

**Stand 09.08.13**

## **Gesetz zur Änderung des Polizeigesetzes und des Landesverfassungsschutzgesetzes**

Vorblatt

### A. Zielsetzung

Das Bundesverfassungsgericht hat mit Beschluss vom 24. Januar 2012 (BVerfGE 130, 151 ff.) festgestellt, dass die Ermächtigung zur Bestandsdatenauskunft in § 113 des Telekommunikationsgesetzes sowie in den Fachgesetzen der Sicherheits- und Verfassungsschutzbehörden unzureichend sei. Erforderlich sei eine qualifizierte Rechtsgrundlage zur Auskunftspflicht der Telekommunikationsunternehmen und zur Zuordnung dynamischer Internetprotokoll-Adressen. Die Voraussetzungen für eine Auskunft über Zugangssicherungs\_codes seien zudem dahingehend zu ergänzen, dass zugleich die Bedingungen für die Datennutzung vorliegen müssen. Das Gericht hatte jedoch festgestellt, dass die beanstandeten Regelungen übergangsweise bis längstens Ende Juni 2013 angewendet werden dürfen. Der Bundesgesetzgeber hat für seinen Kompetenzbereich die Normen den verfassungsrechtlichen Vorgaben bereits angepasst. Mit dem Gesetz zur Änderung des Polizeigesetzes und des Gesetzes über den Verfassungsschutz in Baden-Württemberg soll die Entscheidung des Bundesverfassungsgerichts nun auf Landesebene umgesetzt werden.

### B. Wesentlicher Inhalt

Mit der Gesetzesänderung sollen den Vorgaben des Bundesverfassungsgerichtes entsprechende Ermächtigungsgrundlagen für materielle Anforderungen

- an die Datenerhebung durch Polizei und Landesamt für Verfassungsschutz mittels identifizierender Zuordnung dynamischer Internetprotokoll-Adressen,
- an die Auskunftserteilung über Zugangssicherungs\_codes von Mobilfunkendgeräten und Speichereinrichtungen sowie
- an die Erhebung von Bestandsdaten durch das Landesamt für Verfassungsschutz

geschaffen werden. Gleichzeitig wird klargestellt, dass die Befugnis zur Erhebung von Bestands- und Nutzungsdaten (Nutzungsdaten nur im Polizeibereich) auch solche nach dem Telemediengesetz umfasst.

### C. Alternativen

Keine.

### D. Wesentliche Ergebnisse der Regelungsfolgenabschätzung und Nachhaltigkeitsprüfung

Durch die Änderung des Polizeigesetzes und des Landesverfassungsschutzgesetzes sind keine erheblichen Auswirkungen auf die ökonomischen, ökologischen und sozialen Verhältnisse zu erwarten. Auch nennenswerte Kosten für die öffentlichen Haushalte oder für Private entstehen durch die Gesetzesänderungen nicht.

## **Gesetz zur Änderung des Polizeigesetzes und des Landesverfassungsschutzgesetzes**

Vom ...

### Artikel 1 Änderung des Polizeigesetzes

§ 23a des Polizeigesetzes in der Fassung vom 13. Januar 1992 (GBl. S. 1, ber. S. 596, 1993 S. 155), zuletzt geändert durch Artikel 1 und 2 des Gesetzes vom 20. November 2012 (GBl. S. 625), wird wie folgt geändert:

1. In Absatz 1 Satz 1 werden nach dem Wort „Telekommunikationsgesetzes“ die Wörter „und Nutzungsdaten im Sinne des § 15 Absatz 1 Satz 2 Nummer 2 und 3 des Telemediengesetzes“ eingefügt.
2. Absatz 2 wird wie folgt geändert:
  - a) In Satz 5 werden nach dem Wort „wird“ die Wörter „oder eine Bezeichnung des Nutzers der Telemedien, dessen Daten erhoben werden“ eingefügt.
  - b) In Satz 6 werden nach dem Wort „Telekommunikation“ die Wörter „oder Telemediennutzung“ eingefügt.
3. Absatz 5 wird wie folgt geändert:
  - a) In Satz 1 werden nach dem Wort „Telekommunikationsdienste“ die Wörter „oder Telemediendienste“ eingefügt.
  - b) In Satz 2 werden nach dem Wort „Verkehrsdaten“ die Wörter „und Nutzungsdaten“ eingefügt.
  - c) In Satz 3 werden nach dem Wort „Telekommunikations-Überwachungsverordnung“ die Wörter „sowie dem Telemediengesetz“ eingefügt.
4. Absatz 9 erhält folgende Fassung:

„Der Polizeivollzugsdienst kann ohne Wissen des Betroffenen Daten im Sinne der

§§ 95 und 111 des Telekommunikationsgesetzes und der §§ 14 und 15 Absatz 1 Satz 2 Nummer 1 des Telemediengesetzes über die in §§ 6 und 7 sowie unter den Voraussetzungen des § 9 über die dort genannten Personen erheben, soweit dies zur Abwehr einer Gefahr für die öffentliche Sicherheit erforderlich ist. Die Auskunft nach Satz 1 darf zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder eine gemeine Gefahr auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse sowie weiterer zur Individualisierung erforderlicher technischer Daten verlangt werden. Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, darf die Auskunft zur Abwehr der in Satz 2 genannten Gefahren nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. Absatz 1 Satz 4 sowie Absatz 5 Satz 1, 3 und 4 gelten entsprechend. Die betroffenen Personen sind von Maßnahmen nach Satz 2 und Satz 3 zu unterrichten, soweit und sobald hierdurch der Zweck der Maßnahme nicht vereitelt wird. Die Unterrichtung unterbleibt, wenn die betroffene Person vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Unterrichtung zurückgestellt oder von ihr abgesehen, sind die Gründe aktenkundig zu machen.“

## Artikel 2

### Änderung des Landesverfassungsschutzgesetzes

Das Landesverfassungsschutzgesetz in der Fassung vom 5. Dezember 2005 (GBl. 2006 S. 1) wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach den Wörtern „§ 5 a Einholung von Auskünften bei nicht-öffentlichen Stellen“ folgende Zeile eingefügt:

„5 b Weitere Auskunftsverlangen“.

2. Nach § 5 a wird folgender § 5 b eingefügt:

## „§ 5 b

## Weitere Auskunftsverlangen

(1) Soweit dies zur Erfüllung der Aufgaben des Landesamtes für Verfassungsschutz erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste und beziehungsweise oder Telemediendienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 Telekommunikationsgesetz sowie nach § 14 Telemediengesetz erhobenen Daten verlangt werden. Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse sowie weiterer zur Individualisierung erforderlicher technischer Daten verlangt werden.

(3) Aufgrund eines Auskunftsverlangens nach Absatz 1 oder 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste und beziehungsweise oder Telemediendienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich, vollständig und richtig zu übermitteln.

(4) Das Landesamt für Verfassungsschutz hat für ihm erteilte Auskünfte eine Entschädigung zu gewähren, deren Umfang sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes bemisst; die Vorschriften über die Verjährung in § 2 Absatz 1 und 4 des Justizvergütungs- und -entschädigungsgesetzes finden entsprechend Anwendung.“

## Artikel 3

## Einschränkungen von Grundrechten

Durch Artikel 1 und 2 wird das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) eingeschränkt.

Artikel 4  
Inkrafttreten

(1) Dieses Gesetz tritt am 1. März 2014 in Kraft.

(2) Die polizeiliche Befugnis zur Erhebung von Bestandsdaten ist spätestens fünf Jahre nach ihrem Inkrafttreten zu evaluieren.

Stuttgart, den

Die Regierung des Landes Baden-Württemberg:

## **Begründung**

### *A. Allgemeiner Teil*

#### I. Änderung des Polizeigesetzes

Mit Beschluss vom 24.01.2012 (BVerfGE 130, 151 ff.) hat das Bundesverfassungsgericht zu § 113 Telekommunikationsgesetz (TKG) festgestellt, dass

- a) Telekommunikationsbestandsdaten durch die Sicherheitsbehörden nur mittels einer qualifizierten Rechtsgrundlage für den Datenabruf erhoben werden dürfen,
- b) die bislang nach überwiegender Auffassung den § 111 ff. TKG zugeordneten dynamischen Internetprotokoll-Adressen nicht der Abrufermächtigung des § 113 TKG unterfielen, sondern hierfür eine normenklare Regelung, die den Eingriff in das Fernmeldegeheimnis beachtet, erforderlich sei und
- c) der bisher durch § 113 Absatz 1 Satz 2 TKG eröffnete Zugriff auf Zugangssicherungs-codes unverhältnismäßig sei, da nicht zugleich festgelegt werde, wann und in welchem Umfang die Behörden von den Daten Gebrauch machen dürfen.

Um eine Anpassung der gesetzlichen Regelungen zu ermöglichen, hatte das Bundesverfassungsgericht eine Übergangsfrist bis zum 30. Juni 2013 festgesetzt.

Die unter a) erwähnte qualifizierte Ermächtigungsgrundlage für die polizeiliche Erhebung von Bestandsdaten wurde bereits mit Gesetz vom 20. November 2012 (GBl. S. 625) in § 23 a Absatz 9 PolG geschaffen.

Die Änderung des Polizeigesetzes aufgrund der unter b) und c) genannten Feststellungen des Bundesverfassungsgerichts setzte dagegen zunächst die Anpassung durch den Bundesgesetzgeber voraus, wie sie mit dem Gesetz zur Änderung des TKG und zur Neuregelung der Bestandsdatenauskunft vom 20. Juni 2013 erfolgt ist (BGBl. I S. 1602). Hierzu korrespondierend soll § 23 a Absatz 9 PolG hinsichtlich der Zuordnung dynamischer Internetprotokoll-Adressen sowie für den Zugriff auf Zugangssicherungs-codes ergänzt werden.

Der Beschluss des Bundesverfassungsgerichts zum TKG ist sinngemäß auf das Telemediengesetz (TMG) übertragbar. Hinzu treten Überschneidungen und Abgrenzungsschwierigkeiten zwischen TKG und TMG für einzelne Internetdienste. Jedoch

hat die Polizei auf gleichartige Gefahren zu reagieren. Zum Beispiel bedarf es bei Androhung eines Suizids in einem Internetforum zur Identifizierung des Nutzers der Auskunft über dessen selbstgewählte Kennung (Nickname) durch den Telemediendiensteanbieter. Wenn dabei nicht der tatsächliche Name, sondern nur die genutzte dynamische Internetprotokoll-Adresse übermittelt werden kann, muss als zweiter Schritt beim Telekommunikationsdiensteanbieter die Zuordnung der IP-Adresse zu dem Anschlussinhaber und dessen Adresse folgen. Deshalb ist klarzustellen, dass die Bestands- und Nutzungsdaten des TMG ebenfalls erhoben und genutzt werden dürfen. Dabei werden die Daten zur Identifizierung des Nutzers (§§ 14 und 15 Absatz 1 Satz 2 Nummer 1 TMG) wegen der Vergleichbarkeit zu Telekommunikationsbestandsdaten an diese Erhebungsvoraussetzungen geknüpft. Demgegenüber dürfen die Daten, die Telekommunikationsverkehrsdaten gleichzusetzen sind (§ 15 Absatz 1 Satz 2 Nummer 2 und 3 TMG, z. B. Dauer oder Umfang einer Telemediennutzung), nur unter den erhöhten Voraussetzungen aus § 23a Absatz 1 PolG erhoben werden.

Die Möglichkeit, unter den Voraussetzungen von § 112 TKG durch die Bundesnetzagentur Auskunft über Bestandsdaten zu erhalten, besteht fort. Das Bundesverfassungsgericht hatte im Beschluss vom 24. Januar 2012 die Regelung in § 112 TKG als verfassungsgemäß bestätigt.

## II. Änderung des Gesetzes über den Verfassungsschutz in Baden-Württemberg

Zum Beschluss des Bundesverfassungsgerichts vom 24. Januar 2012 (BVerfGE 130, 151ff.) sowie der aktuellen Gesetzgebung des Bundes wird auf die Ausführungen unter I. verwiesen.

Mit der Neufassung des § 5 b Landesverfassungsschutzgesetz (LVSG) wird die unter I. a) benannte qualifizierte Ermächtigungsgrundlage für die Erhebung von Bestandsdaten geschaffen.

Da die Forderung des Bundesverfassungsgerichts nach qualifizierten Rechtsgrundlagen für den Abruf von Bestandsdaten nicht nur für die Abfragen nach dem TKG gilt, sondern auch auf die Abfragen nach dem TMG übertragbar ist, wird mit der ausdrücklichen Nennung der Anbieter von Telekommunikationsdiensten und Telemediendiensten diese qualifizierte Rechtsgrundlage geschaffen.

Bislang hat man die Abfragen von Bestandsdaten bei Anbietern von Telekommunikationsdiensten auf § 5 Absatz 1 LVSG in Verbindung mit § 113 Absatz 1 Satz 1 TKG

und bei Anbietern von Telemediendiensten auf § 5 Absatz 1 LVSG in Verbindung mit § 14 Absatz 2 TMG gestützt. Neue Befugnisse für den Verfassungsschutz werden daher nicht begründet.

Bestandsdaten sind Daten eines Nutzers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste oder Telemediendienste erhoben werden (z.B. Name, Anschrift, Rufnummer, etc.).

Die Änderungen des LVSG aufgrund der unter I. b) und I. c) genannten Feststellungen des Bundesverfassungsgerichts setzten eine Anpassung der entsprechenden Vorschriften durch den Bundesgesetzgeber voraus. Diese sind im Gesetz zur Änderung des TKG und zur Neuregelung der Bestandsdatenauskunft vom 20. Juni 2013 (BGBl. I S. 1602) erfolgt. § 5 b LVSG n. F. nimmt die Regelungen hinsichtlich der Zuordnung dynamischer Internetprotokoll-Adressen und der Regelungen für den Zugriff auf Zugangssicherungs-codes auf. Die Änderungen beschränken sich dabei auf die Umsetzung der Vorgaben des Bundesverfassungsgerichts.

## *B. Einzelbegründung*

### I. Zu Artikel 1 (§ 23 a PolG)

#### Zu Nummer 1) (§ 23 a Absatz 1 Satz 1)

Durch die Regelung wird klargestellt, dass auch die den Verkehrsdaten im Sinne des § 96 Absatz 1 des Telekommunikationsgesetzes gleichzusetzenden Nutzungsdaten gemäß § 15 Absatz 1 Satz 2 Nummer 2 und 3 des Telemediengesetzes unter denselben Voraussetzungen wie Telekommunikationsverkehrsdaten erhoben werden dürfen. D. h., diese Telemediennutzungsdaten dürfen nur unter den in Absatz 1 benannten qualifizierten Voraussetzungen erhoben werden. Die dadurch definierte Gefahrenschwelle wäre nach der Rechtsprechung des Bundesverfassungsgerichts selbst für eingriffsintensivere Datenerhebungen von vorsorglich anlasslos gespeicherten Telekommunikationsverkehrsdaten zulässig (BVerfGE 125, 260, 329 f).

#### Zu Nummer 2 Buchstabe a) (§ 23 a Absatz 2 Satz 5)

Es handelt sich um eine redaktionelle Folgeänderung zu Nummer 1.

Zu Nummer 2 Buchstabe b) (§ 23 a Absatz 2 Satz 6)

Es handelt sich um eine redaktionelle Folgeänderung zu Nummer 1.

Zu Nummer 3 Buchstabe a) (§ 23 a Absatz 5 Satz 1)

Es handelt sich um eine redaktionelle Folgeänderung zu Nummer 1.

Zu Nummer 3 Buchstabe b) (§ 23 a Absatz 5 Satz 2)

Es handelt sich um eine redaktionelle Folgeänderung zu Nummer 1.

Zu Nummer 3 Buchstabe c) (§ 23 a Absatz 5 Satz 3)

Es handelt sich um eine redaktionelle Folgeänderung zu Nummer 1.

Zu Nummer 4 (§ 23 a Absatz 9)

Es wird klargestellt, dass Identifikationsmerkmale eines Telemediennutzers unter denselben Voraussetzungen erhoben werden dürfen wie die Bestandsdaten zur Identifikation des Nutzers eines Telekommunikationsvertrags. Die Daten werden beispielsweise benötigt, um bei Ankündigung einer Amoktat, eines Suizids oder einer anderen Gefahr in einem Chat oder ähnlichen Internetmedium den unter einem Kurz- oder Phantasienamen (Nickname) auftretenden Betroffenen identifizieren und die Gefahr abwehren zu können.

Die Zulässigkeit von Auskunftsverlangen wird auf Gefahren für die öffentliche Sicherheit beschränkt.

Mit Absatz 9 Satz 2 und 3 wird, korrespondierend zu § 113 des Telekommunikationsgesetzes (TKG), die Erhebung der Daten zu Internetprotokoll-Adressen sowie den Zugriff auf Endgeräte geregelt. Für das ebenfalls betroffene Telemedienrecht gilt dies entsprechend.

In Satz 2 wird die polizeiliche Datenerhebungsbefugnis definiert und geregelt, dass die Auskunft nach Satz 1 auch anlassbezogen zu bekannten Internetprotokoll-Adressen, die zu einem bestimmten Zeitpunkt zugewiesen waren oder noch sind, zu erteilen ist (vgl. auch § 113 Absatz 1 Satz 3 TKG). Die Befugnis ist auf die Abwehr konkreter Gefahren für die benannten hochrangigen Rechtsgüter - ent-

sprechend deren Nennung in § 23 a Absatz 1 - beschränkt. Die Telekommunikations- und Telemediendiensteanbieter sind, ausgesprochen durch Verweis auf § 23 a Absatz 5, zur Auskunft verpflichtet.

Die technische Entwicklung kann es bedingen, dass zusätzlich zu der zu einem bestimmten Zeitpunkt zugewiesenen dynamischen Internetprotokoll-Adresse weitere technische Daten für die Zuordnung zu der betroffenen Person erforderlich sind. Dies ist u. a. bei der Verbreitung findenden Network Address Port Translation-Technologie der Fall, bei der dynamische Internetprotokoll-Adressen zeitgleich mehrfach an verschiedene Nutzer vergeben werden und daher die Auskunft über einen Nutzer der Einbeziehung zusätzlicher Daten bedarf.

Der Eingriff in das Fernmeldegeheimnis ist durch den mit der Ermächtigung verfolgten Zweck gerechtfertigt. Die Daten werden insbesondere zur Fahndungsunterstützung bei der Ermittlung von Personalien und Standort bei Amok- und Suizidankündigungen benötigt.

Satz 3 regelt die Datenerhebungsbefugnis für Auskünfte der Diensteanbieter über Zugangssicherungs\_codes wie z. B. Passwort, Persönliche Identifikationsnummer (PIN) oder Personal Unblocking Key (PUK) von Mobilfunkendgeräten oder Speichereinrichtungen (vgl. auch § 113 Absatz 1 Satz 2 TKG). Die Befugnis ist, ebenso wie in Satz 2, auf die Abwehr konkreter Gefahren für die hochrangigen Rechtsgüter Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder eine gemeine Gefahr beschränkt. Damit wird dem Umstand Rechnung getragen, dass der damit verbundene Eingriff in das Grundrecht auf informationelle Selbstbestimmung wegen der Überwindung der durch den Zugangssicherungscode gesetzten Barriere von den Betroffenen als besonders gravierend empfunden wird.

Satz 3 beinhaltet zudem die zusätzliche Einschränkung, dass für solche Daten die Auskunft nur verlangt werden darf, wenn zugleich die gesetzlichen Voraussetzungen für die Datennutzung vorliegen. Eine Behörde darf nach der Rechtsprechung des Bundesverfassungsgerichts nur dann die Möglichkeit zur Erhebung eines Zugangssicherungs\_codes haben, wenn sie diesen in der konkreten Abfragesituation zur Erfüllung ihrer Gefahrenabwehraufgabe benötigt (BVerfGE 130, 151, 207 ff.). Die materiellen und formellen Voraussetzungen für die Nutzung sind in eigenständigen Rechtsgrundlagen, z. B. § 20 PolG, geregelt.

Zur Gefahrenabwehr kann der Zugriff auf einen derartigen Zugangssicherungscode beispielsweise erforderlich werden, wenn die Daten auf einem aufgefundenen Mobiltelefon, das nur über PIN oder PUK reaktiviert werden kann, Hinweise zum Aufenthaltsort einer vermissten Person enthalten können. Die Nutzung dieser Daten, d. h. Anrufkontakte oder versandte Kurzmitteilungen, wäre dann nach §§ 20, 37 PolG zulässig.

Der Zugangssicherungscode ist aufgrund von §§ 46, 37 Absatz 1 Satz 1 PolG unverzüglich nach dessen Nutzung zu löschen.

Die in den Sätzen 5 bis 7 geregelte Unterrichtung des Betroffenen trägt dem Grundsatz der Transparenz Rechnung und eröffnet die Möglichkeit nachträglichen Rechtsschutzes. Sie korrespondiert mit der Neuregelung der Bestandsdatenauskunft durch den Bundesgesetzgeber etwa in § 100 j Absatz 4 StPO. Die Benachrichtigung ist auch dann nicht erforderlich, wenn der Betroffene bereits durch das Tätigwerden der Polizei, beispielsweise aus deren Erscheinen am Ort des geplanten Suizids, Kenntnis von der Datenverarbeitung hat oder haben muss.

## II. Zu Artikel 2 (§ 5 b LVSG)

### Zu Nummer 1 (Inhaltsübersicht)

Die Inhaltsübersicht wird angepasst.

### Zu Nummer 2 (§ 5 b neu)

In der Vergangenheit wurden die Abfragen von Bestandsdaten (z. B. Rufnummern und andere Anschlusskennungen, Name und Anschrift des Anschlussinhabers, etc.) bei Anbietern, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, auf § 5 Absatz 1 LVSG in Verbindung mit § 113 Absatz 1 Satz 1 TKG gestützt. Diese Rechtsgrundlage entspricht jedoch nicht den Vorgaben der o. g. Entscheidung des Bundesverfassungsgerichts. Mit § 5 b Absatz 1 wird nunmehr die geforderte qualifizierte Rechtsgrundlage zur Erhebung der Bestandsdaten geschaffen.

Wenngleich Gegenstand des Beschlusses des Bundesverfassungsgerichts vom 24. Januar 2012 nur die Regelungen des TKG waren, soll aus Klarstellungsgründen auch der Abruf von Bestandsdaten nach dem TMG in einer spezifischen Rechtsgrundlage erfasst werden. § 14 Absatz 2 TMG legt, vergleichbar § 113 Ab-

satz 1 Satz 1 TKG, insoweit bereits fest, in welchen Fällen die Diensteanbieter zur Übermittlung der betreffenden Daten berechtigt sind. Die Rechtsprechung des Bundesverfassungsgerichts ist insoweit übertragbar auf Auskunftsverlangen gemäß § 14 Absatz 2 TMG, die Bestandsdaten der Nutzerinnen und Nutzern von Telemedienangeboten (u. a. Videoplattformen, Online-Auktionen sowie soziale Netzwerke) betreffen.

In Absatz 1 Satz 1 wird die Berechtigung der Verfassungsschutzbehörde zur Abfrage von Bestandsdaten im manuellen Verfahren erteilt. Die Beauskunftung von Bestandsdaten ist nur im Einzelfall zulässig. 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 (Artikel 10-Gesetz - G 10).

Die Abfrage von Bestandsdaten bei Dienstleistern für Telemediendienste im Sinne des Absatzes 1 Satz 1 kommt z. B. dann in Betracht, wenn die Verfassungsschutzbehörde bei der Beobachtung eines extremistischen Versandhandels überprüfen möchte, ob der Betreiber des Versandhandels auch auf Verkaufsplattformen im Internet aktiv ist. Sie ist aber auch in den Fällen relevant, in denen der Urheber eines Videos, z. B. bei einem Spendenaufruf für eine legalistische extremistische Organisation, auf einem Videoportal zu identifizieren ist.

In Erfüllung der durch das Bundesverfassungsgericht aufgestellten Erfordernisse regelt Absatz 1 Satz 2, dass Abfragen von Bestandsdaten, sofern diese Passwörter oder sonstige Zugangsberechtigungen umfassen (insbesondere PIN und PUK für den Zugriff auf Mobilfunkendgeräte), nur zulässig sind, sofern die gesetzlichen Voraussetzungen für die Nutzung dieser erlangten Passwörter etc. vorliegen.

Die Regelungen zu dem Auskunftsverlangen aufgrund einer dynamischen Internetprotokoll-Adresse wurden in Absatz 2 aufgenommen. Die technische Entwicklung kann es bedingen, dass weitere technische Daten für die Zuordnung einer dynamischen Internetprotokoll-Adresse erforderlich sind. Dies ist u. a. bei der Verbreitung findenden Network Address Port Translation-Technologie der Fall, bei der dynamische Internetprotokoll-Adressen zeitgleich mehrfach an verschiedene Nut-

zer vergeben werden und daher die Auskunft über einen Nutzer der Einbeziehung zusätzlicher Daten zur Individualisierung bedarf. Andernfalls würden auch die Daten der anderen Nutzer herausgegeben, denen zeitgleich die Internetprotokoll-Adresse zugewiesen wurde, die aber nicht im Fokus der Verfassungsschutzbehörde stehen. Daher wurde eine entsprechende Ergänzung in Absatz 2 vorgenommen.

Die Daten über die Zuordnung der Internetprotokoll-Adressen werden z. B. in den Fällen benötigt, in denen der Verfassungsschutzbehörde als Ermittlungsansatz lediglich eine Internetprotokoll-Adresse bekannt ist. Dies ist unter anderem dann der Fall, wenn Personen über Internettelefonie verschlüsselt miteinander kommunizieren und die Verfassungsschutzbehörde im Rahmen einer Überwachungsmaßnahme nach dem Artikel 10-Gesetz lediglich die Internetprotokoll-Adresse des Kommunikationspartners der überwachten Person erlangt.

Mit der Regelung in Absatz 3 werden die Diensteanbieter ausdrücklich zur Auskunftserteilung verpflichtet. Dies entspricht den Vorgaben des Bundesverfassungsgerichts.

In Absatz 4 wird eine Regelung über den Anspruch der zur Auskunft verpflichteten Anbieter von geschäftsmäßigen Telekommunikationsdiensten und Telemediendiensten auf eine Entschädigung für die Auskunftserteilung geschaffen. Diese Regelung beinhaltet Entschädigungen für Auskünfte zu Bestandsdaten. Hinsichtlich der Höhe wird auf die entsprechende Anwendung des § 23 des Justizvergütungs- und -entschädigungsgesetzes (JVEG) verwiesen. Diese Regelung entspricht derjenigen im Bundesverfassungsschutzgesetz. Auch die Telemediendiensteanbieter, die das JVEG nicht ausdrücklich erwähnt, werden auf der Grundlage des § 23 JVEG entschädigt.

### III. Zu Artikel 3

Die Bestimmung trägt dem Zitiergebot Rechnung.

### IV. Zu Artikel 4

Die Bestimmung in Absatz 1 regelt das Inkrafttreten.

Die Befugnis zur Bestandsdatenerhebung durch die Polizei in § 23 a Absatz 9 PolG wird spätestens fünf Jahre nach dem Inkrafttreten evaluiert. Die Bundesregierung

berichtet zum 31. Dezember 2015 dem Bundestag über den Stand der Einführung des Internetprotokolls Version 6 durch Diensteanbieter und die Auswirkungen auf den Schutz der Grundrechte und die Ermittlungsmöglichkeiten der in § 113 des Telekommunikationsgesetzes benannten Stellen (Artikel 10 des Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft). Eine Evaluation der neuen landesrechtlichen Regelungen vor diesem Zeitpunkt ist untunlich.