Verkehrsdaten": Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden.")



setzlichen Voraussetzungen für ihre Nutzung gegeben sind. Mit anderen Worten: Für eine auf die Zugangssicherungs\_codes gerichtete Abfrage (§ 113 TKG) müssen die jeweils (fach-)gesetzlichen Voraussetzungen des damit konkret angestrebten Nutzungszweckes erfüllt sein (beispielsweise für eine TK-Überwachung oder für eine Beschlagnahme / Sicherstellung).

4. Der Abruf von Bestandsdaten (mittelbare Bestandsdatenauskunft), der nur über die Zuordnung einer zu einem bestimmten Zeitpunkt (bekannten) dynamischen Internet-Protokolladresse (TK-Verkehrsdatum) möglich ist, bedarf einer ausdrücklichen gesetzlichen Regelung.

Das Gesetz schafft für die bisher möglichen und für die Gefahrenabwehrarbeit der Landespolizei und für den Aufgabenbereich des Landesverfassungsschutzes unverzichtbaren Bestandsdatenauskünfte eine den Anforderungen des Bundesverfassungsgerichts mehr als genügende neue normative Grundlage. Für die polizeiliche Gefahrenabwehr sind Bestandsdatenauskünfte vor allem zur Verhinderung von angedrohten Suiziden, zum Auffinden von vermissten und hilflosen Personen oder Verhinderung von angedrohten Straftaten gegen Leben, Gesundheit und Freiheit (Amoklagen) von großer Bedeutung. Dies gilt für den Verfassungsschutz gleichermaßen. Wird im Rahmen einer vom Verfassungsschutz zu beobachtenden Szene eine Mobilfunknummer bekannt, wird über die Bestandsdatenabfrage der Anschlussinhaber personalisiert. Nachfolgend wird der Verfassungsschutz mittels der ihm zur Verfügung stehenden Befugnisse feststellen können, ob die Person der Szene zuordnen oder aus seinem Fokus zu nehmen ist.

Der Landesgesetzgeber regelt das Ob und Wie des Zugriffs auf die auf die nach Bundesrecht gespeicherten Bestandsdaten. Neue Befugnisse für die Landespolizei oder den Landesverfassungsschutz werden nicht geschaffen. Landespolizei und Landesverfassungsschutz sollen nach dem 30. Juni 2013 für ihre jeweilige Aufgabenerfüllung Bestandsdaten bei den Diensteanbietern abrufen dürfen.

Es findet insoweit eine Konkretisierung der Datenabrufvorschriften nach den verfassungsrechtlichen Vorgaben für die Landespolizei im Landesverwaltungsgesetz und für den Landesverfassungsschutz im Landesverfassungsschutzgesetz statt.

Die Voraussetzungen manueller Bestandsdatenauskünfte staffelt das Gesetz für Polizei und Verfassungsschutz den unterschiedlichen Eingriffstiefen entsprechend aufsteigend, gefolgt von einem ebenso gestaffelten Anordnungsverfahren. Es berücksichtigt, dass der Zugriff auf die durch Sicherungscodes (PIN und PUK) geschützten Endgeräte oder Speichereinrichtungen und die den Schutzbereich des Artikel 10 des Grundgesetzes tangierende Bestandsdatenauskunft anhand zu bestimmter Zeit zugewiesener Internetprotokoll-Adresse (dynamische IP-Adresse) gegenüber der einfachen Bestandsdatenauskunft von gesteigerten Anforderungen und Verfahrenssicherungen abhängig zu machen ist. Der Gesetzesvorschlag berücksichtigt auch teilweise über die Vorgaben des Bundesverfassungsgerichtes hinausgehende Forderungen des Schleswig-Holsteinischen Landtages zum Schutz der Vertraulichkeit und

Anonymität der Telekommunikation (Beschluss vom 12.12.12, Annahme des Antrages gem. Drucksache 18/311 in der Fassung der Drucksache 18/370), greift Anregungen des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD SH) sowie aus dem parlamentarischen Bereich des Schleswig-Holsteinischen Landtages, anderer Länderparlamente und des Bundestages auf.

Für den Bund regelt den fachgesetzlichen Datenabruf der Gesetzentwurf zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft (Bundratsdrucksache 664/12, Bundestagsdrucksache 17/12034).

Ein Zuwarten des Landesgesetzgebers auf den Bund wäre zwar wünschenswert, ist aber wegen der vom BVerfG auch den Landesgesetzgebern gesetzten Frist nicht möglich. Anderenfalls könnten Landespolizei und Landesverfassungsschutz ab dem 1. Juli 2013 nur die nach § 111 TKG gespeicherten Telekommunikationsbestandsdaten im verfassungsrechtlichen Anforderungen genügenden automatisierten Abrufverfahren (§ 112 TKG) über die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen abrufen<sup>4</sup>. Das automatisierte Abrufverfahren ist für die Belange der Sicherheitsbehörden nicht (immer) ausreichend. Zum einen sind die bei den Telekommunikationsdiensteanbietern geführten Abrufdateien nicht immer aktuell, zum anderen erfasst die manuelle Auskunft neben den Daten nach § 111 TKG auch Daten, die die Anbieter zur inhaltlichen Ausgestaltung, Änderung oder Beendigung ihrer Vertragsverhältnisse gemäß § 95 Abs. 1 i. V. m. mit § 3 Nr. 3 TKG erheben und speichern dürfen (beispielsweise Bankverbindung). Darüber hinaus werden Zugangssicherungs\_codes den Sicherheitsbehörden erst über die manuelle Bestandsdatenabfrage zugänglich. Sie ist deshalb neben und ergänzend zur automatisierten Anfrage für die Sicherheitsbehörden unverzichtbar. Für die Fachgesetze des Bundes (StPO, BKAG, BPolG, Bundesverfassungsschutzgesetz u. a., Bundratsdrucksache 664/12, a. a. O.: Art. 2 ff) wird das im laufenden Gesetzgebungsverfahren bestätigt. Auch in den Ländern (beispielsweise Nordrhein-Westfalen, Mecklenburg-Vorpommern) laufen deshalb vergleichbare Gesetzgebungsverfahren, die alle zum 1. Juli 2013 abgeschlossen sein müssen.

Zwar müssen nach den Vorgaben des BVerfG auch die auf das TKG zugreifenden Abrufnormen in der Gesetzgebungskompetenz der Länder selbst eine Auskunftspflicht der Telekommunikationsunternehmen normenklar begründen. Der Gesetzentwurf der Bundesregierung zur Neuregelung der Bestandsdatenauskunft (Bundratsdrucksache 664/12) löst diese Aufgabe, indem in den zugreifenden Fachgesetzen auf die geschäftsmäßigen Erbringer von Telekommunikationsdiensten unter Nennung der für Bestandsdaten einschlägigen §§ 95, 111 TKG und der in Klammer gesetzten Fundstelle für das manuelle Auskunftsverfahren des § 113 Abs. 1 Satz 1 TKG-E Bezug genommen wird. Insofern beziehen sich diese Fundstellenangaben zum manuel-

---

<sup>4</sup> Die Telekommunikationsdiensteanbieter haben die von ihnen nach § 111 TKG zu speichernden Daten für die Bundesnetzagentur bereitzuhalten. Die Bundesnetzagentur ruft entsprechende Datensätze auf Ersuchen anfrageberechtigter Behörden im automatisierten Verfahren bei den Telekommunikationsanbietern ab und übermittelt sie den anfragende Behörden.

len Auskunftsverfahren in diesem Entwurf auf die Vorschläge des o. a. Gesetzentwurfes der Bundesregierung. Sie müssten gegebenenfalls im weiteren Gesetzgebungsverfahren dem zustande gekommenen Bundesgesetz angepasst werden.

Die Bestandsdatenauskünfte setzen Polizei und Verfassungsschutz in die Lage, nachfolgende Maßnahmen im jeweiligen Aufgabenspektrum durchzuführen. Dazu folgende Beispiele: Wird eine Person vermisst, zu der bekannt ist, dass sie möglicherweise ihr Handy bei sich führt, kann die dem Handy zugewiesene Nummer bei einem bekannten Diensteanbieter mittels gezielter oder durch an alle Netzbetreiber bzw. Provider gerichteten Bestandsdatenabfrage der Polizei schnell bekannt gemacht werden. Danach könnte eine präventive Handy-Ortung folgen, um den Aufenthaltsort der vermissten Person besser eingrenzen zu können. Wird dann in dem Suchgebiet das gesperrte Handy nicht aber die vermisste Person gefunden, könnte über den beim Diensteanbieter zu hinterfragenden Zugangscode (PIN, PUK) das Handy entsperrt werden, um möglicherweise von den Anschlussinhabern der im Suchzeitraum durch die vermisste Person angerufenen oder per SMS angeschriebenen Teilnehmern weitere Ermittlungsansätze für die Suche zu erhalten. Ein unbekannter Nutzer hat über seinen Internet-Account seinen Suizid angekündigt. Wo der Computer steht (Anschrift des Anschlussinhabers des Internet-Zuganges), ist nur über eine Bestandsdatenabfrage bei den Internet-Zugangsanbietern zu erfahren. Diese können, sofern bei ihnen noch gespeichert, über die von ihnen zur fraglichen Zeit der Suizidankündigung jeweils vergebene dynamische Internetprotokoll-Adresse den diese IP-Adresse nutzenden Anschlussinhaber personifizieren und der Polizei für weitere gefahrenabwehrende Maßnahmen die Anschrift mitteilen.

Ähnliches gilt für den Aufgabenbereich des Verfassungsschutzes. Wird im Rahmen einer nachrichtendienstlichen Sachverhaltsaufklärung eine Handy-Nummer bekannt, kann der Anschlussinhaber mittels Bestandsdatenabfrage ermittelt werden. Dessen Zugehörigkeit zu einer vom Verfassungsschutz zu beobachtenden Szene kann im Anschluss daran veri- oder falsifiziert werden.

Der Entwurf übernimmt das vom Bundesverfassungsgericht für das Vorhalten und für die Abfrage von Bestandsdaten nach dem Telekommunikationsgesetz entwickelte, die Grundrechte sichernde Doppeltürenmodell klarstellend auch für das Auskunftsverlangen nach den Bestandsdaten gemäß § 14 Abs. 2 des Telemediengesetzes. Das ist konsequent. Die Abrufnormen für Bestands- und Nutzungsdaten nach dem Telemediengesetz (§§ 14, 15 TMG) stellen den Datenabruf einzig auf die im jeweiligen Fachgesetz nicht weiter eingegrenzte Erforderlichkeit für Strafverfolgung, Gefahrenabwehr und nachrichtendienstliche Aufgabenerfüllung ab. Das gerade kritisiert das Bundesverfassungsgericht in Bezug auf die Bestandsdaten des Telekommunikationsgesetzes abrufenden Fachgesetze. Deshalb bringt Schleswig-Holstein eine Konkretisierung nun auch im anderen Fachgesetz. Auch in den - je nach Nutzung unter der Herrschaft des Telekommunikationsgesetzes oder des Telemediengesetzes stehenden - sozialen Netzwerken werden Amoktaten, Suizide oder polizeilich relevante Rechts-Rock-Konzerte angekündigt, die es rechtssicher zu verhindern gilt.

Das aktuelle Gesetzesvorhaben der Landesregierung in Nordrhein-Westfalen zum dortigen Polizeigesetz sieht Entsprechendes vor (NW-Landtagsdrucksache 16/2256, § 20 a PolG-E NW).

Das geltende Landesrecht hat den Zugriff auf die Telemedien-Bestandsdaten als ein „besonderes Auskunftsverlangen“ (§ 8 a Abs. 1 Satz 1 und Abs. 2 Nr. 5 LVerfSchG) dem Verfassungsschutz bereits zur Verfügung gestellt.

## II. Einzelbegründung

### Zu Artikel 1 (Anpassung des LVwG)

#### Zu Nr. 1 (Inhaltsverzeichnis)

Das Inhaltsverzeichnis wird den Änderungen dieses Entwurfes angepasst.

#### Zu Nr. 2 a) - § 180 a LVwG

Die Norm regelt nach den verfassungsrechtlichen Vorgaben ansteigende materielle rechtliche Zugriffsvoraussetzungen auf die Bestandsdaten mittels manuellem Abrufverfahren (§ 113 TKG) durch die Landespolizei.

Mit **Absatz 1** Satz 1 wird durch Bezugnahme auf die vom BVerfG nicht beanstandeten §§ 95, 111 TKG zunächst der Umfang der abfragbaren Bestandsdaten beschrieben. Im Wesentlichen gelangen die in § 111 TKG gelisteten Bestandsdaten zur Abfrage. Das sind Rufnummern oder andere Anschlusskennungen, Namen und Anschrift des Anschlussinhabers, bei natürlichen Personen deren Geburtsdatum, bei Festnetzanschlüssen zusätzlich auch die Anschrift des Anschlusses, in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie das Datum des Vertragsbeginns.

Die zum Tatbestand gehörende Erforderlichkeit gibt dem Rechtsanwender Polizei auf, in jedem Einzelfall zu prüfen, ob die Bestandsdatenauskunft für den jeweils aktuell zu beurteilenden Gefahrensachverhalt tatsächlich notwendig ist.

Als materielle Zugriffsvoraussetzung muss die im Einzelfall bevorstehende Gefahr für die öffentliche Sicherheit (= konkrete Gefahr) gegeben sein. Die konkrete Gefahr umfasst neben dem Gefahrenverdacht auch die Dauergefahr, wie vom Bundesverfassungsgericht in seiner Rasterfahndungsentscheidung entwickelt (Beschluss vom 04. April 2006 – 1 BvR 518/02). Sachverhalte weit im Vorfelde konkreter Gefahr sind vom Regelungskreis der Norm ausdrücklich nicht erfasst.

Das polizeiliche Auskunftsverlangen muss unter Beachtung des vom Telekommunikationsgesetz dazu vorgegebenen Verfahrens erfolgen (Satz 2). Der Gesetzentwurf der Bundesregierung sieht dazu Folgendes vor: Das Auskunftsbegehren ist in Textform zu stellen. Es muss die Abrufberechtigung durch Übermittlung der gesetzlichen Befugnis belegen. Bei Gefahr im Verzuge kann auf die Textform verzichtet werden. Das polizeiliche Auskunftsverlangen ist dann unverzüglich schriftlich dem Diensteanbieter zu bestätigen.

Mit **Absatz 2** Satz 1 wird die Forderung des BVerfG erfüllt, dass die Polizei Auskünfte über Zugangssicherungs\_codes wie Passwörter, PIN und PUK nur dann verlangen darf, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind. Mit anderen Worten: Für eine auf die Zugangssicherungs\_codes gerichtete Abfrage (§ 113 TKG) müssen die jeweils fachgesetzlichen Voraussetzungen des damit konkret angestrebten Nutzungszweckes erfüllt sein. Sollen über die Zugangscodes Maßnahmen zur gefahrenabwehrenden Überwachung der Telekommunikation vorbereitet werden, müssen die in § 185a enthaltenen Voraussetzungen vorliegen. Soll über die Zugangscodes auf die nicht mehr dem Fernmeldegeheimnis unterworfenen und im

Handy nach Ende des jeweiligen Telekommunikationsvorganges abgelegten Daten zugegriffen werden (s. o. a. Beispiel), müssen die Voraussetzungen der präventiven Sicherstellung gemäß § 210 gegeben sein. Die Nutzung für andere, vom Entwurf nicht ausdrücklich benannte und zurzeit darüber hinaus auch nicht zu konkretisierende Maßnahmen ist ausgeschlossen (abgeschlossener Katalog).

Absatz 2 Satz 2 regelt, dass die Auskunft auch zu bekannten Internetprotokoll-Adressen, die zu einer bestimmten Zeit zugewiesen waren oder noch sind, zu erteilen ist. Durch die Bezugnahme auf Satz 1 und Absatz 1 gelten die dort geregelten Eingriffsschwellen auch für diese Bestandsdatenauskunft zu einer bekannten Internetprotokoll-Adresse. Mit Absatz 2 Satz 3 erfolgt durch die Bezugnahme auf Satz 2 die Gleichsetzung der Bestandsdatenauskunft von dynamischer und fest zugewiesener Internet-Protokoll-Adresse.

**Absatz 3** bestimmt nach dem Vorbild des Gesetzentwurfes der Bundesregierung zur Neuregelung der Bestandsdatenauskunft und in Anlehnung an § 185 a Abs. 4 Satz 2, dass die Entschädigungsregelung des § 23 Justizvergütungs- und entschädigungsgesetzes für die Diensteanbieter entsprechend zur Anwendung kommen soll.

**Absatz 4:** Für an die Telemedien-Diensteanbieter gerichteten Auskunftsverlangen nach Bestandsdaten unter dem Regime des Telemediengesetzes gelten die für den Zugriff auf die Telekommunikationsbestandsdaten entwickelten Regelungen gemäß Absatz 1 bis 3 entsprechend.

### **Zu Nr. 2 b) - § 180 b LVwG**

Für Auskunftsverlangen ohne Inanspruchnahme von Zugangscodes oder IP-Adressen bedarf es keines besonderen Verfahrens (§ 180 a Abs. 1 Satz 1). Sie können von jeder Polizeivollzugskraft unter Beachtung des vom Telekommunikationsgesetzes vorgegebenen Übermittlungsmodus (§ 180 a Abs. 1 Satz 2) an die Diensteanbieter gerichtet werden. Details können einem Erlass des Innenministeriums oder in dessen Auftrag eines Polizeiamts vorbehalten bleiben.

**Absatz 1** stellt das auf Sicherungscodes (§ 180 a Abs. 2 Satz 1 Nr. 1 und 2) und auf IP-Adressen (§ 180 a Abs. 2 Satz 2) gerichtete Auskunftsverlangen unter einen eigenständigen Richtervorbehalt (Satz 1). Zuständig ist das Amtsgericht am Sitz des beantragenden Landeskriminal- oder Landespolizeiamtes oder der Polizeibehörde (§ 186 Abs. 2 Satz 1). Für das Verfahren soll – wie bei allen richterlich zu bewertenden polizeilichen Maßnahmen – das Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend Anwendung finden (Satz 2). Einer – auch nachträglichen – Anhörung der von der Bestandsdatenauskunft betroffenen Person bedarf es wegen der im Grunde geringen Eingriffstiefe und nachfolgend weiterer Grundrechte sichernder Regelungen nicht (Satz 3).

Absatz 1 lässt bei Gefahr im Verzuge die polizeiliche Anordnung durch die Amts- bzw. Behördenleitung oder durch von ihr besonders Beauftragte des Polizeivollzugs-

dienstes zu (Satz 4 und 5). Das im Zusammenhang mit anderen heimlichen Datenerhebungen bei polizeilicher Eilkompetenz bewährte Verfahren nach § 186 Abs. 1 Satz 3 bis 5 und § 186 a Abs. 6 gilt entsprechend (Satz 5). Im Wesentlichen sind das die unverzüglich nachzuholende richterliche Bestätigung der polizeilichen Eilordnung (§ 186 Abs. 1 Satz 5) und die Möglichkeit des Gerichtes die polizeiliche Anordnung aufzuheben, zu ändern oder anders anzuordnen (§ 186 a Abs. 6 Satz 2 und 3).

Absatz 1 verlangt nach Abschluss der Maßnahme die Betroffenenbenachrichtigung (Satz 8), die unter gewissen Bedingungen zurückgestellt werden (Satz 9) oder in Ausnahmefällen mit richterlicher Befürwortung ganz unterbleiben kann (Satz 10 und 11) und gewährt die Möglichkeit nachträglichen Rechtsschutzes (Satz 8). Die Subsidiaritätsklausel (Satz 6) vermeidet doppelte gerichtliche Entscheidungen, wenn der Maßnahmenbetroffene vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung beispielsweise für Maßnahmen der Telekommunikationsüberwachung gestattet wird. Eine doppelte Benachrichtigungspflicht wäre keine zusätzliche Verfahrenssicherung und kann deshalb zur Vermeidung von Bürokratiekosten entfallen. Ähnliches sieht der im Bundestagsinnenausschuss zwischen den Bundestagsfraktionen der Union, der FDP und der SPD abgestimmte Änderungsantrag zum Gesetzentwurf der Bundesregierung vor (19.0.13).

**Absatz 2** lässt klarstellend den Auskunftsanspruch auf Telemedien-Bestandsdaten (§ 14 Telemediengesetz) nach den vom Entwurf für den Zugriff auf Bestandsdaten nach dem Telekommunikationsgesetz festgelegten Voraussetzungen und Verfahren rechtssicher zu. Denn in den – je nach Nutzung unter der Herrschaft des Telekommunikationsgesetzes oder des Telemediengesetzes stehenden – sozialen Netzwerken werden Suizide oder Amoktaten angekündigt, die es rechtssicher zu verhindern gilt. Der aktuelle Gesetzentwurf der Landesregierung in Nordrhein-Westfalen regelt das für ihre Polizei ähnlich (NW-Landtagsdrucksache 16/2256 für PoIG NW, ausgegeben am 12.03.13). Er überträgt das vom Bundesverfassungsgericht für den Bestandsdaten-Abruf nach dem Telekommunikationsgesetz entwickelte Doppeltürenmodell im Interesse rechtssicheren staatlichen Handelns auf die Abfrage zu den Telemedien-Bestandsdaten (§ 14 Abs. 2 Telemediengesetz). Das ist konsequent. Die Abrufnormen für Bestands- und Nutzungsdaten nach dem Telemediengesetz (§§ 14, 15 TMG) stellen den Datenabruf einzig auf die im jeweiligen Fachgesetz nicht weiter eingegrenzte Erforderlichkeit für Strafverfolgung, Gefahrenabwehr und nachrichtendienstliche Aufgabenerfüllung ab. Das gerade kritisiert das Bundesverfassungsgericht in Bezug auf die Bestandsdaten des Telekommunikationsgesetzes abrufenden Fachgesetze. Deshalb bringt Schleswig-Holstein eine Konkretisierung nun auch im anderen Fachgesetz. Dem Verfassungsschutz des Landes Schleswig-Holstein steht der Zugriff auf die Telemedien-Bestandsdaten bereits de lege lata als ein „besonderes Auskunftsverlangen“ zur Verfügung (§ 8 a Abs. 1 Satz 1, Abs. 2 Nr. 5 LVerSchG).

**Zu Artikel 2 (Anpassung des §§ 8 a, 26 a LVerfSchG)****Zu Nr. 1 § 8 a Besonderes Auskunftsverlangen****Zu 1 a) – § 8 a Abs. 1**

In § 8 a Abs. 1 des Landesverfassungsschutzgesetzes (LVerfSchG) war bereits eine Befugnisnorm für die Einholung von Bestandsdaten bei Anbietern, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, enthalten. Allerdings entspricht sie nicht mehr den konkreten Vorgaben des Bundesverfassungsgerichtes. Daher werden die Telekommunikationsdienste aus der Regelung in Absatz 1 Satz 1 herausgenommen und in den Sätzen 2 bis 4 die Vorgaben des Bundesverfassungsgerichtes entsprechend umgesetzt. Die Berechtigung der Verfassungsschutzbehörde im Einzelfall Bestandsdaten im manuellen Verfahren nach § 113 Telekommunikationsgesetz abzufragen, wird konkretisiert und die einzelnen Fallgestaltungen aufgeführt. Die Auskunftsverlangen von Daten, mittels derer der Zugriff auf Endgeräte oder Speichereinrichtungen durch Zugangssicherungs\_codes, wie Passwörter, PIN und PUK geschützt ist, werden in Satz 3 und die Auskunftsverlangen aufgrund einer dynamischen Internetprotokoll-Adresse in Satz 4 geregelt.

Die Abfrage von Bestandsdaten ist für die gesetzliche Aufgabenerfüllung der Verfassungsschutzbehörde unerlässlich, weil nur anhand dieser Auskünfte die Absender oder sonstige Beteiligte an Kommunikationsvorgängen identifizierbar sind. Diese Informationen können wiederum das Erkenntnisbild von relevanten Personen erheblich vervollständigen. Darüber hinaus erhält die Verfassungsschutzbehörde durch die Abfrage von Bestandsdaten wesentliche Informationen und Daten für die Durchführung von Maßnahmen nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses. Die Regelung in Satz 5 verpflichtet die Diensteanbieter die abgefragten Daten unverzüglich, vollständig und richtig zu übermitteln.

**Zu 1 b) – § 8 a Abs. 7**

Durch die Ergänzung in Absatz 7 werden Auskunftspflichten von Diensteanbietern zu Telekommunikationsbestandsdaten nach Absatz 1 Satz 3 und 4, also Bestandsdaten, mittels derer ein Zugriff auf Endgeräte oder Speichereinrichtungen durch Zugangssicherungs\_codes geschützt ist (durch Passwörter, PIN und PUK) und Bestandsdaten anhand einer dynamischen Internetprotokoll-Adresse (IP-Adresse) von der Innenministerin oder dem Innenminister angeordnet. Über die Anordnung unterrichtet die Verfassungsschutzbehörde die G 10-Kommission. Ferner teilt sie die Anordnung der betroffenen Person nach Einstellung der Maßnahme mit. Eine Mitteilung unterbleibt, solange eine Gefährdung des Zwecks der Maßnahme nicht ausgeschlossen werden kann oder solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist. Darüber hinaus wird klargestellt, dass bei dieser Auskunftspflicht – wie auch bei der Auskunftspflicht zu Post- und Telekommunikationsverkehrsdaten – das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 GG) eingeschränkt wird. Durch diese erhöhten Anordnungs- und Unterrichtungspflichten wird sichergestellt, dass derartige Daten nur aufgrund besonderer Verfahrensregelungen bei den Diensteanbietern erfragt werden



können. Ferner besteht durch die Unterrichtung der G10-Kommission über derartige Maßnahmen eine weitere Kontrollbefugnis. Aufgrund der besonderen Sensibilität von Bestandsdaten eines Betroffenen, die durch Passwörter geschützt sind oder die aufgrund einer dynamischen IP-Adresse erfolgen, ist eine Gleichstellung dieser Bestandsdaten mit den Verkehrsdaten bei den Anordnungs- und Unterrichtungspflichten angezeigt.

#### **Zu 1 c) – § 8 a Abs. 9**

In Absatz 9 wird erstmals eine Regelung über den Anspruch der zur Auskunft verpflichteten Anbieter von geschäftsmäßigen Telekommunikationsdiensten auf eine Entschädigung für die Auskunftserteilung geschaffen. Diese Regelung beinhaltet Entschädigungen für Auskünfte zu Telekommunikationsbestandsdaten (Absatz 1 Satz 2 bis 4). Hinsichtlich der Höhe der Entschädigung wird auf die entsprechende Anwendung den § 23 des Justizvergütungs- und -entschädigungsgesetzes verwiesen. Diese Regelung entspricht der im Bundesverfassungsschutzgesetz.

#### **Zu Nr. 2 – § 26 a Abs. 1 Nr. 2 G 10-Kommission**

In Absatz 1 Nr. 2 wird die Beteiligung bzw. Unterrichtung der G 10-Kommission über die Anordnung von Auskunftsverlangen über Telekommunikationsbestandsdaten nach § 8 a Absatz 1 Satz 3 und 4, die durch die Innenministerin oder den Innenminister erfolgt, ergänzt.

#### **Zu Artikel 3**

Bestandsdatenauskunft anhand dynamischer Internetprotokoll-Adressen stellt einen Eingriff in Artikel 10 Absatz 1 des Grundgesetzes dar (Art. 1 Nr. 2a - § 180 a Abs. 2 LVwG; Art. 2 Nr. 1a - § 8a Abs. 1 LVerfSchG). Für derartige Eingriffe gilt das Zitiergebot gemäß Artikel 19 Absatz 1 Satz 2 des Grundgesetzes. Dem Zitiergebot wird mit der Vorschrift entsprochen.

#### **Zu Artikel 4**

Artikel 4 regelt das Inkrafttreten.