LANDTAG RHEINLAND-PFALZ
17. Wahlperiode

Drucksache 17/2895
26. 04. 2017

Gesetzentwurf

der Fraktionen der SPD, FDP und BÜNDNIS 90/DIE GRÜNEN

…tes Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes

A. Problem und Regelungsbedürfnis

Aufgrund der anhaltenden Bedrohungslage durch den internationalen Terrorismus und die besonders sozialschädlichen Kriminalitätsphänomene des Extremismus und des Wohnungseinbruchdiebstahls ist eine Stärkung der polizeilichen Befugnisse erforderlich. So soll die Polizei die Befugnis zum anlassbezogenen Einsatz von Kennzeichenlesegeräten erhalten, um bei Gefahren für die öffentliche Sicherheit die Fahndung nach Fahrzeugen und deren Insassen zu verbessern. Darüber hinaus werden verdeckte Datenerhebungen bereits im Vorfeld konkreter Gefahren zugelassen, soweit es um die Verhütung terroristischer Straftaten geht. In seinem Urteil vom 20. April 2016 (1 BvR 966/09, 1 BvR 1140/09) zum Bundeskriminalamtgesetz hat das Bundesverfassungsgericht (BVerfG) deutlich gemacht, dass der Gesetzgeber von Verfassungs wegen auch bei eingriffsintensiven heimlichen Überwachungsmaßnahmen nicht daran gehindert ist, die Einschreitschwelle für bestimmte Bereiche der Straftatenverhütung weiterzuziehen. In Bezug auf terroristische Straftaten können Überwachungsmaßnahmen bereits dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird (BVerfG, a. a. O, Rn. 112).

Ferner wird die Fortentwicklung polizeilicher Einsatzmittel aufgegriffen und eine bereichsspezifische Ermächtigungsnorm für den Einsatz der Bodycam eingeführt. Im Rahmen eines Pilotprojekts hat sich gezeigt, dass der Einsatz mobiler Kameras geeignet ist, um den Schutz von Polizeibeamtinnen und Polizeibeamten sowie von Dritten vor gewalttätigen Übergriffen zu verbessern.

Weiterer Anpassungsbedarf ergibt sich aus einer Entscheidung des Bundesverfassungsgerichts zur Bestandsdatenauskunft nach § 113 des Telekommunikationsgesetzes (TKG) vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 6 Abs. 41 des Gesetzes vom 13. April 2017 (BGBl. I S. 872). Das Bundesverfassungsgericht hat der in der Vergangenheit üblichen Praxis, Anfragen der Sicherheitsbehörden zu Bestandsdaten im manuellen Auskunftsverfahren nach § 113 Abs. 1 Satz 1 TKG auf schlichte Datenerhebungsgeneralklauseln zu stützen, eine Absage erteilt. Erforderlich sei vielmehr eine bereichsspezifische Abrufnorm, die eine entsprechende Verpflichtung der Telekommunikationsdiensteanbieter gegenüber der abrufberechtigten Behörde aus sich heraus normenklar begründet (BVerfG, Beschluss vom 24. Januar 2012, 1 BvR 1299/05, juris, Rn. 167). Mit diesem Gesetzentwurf wird die für die Abfrage von Bestandsdaten im manuellen Auskunftsverfahren erforderliche bereichsspezifische Ermächtigungsnorm geschaffen.

Ein wesentlicher Teil des Gesetzentwurfs dient der Umsetzung der Entscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtgesetz. Mit dem Urteil vom 20. April 2016 hat das Gericht grundlegende Anforderungen an die konkrete Ausgestaltung heimlicher Überwachungsmaßnahmen sowie die weitere Verwendung der Daten bis hin zur Datenübermittlung formuliert. Mit diesem Gesetzentwurf werden

Druck: Landtag Rheinland-Pfalz, 17. Mai 2017 – Vorabdruck verteilt am 27. April 2017

zunächst die Vorgaben an die Begrenzung des Adressatenkreises bei eingriffsintensiven heimlichen Datenerhebungen, den Richtervorbehalt, den Kernbereichsschutz, die Zweckänderung, die Berichtspflichten und die aufsichtliche Kontrolle durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit umgesetzt. Weitere erforderliche Änderungen, z. B. zur Datenübermittlung an Drittstaaten, bleiben einem weiteren Gesetzgebungsvorhaben vorbehalten, mit dem auch 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 des Rates (ABl. EU Nr. L 119/, S. 89) umgesetzt werden soll.

B. Lösung

Durch die vorgesehenen Änderungen werden die polizeilichen Befugnisse gestärkt, damit die Polizei – nicht zuletzt in Anbetracht der angespannten Sicherheitslage aufgrund der Gefahren durch den internationalen Terrorismus – auch künftig die Sicherheit der Bürgerinnen und Bürger gewährleisten kann. Gleichzeitig werden wesentliche Vorgaben aus dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 umgesetzt.

C. Alternativen

Keine.

D. Kosten

Für die Beschaffung von Videoüberwachungstechnik zur Überwachung öffentlicher Plätze sind Kosten in Höhe von 210 000 Euro veranschlagt. Die Höhe der Kosten speziell für Videotechnik zur Überwachung von Großveranstaltungen kann gegenwärtig nicht beziffert werden. Das Kostenvolumen für die Beschaffung von Kennzeichenlesegeräten beläuft sich nach vorläufiger Schätzung auf zunächst ca. 350 000 Euro. Im Jahr 2017 sollen darüber hinaus – zusätzlich zu den bereits vorhandenen Bodycams – 150 weitere Bodycams beschafft werden. Hierdurch fallen Kosten in Höhe von mindestens 135 000 Euro an, die bereits etatisiert sind.

Kosten können dem Land auch aufgrund der neuen Befugnis zur Bestandsdatenabfrage durch die Entschädigung der Telekommunikationsunternehmen nach dem Justizvergütungs- und -entschädigungsgesetz vom 5. Mai 2004 (BGBl. I S. 718, 776), zuletzt geändert durch Artikel 5 Abs. 2 des Gesetzes vom 11. Oktober 2016 (BGBl. I S. 2222), entstehen. Soweit für die Auskunftserteilung nicht auf Verkehrsdaten zurückgegriffen werden muss, beträgt die Entschädigung je angefragtem Kundendatensatz 18 Euro; für Auskünfte über Bestandsdaten, zu deren Erteilung auf Verkehrsdaten zurückgegriffen werden muss (wie bei der Identifizierung dynamischer IP-Adressen), beträgt die Entschädigung für bis zu zehn in demselben Verfahren gleichzeitig angefragte Kennungen 35 Euro. Angesichts der zu erwartenden geringen Anzahl von Auskunftsersuchen im manuellen Auskunftsverfahren nach § 113 TKG zu Zwecken der Gefahrenabwehr dürfte der Umfang der zusätzlichen Kosten gering sein.

Mit seinem Urteil zum Bundeskriminalamtgesetz vom 20. April 2016 hat das Bundesverfassungsgericht die bisherige Rechtsprechung zu den verfassungsrechtlichen Anforderungen an die Zweckbindung und Zweckänderung fortentwickelt. So hat es unter anderem ausgeführt, dass sich die Verhältnismäßigkeitsanforderungen für eine zweckändernde Datenverwendung am Grundsatz der hypothetischen Datenneuerhebung zu orientieren haben. Danach muss die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten (BVerfG, a. a. O, Rn. 287 f.). Die bestehende IT-Architektur des Bundeskriminalamtes ist für die Umsetzung der Vorgaben des Bun-

desverfassungsgerichts nicht geeignet und deshalb grundlegend neu zu strukturieren. Damit verbunden sind auch Anpassungen der rheinland-pfälzischen Fall- und Vorgangsbearbeitungssysteme sowie des Fahndungssystems. Hierdurch entsteht ein Erfüllungsaufwand in noch nicht bezifferbarer Höhe.

...tes Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes

Der Landtag Rheinland-Pfalz hat das folgende Gesetz beschlossen:

Artikel 1

Das Polizei- und Ordnungsbehördengesetz (POG) in der Fassung vom 10. November 1993 (GVBl. S. 595), zuletzt geändert durch Artikel 4 des Gesetzes vom 19. Dezember 2014 (GVBl. S. 332), BS 2012-1, wird wie folgt geändert:

1. In § 13 Abs. 2 wird das Wort „gegenwärtigen“ gestrichen.
2. In § 18 Abs. 3 Satz 7 werden die Worte „Beamten des höheren Dienstes“ durch die Worte „Beamten mit der Befähigung für das vierte Einstiegsamt“ ersetzt.
3. § 27 wird wie folgt geändert:

   a) Nach Absatz 2 wird folgender neue Absatz 3 eingefügt:

      „(3) Die Polizei kann bei öffentlichen Veranstaltungen und Ansammlungen, die nicht dem Versammlungsgesetz unterliegen und an denen voraussichtlich mehr als 500 Personen zeitgleich teilnehmen, zur vorbeugenden Bekämpfung von Straftaten personenbezogene Daten von Teilnehmern durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen erheben.“

   b) Die bisherigen Absätze 3 und 4 werden Absätze 4 und 5.

   c) Der bisherige Absatz 5 wird Absatz 6 und wie folgt geändert:

      aa) In Satz 1 wird die Verweisung „Absätzen 1 bis 4“ durch die Verweisung „Absätzen 1 bis 5“ ersetzt.

      bb) In Satz 2 wird nach den Worten „Bild- und Tonaufzeichnungen“ die Verweisung „nach den Absätzen 1, 2, 4 und 5“ eingefügt.

      cc) Folgender neue Satz 3 wird eingefügt:

      „Nach Absatz 3 erlangte Daten sowie daraus gefertigte Unterlagen sind unverzüglich zu löschen oder zu vernichten, soweit sich aus ihnen nicht im Einzelfall konkrete Ermittlungsansätze zur
      1. Verfolgung oder Verhütung von Straftaten oder
      2. zur Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für Leib, Leben oder Eigentum einer Person

      ergeben und die Verwendung der Daten zu diesem Zweck erforderlich ist.“

      dd) Der bisherige Satz 3 wird Satz 4.

   d) der bisherige Absatz 6 wird Absatz 7.

e) Der bisherige Absatz 7 wird Absatz 8 und wie folgt geändert:

In Satz 2 wird die Verweisung „Absätzen 1 und 3“ durch die Verweisung „Absätzen 1 und 4“ ersetzt.

4. Nach § 27 werden folgende neue §§ 27 a und 27 b eingefügt:

„§ 27 a
Mobile Bild- und Tonaufzeichnungsgeräte

(1) Die Polizei kann in öffentlich zugänglichen Räumen personenbezogene Daten durch den offenen Einsatz körpernah getragener Bild- und Tonaufzeichnungsgeräte erheben, wenn durch Tatsachen begründete Anhaltspunkte die Annahme rechtfertigen, dass dies zum Schutz eines Polizeibeamten oder eines Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist.

(2) Die Datenerhebung darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen sind. Datenerhebungen in einem durch ein Berufsgeheimnis geschützten Vertrauensverhältnis im Sinne des § 53 Abs. 1 und des § 53 a Abs. 1 der Strafprozessordnung sind unzulässig. Auf eine Datenerhebung nach Absatz 1 ist in geeigneter Form hinzuweisen.

(3) Die kurzzeitige Datenerfassung im Zwischenspeicher der Bild- und Tonaufzeichnungsgeräte durch Vorabaufnahmen (Prerecording) ist unzulässig.

(4) Bild- und Tonaufzeichnungen nach Absatz 1 sind nach 30 Tagen zu löschen, soweit diese nicht benötigt werden
1. zur Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung,
2. im Einzelfall zur Gefahrenabwehr oder
3. im Einzelfall, insbesondere auf Verlangen des Betroffenen, für die Überprüfung der Rechtmäßigkeit von aufgezeichneten polizeilichen Maßnahmen.

Die Zweckänderung der Daten muss im Einzelfall festgestellt und dokumentiert werden.

§ 27 b
Anlassbezogene Kennzeichenerfassung

(1) Die Polizei kann im öffentlichen Verkehrsraum vorübergehend und nicht flächendeckend die Kennzeichen von Fahrzeugen ohne Wissen der Person durch den Einsatz technischer Mittel automatisiert erheben, wenn
1. dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben, Freiheit oder Eigentum einer Person,
2. dies zur Abwehr einer gegenwärtigen Gefahr erforderlich ist und die Voraussetzungen für eine Identitätsfeststellung nach § 10 Abs. 1 Satz 2 Nr. 1 bis 3 vorliegen oder
3. eine Person oder ein Fahrzeug ausgeschrieben wurde und Tatsachen die Annahme rechtfertigen, dass die Begehung einer Straftat von erheblicher Bedeutung durch diese Person oder mittels des ausgeschriebenen Fahrzeugs unmittelbar bevorsteht.

(2) Die erfassten Kennzeichen dürfen mit dem Fahndungsbestand der Sachfahndungsdateien des beim Bundeskriminalamt nach den Vorschriften des Bundeskriminalamtgesetzes und des beim Landeskriminalamt Rheinland-Pfalz nach den Vorschriften dieses Gesetzes geführten

polizeilichen Informationssystems abgeglichen werden. Die Sachfahndungsdateien des polizeilichen Informationssystems umfassen auch die nach den Vorschriften des Schengener Durchführungsübereinkommens zulässigen Ausschreibungen von Fahrzeugkennzeichen im Schengener Informationssystem. Der Abgleich nach Satz 1 beschränkt sich auf Kennzeichen von Fahrzeugen, die

1. nach § 32 dieses Gesetzes, den §§ 163 e und 463 a der Strafprozessordnung, Artikel 99 des Schengener Durchführungsübereinkommens, § 17 Abs. 3 des Bundesverfassungsschutzgesetzes und § 20 i des Bundeskriminalamtgesetzes,
2. aufgrund einer Gefahr für Zwecke der Gefahrenabwehr,
3. aufgrund des Verdachts einer Straftat für Zwecke der Strafverfolgung,
4. aus Gründen der Strafvollstreckung

ausgeschrieben sind. Der Abgleich darf nur mit vollständigen Kennzeichen des Fahndungsbestands erfolgen.

(3) Sofern das ermittelte Kennzeichen nicht im Fahndungsbestand enthalten ist, sind die erhobenen Daten sofort nach Durchführung des Datenabgleichs automatisiert zu löschen. Ist das ermittelte Kennzeichen im Fahndungsbestand enthalten (Trefferfall), dürfen das Kennzeichen sowie Angaben zu Ort, Datum, Uhrzeit und Fahrtrichtung gespeichert werden. Im Trefferfall ist unverzüglich die Übereinstimmung zwischen den erfassten Daten und den Daten aus dem Fahndungsbestand zu überprüfen. Liegt keine Übereinstimmung vor, sind die Daten sofort und spurenlos zu löschen. Das Fahrzeug und die Insassen können im Trefferfall angehalten werden. Weitere Maßnahmen dürfen erst erfolgen, wenn die Übereinstimmung zwischen den erfassten Daten und den Daten aus dem Fahndungsbestand festgestellt wurde. Bei Datenübereinstimmung können die Daten polizeilich verarbeitet und im Falle des Absatzes 1 Nr. 3 zusammen mit den gewonnenen Erkenntnissen an die ausschreibende Stelle übermittelt werden. Sofern der Abgleich der erhobenen Daten mit dem Fahndungsbestand zwar einen Treffer ergibt, die Ausschreibung im Fahndungsbestand jedoch nicht im Zusammenhang mit der Verfolgung der in Absatz 1 Nr. 1 bis 3 genannten Zwecke steht, sind die Daten sofort und spurenlos zu löschen, es sei denn, sie werden zur Verfolgung einer Straftat von erheblicher Bedeutung benötigt."

5. § 28 wird wie folgt geändert:

   a) Absatz 1 Satz 1 wird wie folgt geändert:

      aa) Nummer 2 erhält folgende Fassung:

         „2. Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise Straftaten von erheblicher Bedeutung begehen und die Datenerhebung zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist,"

bb) Nach der Nummer 2 wird folgende neue Nummer 3 eingefügt:

„3. Personen, deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine in § 129 a Abs. 1 und 2 des Strafgesetzbuchs bezeichnete Straftat begeht, die dazu bestimmt ist

a) die Bevölkerung auf erhebliche Weise einzuschüchtern,

b) eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder

c) die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen,

und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen können,“

cc) Die bisherigen Nummern 3 und 4 werden Nummern 4 und 5.

b) Absatz 2 wird wie folgt geändert:

aa) In Nummer 2 werden nach dem Wort „Bildaufzeichnungen“ die Worte „sowie zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes“ gestrichen.

bb) Folgende neue Nummer 3 wird eingefügt:

„3. der verdeckte Einsatz technischer Mittel zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes,“

cc) Die bisherigen Nummern 3 bis 5 werden Nummern 4 bis 6.

c) Absatz 4 erhält folgende Fassung:

„(4) Der Einsatz besonderer Mittel nach

1. Absatz 2 Nr. 1,
2. Absatz 2 Nr. 2, soweit Bildaufzeichnungen bestimmter Personen durchgehend länger als 24 Stunden oder über einen Zeitraum von mehr als einer Woche angefertigt werden sollen,
3. Absatz 2 Nr. 3 bis 5

bedarf der richterlichen Entscheidung. Die Maßnahme nach Absatz 2 Nr. 1 bis 3 ist auf höchstens einen Monat zu befristen; im Fall des Absatzes 2 Nr. 4 und 5 ist die Maßnahme auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als denselben Zeitraum ist zulässig, sofern die Voraussetzungen der Anordnung weiterhin vorliegen. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. § 21 Abs. 1 Satz 3 gilt entsprechend. Bei Gefahr im Verzug kann die Maßnahme vorläufig durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten mit der Befähigung für das vierte Einstiegsamt angeordnet werden; die richterliche Entscheidung ist unverzüglich nachzuholen.“

d) Nach Absatz 4 wird folgender neue Absatz 5 eingefügt:

„(5) Der Einsatz besonderer Mittel nach Absatz 2 Nr. 2, soweit er keiner richterlichen Entscheidung nach Absatz 4 Satz 1 Nr. 2 bedarf, und Absatz 2 Nr. 6 darf nur durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten mit der Befähigung für das vierte Einstiegsamt angeordnet werden. Die Maßnahme ist zu befristen und kann wiederholt angeordnet werden. Bei Gefahr im Verzug können besondere Mittel nach Absatz 2 Nr. 2 und 6 vorläufig eingesetzt werden; eine Entscheidung nach Satz 1 ist unverzüglich nachzuholen.“

e) Der bisherige Absatz 5 wird Absatz 6 und erhält folgende Fassung:

„(6) Nach Absatz 2 Satz 1 Nr. 1, 3 bis 5 erlangte personenbezogene Daten sind besonders zu kennzeichnen. Nach einer Übermittlung ist die Kennzeichnung durch die Empfänger aufrechtzuerhalten. Solche Daten dürfen für einen anderen Zweck verwendet werden, soweit sich aus ihnen konkrete Ermittlungsansätze zur

1. Verfolgung oder Verhütung von Straftaten von erheblicher Bedeutung nach Absatz 3 oder
2. zur Abwehr einer Gefahr für Leib oder Leben einer Person

ergeben und die Verwendung der Daten zu diesem Zweck erforderlich ist. Die Zweckänderung muss im Einzelfall festgestellt und dokumentiert werden.“

f) Nach Absatz 6 wird folgender neue Absatz 7 eingefügt:

„(7) Nach Absatz 2 Satz 1 Nr. 2 und 6 erlangte personenbezogene Daten dürfen für einen anderen Zweck verwendet werden, soweit dies zur Verfolgung oder Verhütung von Straftaten von erheblicher Bedeutung nach Absatz 3 oder zur Abwehr einer Gefahr für Leib oder Leben einer Person erforderlich ist. Die Zweckänderung der Daten muss im Einzelfall festgestellt und dokumentiert werden.“

g) Der bisherige Absatz 6 wird Absatz 8.

6. § 29 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Die Polizei kann zur Abwehr einer dringenden Gefahr für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, in oder aus Wohnungen personenbezogene Daten durch den verdeckten Einsatz technischer Mittel

1. zur Anfertigung von Bildaufzeichnungen sowie
2. zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes

über die nach den §§ 4 und 5 Verantwortlichen erheben. Die Maßnahme darf sich nur gegen die in Satz 1 oder 6 genannten Personen richten und nur in deren Wohnung durchgeführt werden. In Wohnungen anderer Personen ist die Maßnahme nur zulässig, wenn Tatsachen die Annahme rechtfertigen, dass sich eine in Satz 1 oder 6 genannte Person in der Wohnung aufhält

und die Abwehr der Gefahr auf andere Weise nicht möglich erscheint oder wesentlich erschwert wäre. Die Datenerhebung ist nur zulässig unter den in § 39 a Abs. 2 bezeichneten Voraussetzungen. Die Datenerhebung darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Eine Maßnahme nach Satz 1 ist auch zulässig, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine in § 28 Abs. 1 Satz 1 Nr. 3 bezeichnete Straftat begeht."

b) Absatz 5 wird wie folgt geändert:

aa) Satz 3 erhält folgende Fassung:

„Solche Daten dürfen für einen anderen Zweck verwendet werden, soweit
1. sich aus ihnen konkrete Ermittlungsansätze zur Verfolgung von besonders schweren Straftaten ergeben, die nach der Strafprozessordnung eine Wohnraumüberwachung rechtfertigen,
2. dies zur Abwehr einer dringenden Gefahr im Sinne des Absatzes 1 erforderlich ist."

bb) Nach Satz 3 wird folgender neue Satz 4 eingefügt:

„Personenbezogene Daten, die durch den verdeckten Einsatz technischer Mittel nach Absatz 1 Satz 1 Nr. 1 erlangt wurden, dürfen nicht für Zwecke der Strafverfolgung verwendet werden."

c) In Absatz 7 Satz 3 Halbsatz 1 werden die Worte „Beamten des höheren Dienstes" durch die Worte „Beamten mit der Befähigung für das vierte Einstiegsamt" ersetzt.

d) In Absatz 8 Satz 1 wird die Verweisung „Absätzen 1 und 7" durch die Verweisung „Absätzen 1 und 6" ersetzt.

7. § 31 wird wie folgt geändert:

a) In Absatz 1 wird folgender neue Satz 2 eingefügt:

„Eine Maßnahme nach Satz 1 ist auch zulässig, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine in § 28 Abs. 1 Satz 1 Nr. 3 bezeichnete Straftat begeht."

b) In Absatz 3 wird folgender neue Satz 2 eingefügt:

„Eine Maßnahme nach Satz 1 ist auch zulässig, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine in § 28 Abs. 1 Satz 1 Nr. 3 bezeichnete Straftat begeht."

c) In Absatz 5 Satz 3 werden die Worte „Beamten des höheren Dienstes" durch die Worte „Beamten mit der Befähigung für das vierte Einstiegsamt" ersetzt.

d) Nach Absatz 6 wird folgender neue Absatz 7 eingefügt:

„(7) Nach Absatz 1 oder 3 erlangte Daten sind besonders zu kennzeichnen. Nach einer Übermittlung ist die Kennzeichnung durch die Empfänger aufrechtzuerhalten. Solche Daten dürfen für einen anderen Zweck verwendet werden, soweit

1. sich aus ihnen konkrete Ermittlungsansätze zur Verfolgung von schweren Straftaten ergeben, die nach der Strafprozessordnung eine Telekommunikationsüberwachung rechtfertigen,
2. dies zur Abwehr einer dringenden Gefahr im Sinne des Absatzes 1 erforderlich ist.“

e) Der bisherige Absatz 7 wird Absatz 8 und wie folgt geändert:

Satz 1 wird gestrichen.

8. In § 31 a Abs. 3 Satz 4 Halbsatz 1 werden die Worte „Beamten des höheren Dienstes“ durch die Worte „Beamten mit der Befähigung für das vierte Einstiegsamt“ ersetzt.

9. § 31 b wird wie folgt geändert:

a) In Absatz 1 wird folgender neue Satz 2 eingefügt:

„Eine Maßnahme nach Satz 1 ist auch zulässig, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine in § 28 Abs. 1 Satz 1 Nr. 3 bezeichnete Straftat begeht.“

b) In Absatz 4 wird die Verweisung „§ 29 Abs. 5“ durch die Verweisung „§ 31 Abs. 7“ ersetzt.

10. § 31 c Abs. 1 erhält folgende Fassung:

„(1) Die Polizei kann ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme darf sich nur gegen die nach den §§ 4 und 5 Verantwortlichen richten und nur in die von diesen Personen genutzte informationstechnische Systeme eingreifen; sie ist nur zulässig, soweit die Abwehr der Gefahr auf andere Weise nicht möglich erscheint oder wesentlich erschwert wäre. Die Maßnahme ist auch gegen Personen zulässig, deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine in § 28 Abs. 1 Satz 1 Nr. 3 bezeichnete Straftat begeht. In informationstechnische Systeme anderer Personen darf die Maßnahme nur eingreifen, wenn Tatsachen die Annahme rechtfertigen, dass eine in Satz 2 oder 3 genannte Person dort ermittlungsrelevante Informationen speichert und die Abwehr der Gefahr auf andere Weise nicht möglich erscheint oder wesentlich erschwert wäre. Die Datenerhebung ist nur zulässig unter den in § 39 a Abs. 3 genannten Voraussetzungen. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.“

11. In § 31 d Abs. 3 Satz 5 Halbsatz 1 werden die Worte „Beamten des höheren Dienstes“ durch die Worte „Beamten mit der Befähigung für das vierte Einstiegsamt“ ersetzt.

12. § 31 e wird wie folgt geändert:

    a) Absatz 1 erhält folgende Fassung:

    „(1) Die Polizei kann zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, Auskunft über Verkehrsdaten ohne Kenntnis der Rufnummer oder einer anderen Kennung des zu überwachenden Anschlusses oder des Endgeräts verlangen über
    1. die nach den §§ 4 und 5 Verantwortlichen und unter den Voraussetzungen des § 7 über die dort genannten Personen oder
    2. Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie für die nach den §§ 4 und 5 Verantwortlichen bestimmte oder von ihnen herrührende Mitteilungen entgegennehmen oder weitergeben.

    Eine Maßnahme nach Satz 1 ist auch zulässig, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine in § 28 Abs. 1 Satz 1 Nr. 3 bezeichnete Straftat begeht. Die Datenerhebung ist nur zulässig, sofern anderenfalls die Erreichung des Zwecks der Maßnahme erheblich erschwert wäre. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.“

    b) In Absatz 2 Satz 2 Halbsatz 2 wird die Verweisung „§ 29 Abs. 5“ durch die Verweisung „§ 31 Abs. 7“ ersetzt.

13. Nach § 31 e wird folgender neue § 31 f eingefügt:

„§ 31 f
Auskunft über Bestandsdaten

(1) Die Polizei kann zur Abwehr einer Gefahr Auskünfte über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten (§ 113 Abs. 1 Satz 1 des Telekommunikationsgesetzes) oder die nach § 14 Abs. 1 des Telemediengesetzes erhobenen Daten (§ 14 Abs. 2 des Telemediengesetzes) verlangen, über
1. die nach den §§ 4 und 5 Verantwortlichen und unter den Voraussetzungen des § 7 über die dort genannten Personen oder
2. Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie für die nach den §§ 4 und 5 Verantwortlichen bestimmte oder von ihnen herrührende Mitteilungen entgegennehmen oder weitergeben.

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 (§ 113 Abs. 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die konkret beabsichtigte Nutzung der Daten im Zeitpunkt des Ersuchens vorliegen.

(2) Die Auskunft nach Absatz 1 kann auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internet-Protokolladresse verlangt werden (§ 113 Abs. 1 Satz 3 des Telekommunikationsgesetzes), soweit dies zur Abwehr einer Gefahr für Leib oder Leben einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, erforderlich ist.

(3) Auskunftsverlangen nach Absatz 1 Satz 2 bedürfen der richterlichen Entscheidung. § 31 Abs. 5 gilt entsprechend. Die Sätze 1 und 2 finden 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 dieser Voraussetzungen ist aktenkundig zu machen.

(4) Aufgrund eines Auskunftsverlangens nach Absatz 1 oder 2 hat jeder, der geschäftsmäßig Telekommunikationsdienste oder Telemediendienste erbringt oder daran mitwirkt, unverzüglich die zur Auskunftserteilung erforderlichen Daten zu übermitteln. § 12 Abs. 5 gilt entsprechend.

(5) Bestandsdaten im Sinne des Absatzes 1 und 2 sind die nach den §§ 95 und 111 des Telekommunikationsgesetzes und die nach § 14 des Telemediengesetzes erhobenen Daten.“

14. § 32 wird wie folgt geändert:

    a) In Absatz 3 Satz 1 werden die Worte „Beamten des höheren Dienstes“ durch die Worte „Beamten mit der Befähigung für das vierte Einstiegsamt“ ersetzt.

    b) In Absatz 4 wird die Verweisung „§ 28 Abs. 5“ durch die Verweisung „§ 28 Abs. 6“ ersetzt.

15. § 37 Abs. 3 wird wie folgt geändert:

    a) In Satz 1 wird die Verweisung „und Abs. 3 und 4“ durch die Verweisung „und Abs. 4 und 5“ und die Verweisung „§ 28 Abs. 2 Nr. 2“ durch die Verweisung „§ 28 Abs. 2 Nr. 2 und 3“ ersetzt.

    b) In Satz 2 werden die Worte „Beamten des höheren Dienstes“ durch die Worte „Beamten mit der Befähigung für das vierte Einstiegsamt“ ersetzt.

16. § 38 wird wie folgt geändert:

    a) Absatz 3 wird wie folgt geändert:

        aa) Satz 2 und 3 erhält folgende Fassung:

            „Zuständiges Gericht ist das Oberverwaltungsgericht Rheinland-Pfalz. Das Oberverwaltungsgericht entscheidet nach Maßgabe der Verwaltungsgerichtsordnung.“

        bb) In Satz 5 Halbsatz 1 werden die Worte „Beamten des höheren Dienstes“ durch die Worte „Beamten mit der Befähigung für das vierte Einstiegsamt“ ersetzt.

b) Nach Absatz 3 wird folgender neue Absatz 4 eingefügt:

„(4) Nach Absatz 1 erlangte Daten sind besonders zu kennzeichnen. Nach einer Übermittlung ist die Kennzeichnung durch die Empfänger aufrechtzuerhalten. Solche Daten dürfen für einen anderen Zweck verwendet werden, soweit

1. sich aus ihnen konkrete Ermittlungsansätze zur Verfolgung von Straftaten von erheblicher Bedeutung ergeben, die nach der Strafprozessordnung eine Rasterfahndung rechtfertigen,
2. dies zur Abwehr einer dringenden Gefahr im Sinne des Absatzes 1 erforderlich ist.“

c) Der bisherige Absatz 4 wird Absatz 5 und erhält folgende Fassung:

„(5) Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und die im Zusammenhang mit dem Abgleich zusätzlich angefallenen Daten zu löschen und die Unterlagen zu vernichten, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind. Die getroffene Maßnahme ist zu dokumentieren. Diese Dokumentation ist gesondert aufzubewahren und durch organisatorische und technische Maßnahmen zu sichern. Sie ist sechs Monate nach der Benachrichtigung nach § 40 Abs. 5 zu löschen. Ist die Datenschutzkontrolle nach § 41 b noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.“

17. § 39 a erhält folgende Fassung:

„§ 39 a
Schutz des Kernbereichs privater Lebensgestaltung

(1) Verdeckte Maßnahmen der Datenerhebung, die in den Kernbereich privater Lebensgestaltung eingreifen, sind unzulässig. Dennoch erlangte Daten sind unverzüglich zu löschen. Erkenntnisse hierüber dürfen nicht verwertet werden. Die Tatsache der Datenerhebung und der Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist sechs Monate nach der Benachrichtigung nach § 40 Abs. 5 zu löschen. Ist die Datenschutzkontrolle nach § 41 b noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.

(2) Die Datenerhebung nach § 29 darf nur angeordnet werden, soweit nicht aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Daten erhoben werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Abzustellen ist dabei insbesondere auf die Art der zu überwachenden Räumlichkeiten und das Verhältnis der dort anwesenden Personen zueinander.

(3) Die Datenerhebung nach den §§ 28, 31, 31 b oder 31 c darf nur angeordnet werden, falls nicht tatsächliche Anhaltspunkte für die Annahme vorliegen, dass allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden. Bei einer Datenerhebung nach § 31 c ist, soweit technisch möglich, sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.

(4) Eine Datenerhebung nach § 29 ist unverzüglich zu unterbrechen, sofern sich während der Überwachung tatsächliche Anhaltspunkte ergeben, dass Inhalte erfasst werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Bestehen insoweit Zweifel, darf eine automatische Aufzeichnung fortgesetzt werden. Automatische Aufzeichnungen und alle Erkenntnisse, die durch eine Datenerhebung nach § 29 erlangt worden sind, sind unverzüglich dem Oberverwaltungsgericht Rheinland-Pfalz zur Entscheidung über die Verwertbarkeit oder Löschung vorzulegen. Bei Gefahr im Verzug kann die Behördenleitung oder ein von ihr besonders beauftragter Beamter mit der Befähigung für das vierte Einstiegsamt im Benehmen mit dem behördlichen Datenschutzbeauftragten über die Verwertung der Erkenntnisse entscheiden. Bei der Sichtung der erhobenen Daten kann sie oder er sich der technischen Unterstützung von zwei weiteren Bediensteten der zuständigen Polizeibehörde bedienen, von denen einer die Befähigung zum Richteramt haben muss. Die Bediensteten sind zur Verschwiegenheit über die ihnen bekannt werdenden Erkenntnisse, die nicht verwertet werden dürfen, verpflichtet. Die gerichtliche Entscheidung nach Satz 3 ist unverzüglich nachzuholen. Ist die Datenerhebung unterbrochen worden, darf sie unter den Voraussetzungen des Absatzes 2 Satz 1 fortgeführt werden.

(5) Die unmittelbare Kenntnisnahme einer Datenerhebung nach § 28 Abs. 2 Nr. 1 bis 3 und 6 und § 31 ist unverzüglich zu unterbrechen, sofern sich tatsächliche Anhaltspunkte ergeben, dass Inhalte erfasst werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Bestehen insoweit Zweifel, darf eine automatische Aufzeichnung fortgesetzt werden; diese sind unverzüglich dem Oberverwaltungsgericht Rheinland-Pfalz zur Entscheidung über die Verwertbarkeit oder Löschung vorzulegen. Absatz 4 Satz 4 bis 7 gilt entsprechend. Ergeben sich bei Maßnahmen nach § 28 Abs. 2 Nr. 4 und 5 während der Durchführung tatsächliche Anhaltspunkte dafür, dass Inhalte erfasst werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, ist die Maßnahme zu unterbrechen, sobald dies ohne Gefährdung des verdeckten Ermittlers oder der Vertrauensperson möglich ist. Ist die Datenerhebung unterbrochen worden, darf sie unter den Voraussetzungen des Absatzes 3 Satz 1 fortgeführt werden.

(6) Alle Erkenntnisse, die durch eine Datenerhebung nach § 31 c erlangt worden sind, sind unverzüglich dem Oberverwaltungsgericht Rheinland-Pfalz zur Entscheidung über die Verwertbarkeit oder Löschung vorzulegen. Absatz 4 Satz 4 bis 7 gilt entsprechend.“

18. Nach § 41 a wird folgender neue § 41 b eingefügt:

„§ 41 b
Aufgaben und Befugnisse des Landesbeauftragten
für den Datenschutz und die Informationsfreiheit

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit führt mindestens alle zwei Jahre Kontrollen bezüglich der Datenerhebungen nach den §§ 27 b, 28, 29, 31, 31 b, 31 c, 31 e und 38 durch.“

19. Nach § 99 wird folgender neue § 99 a eingefügt:

„§ 99 a
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig einer vollziehbaren Meldeauflage gemäß § 12 a, einem vollziehbaren Platzverweis gemäß § 13 Abs. 1, einer vollziehbaren Wohnungsverweisung gemäß § 13 Abs. 2, einem vollziehbaren Aufenthaltsverbot gemäß § 13 Abs. 3, einem vollziehbaren Rückkehrverbot gemäß § 13 Abs. 4 Nr. 1 oder einem vollziehbaren Annäherungsverbot gemäß § 13 Abs. 4 Nr. 3 zuwiderhandelt. § 37 des Brand- und Katstrophenschutzgesetzes vom 2. November 1981 (GVBl. S. 247) in der jeweils geltenden Fassung bleibt unberührt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünftausend Euro geahndet werden.

(3) Verwaltungsbehörde nach § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten ist die Behörde, die die Anordnung nach § 12 a oder § 13 getroffen hat.“

20. Die Inhaltsübersicht wird entsprechend den vorstehenden Bestimmungen geändert.

Artikel 2

Durch dieses Gesetz werden die Grundrechte aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 (Recht auf informationelle Selbstbestimmung), Artikel 10 Abs. 1 (Brief- ,Post- und Fernmeldegeheimnis), Artikel 11 Abs. 1 (Freizügigkeit) und Artikel 13 Abs. 1 (Unverletzlichkeit der Wohnung) des Grundgesetzes eingeschränkt.

Artikel 3

Dieses Gesetz tritt am Tage nach der Verkündung in Kraft.

Begründung

A. Allgemeines

Die letzte umfangreichere Änderung des Polizei- und Ordnungsbehördengesetzes (POG) in der Fassung vom 10. November 1993 (GVBl. S. 595), zuletzt geändert durch Artikel 4 des Gesetzes vom 19. Dezember 2014 (GVBl. S. 332), BS 2012-1, erfolgte im Jahr 2011. Mit der nun anstehenden Novellierung sollen einerseits die Befugnisse der Polizei gestärkt werden, damit sie nicht zuletzt den Gefahren des internationalen Terrorismus sowie den besonders sozialschädlichen Kriminalitätsphänomenen des Rechtsextremismus und des Wohnungseinbruchdiebstahls besser begegnen kann. Andererseits ergibt sich aus der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) die Notwendigkeit zur Anpassung verschiedener Vorschriften. So müssen insbesondere die Rechtsgrundlagen für verdeckte Überwachungsmaßnahmen, der Kern Kernbereichsschutz sowie die Regelungen zur Zweckänderung den verfassungsrechtlichen Anforderungen angepasst werden.

Eine effektive Gefahrenabwehr im Bereich der Terrorismusbekämpfung setzt voraus, dass die Polizei die Möglichkeit hat, Gefährder frühzeitig zu überwachen. Dadurch wird sie in die Lage versetzt, drohende Anschlagszenarien rechtzeitig zu erkennen und ihre Realisierung zu verhindern. Unter Beachtung der verfassungsrechtlichen Vorgaben wird die Einschreitschwelle für verdeckte Überwachungsmaßnahmen daher bereits im Vorfeld konkreter Gefahren zugelassen, soweit terroristische Straftaten verhütet werden sollen.

Seit dem 1. Juli 2015 wird in Rheinland-Pfalz – gestützt auf § 27 POG – ein Pilotprojekt zum Einsatz von Körperkameras (sog. Bodycams) durchgeführt. Der offene und damit für das polizeiliche Gegenüber erkennbare Einsatz der Bodycams ist eine Reaktion auf die zunehmende Gewalt gegen Polizeibeamtinnen und Polizeibeamte und soll eine deeskalierende Wirkung auf gewaltbereite Personen erzeugen. Wie sich im Zuge der Evaluation des Pilotprojekts gezeigt hat, hat sich die gewünschte deeskalierende und abschreckende Wirkung in einer Reihe von polizeilichen Einsatzsituationen bestätigt. Mit diesem Gesetzentwurf wird nunmehr eine bereichsspezifische, präzise und normenklare Regelung speziell für den Einsatz mobiler Video- und Audioüberwachungstechnik geschaffen.

Neben redaktionellen Änderungen sieht der Gesetzentwurf folgende wesentliche Änderungen des Polizei- und Ordnungsbehördengesetzes vor:

1. Die Wohnungsverweisung wird bereits zur Abwehr konkreter (statt wie bislang gegenwärtiger) Gefahren für Leib, Leben, Freiheit oder für bedeutende Sach- oder Vermögenswerte einer Person zugelassen (§ 13 Abs. 2 POG).
2. Es wird eine Regelung zur Überwachung von Großveranstaltungen mittels Videotechnik aufgenommen (§ 27 Abs. 3 POG).
3. Für den Einsatz der Bodycams wird eine bereichsspezifische Ermächtigung geschaffen (§ 27 a POG).
4. Die Polizei wird zur anlassbezogenen automatisierten Kennzeichenfahndung ermächtigt (§ 27 b POG).
5. Die §§ 28 (Besondere Mittel der verdeckten Datenerhebung), 29 (Wohnraumüberwachung), 31 (Telekommunikationsüberwachung), 31 b (Auskunft über Nutzungsdaten, 31 c (Online-Durchsuchung) und 31 e POG (Funkzellenabfrage) werden an die Anforderungen aus dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 (1 BvR 966/09, 1 BvR 1140/09) zum Bundeskriminalamtgesetz angepasst. Gleichzeitig wird der Einsatz der besonderen Mittel der verdeckten Datenerhebung – entsprechend den Vorgaben des Bundesverfassungsgerichts in dem genannten Urteil – auch gegenüber Personen zugelassen, deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird.
6. Es wird eine Ermächtigung für die Auskunft über Bestandsdaten geschaffen (§ 31 f POG).
7. Die Anordnungskompetenz für die Rasterfahndung wird vom Amtsgericht auf das Oberverwaltungsgericht Rheinland-Pfalz übertragen. Gleichzeitig werden die Vorgaben aus dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 zum Bundeskriminalamtgesetz umgesetzt (§ 38 POG).
8. Die Regelung zum Schutz des Kernbereichs privater Lebensgestaltung wird entsprechend den Vorgaben aus dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 überarbeitet (§ 39 a POG).
9. In der neu geschaffenen Regelung des § 41 b POG werden regelmäßige Kontrollen in Bezug auf eingriffsintensive Überwachungsmaßnahmen durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit vorgesehen.
10. In § 99 a POG wird ein Ordnungswidrigkeitentatbestand für Verstöße gegen Meldeauflagen, Platzverweise, Aufenthalts- und Näherungsverbote geschaffen.

Das Konnexitätsprinzip ist durch diesen Gesetzentwurf nicht berührt.

Der Gesetzentwurf hat keine Auswirkungen auf die spezifische Lebenssituation von Frauen und Männern. Ebensowenig berührt das Gesetzesvorhaben die Bevölkerungs- und Altersentwicklung.

Der Gesetzentwurf hat keine Auswirkungen auf Verwaltungsaufwand, Arbeitsplätze und Wettbewerbsfähigkeit der mittelständischen Wirtschaft.

B. Zu den einzelnen Bestimmungen

Zu Artikel 1

Zu Nummer 1 (§ 13)

Voraussetzung für die Anordnung einer Wohnungsverweisung ist gemäß § 13 Abs. 2 POG in der bisherigen Fassung das Vorliegen einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person oder für bedeutende Sach- oder Vermögenswerte einer Person. Gegenwärtig ist die Gefahr, wenn die Einwirkung des schädigenden Ereignisses entweder bereits be-

gonnen hat oder aber unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorsteht (BVerfG, Urteil vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 142). Gerade in den hier vorliegenden Fällen von häuslicher Gewalt kann das Erfordernis einer gegenwärtigen Gefahr Schwierigkeiten bereiten, denn wenn die Polizei vor Ort ist und sich die Situation vorübergehend beruhigt hat, wird man häufig nicht davon ausgehen können, dass weitere Gewalttätigkeiten in allernächster Zeit mit an Sicherheit grenzender Wahrscheinlichkeit zu erwarten sind. Gleichwohl besteht häufig die hinreichende Wahrscheinlichkeit, dass es in absehbarer Zeit zu weiteren Gewalttätigkeiten kommt. Diese Sachlage entspricht dem Vorliegen einer einfachen (konkreten) Gefahr, die von Verfassungs wegen für die Anordnung einer Wohnungsverweisung ausreicht. Zum besseren Schutz der von häuslicher Gewalt betroffenen Personen wird daher das Erfordernis der Gegenwärtigkeit einer Gefahr gestrichen, sodass eine Wohnungsverweisung künftig bereits zur Abwehr einer konkreten Gefahr in Betracht kommt.

Zu Nummer 2 (§ 18)

Durch das Landesbeamtengesetz vom 20. Oktober 2010 (GVBl. S. 319), zuletzt geändert durch Artikel 4 des Gesetzes vom 18. Juni 2013 (GVBl. S. 157), BS 2030-1, wurde das Laufbahnrecht neu gestaltet. An die Stelle der bisherigen Laufbahngruppen des einfachen, mittleren, gehobenen und höheren Dienstes ist eine einheitliche Laufbahn mit in Abhängigkeit von Vor- und Ausbildung zugänglichen Einstiegsämtern getreten. Die Änderung zeichnet die neu gestaltete Laufbahnsystematik nach.

Zu Nummer 3 (§ 27)

Zu Buchstabe a

Die neu geschaffene Regelung in Absatz 3 ermächtigt die Polizei zur offenen Anfertigung von Bild- und Tonaufzeichnungen bei öffentlichen Veranstaltungen und Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, wenn voraussichtlich mindestens 500 Personen zeitgleich hieran teilnehmen. Die neue Befugnisnorm dient insbesondere der Abwehr von terroristischen Straftaten. Wie nicht zuletzt der Anschlag auf dem Berliner Weihnachtsmarkt am 19. Dezember 2016 gezeigt hat, sind größere Menschenansammlungen bevorzugte Anschlagsziele terroristischer Attentäter. Zwar wäre der Terroranschlag in Berlin durch Videoüberwachungsmaßnahmen nicht verhindert worden. Auch lassen sich zum Suizid entschlossene Attentäter nicht von Videoüberwachungskameras von der Tatbegehung abhalten. Gleichwohl können begangene Straftaten mittels Videoaufzeichnungen leichter aufgeklärt und flüchtige Straftäter schneller identifiziert werden. Zeitnahe Fahndungserfolge nach terroristischen Anschlägen mittels Videoaufzeichnungen können deshalb nicht nur die Aufklärung begangener Straftaten erleichtern, sondern weitere schwere Straftaten verhüten. Darüber hinaus ist zu berücksichtigen, dass Videoüberwachung durch Bildübertragung zur Gefahrenabwehr grundsätzlich geeignet ist, weil sie der am Monitor sitzenden Person ein frühzeitiges Erkennen einer sich anbahnenden Gefahrensituation ermöglicht, sodass bei einer schnellen Reaktion drohende Schäden verhindert oder zumindest in ihren Auswirkungen verringert werden können.

Aus diesem Grund wird die Polizei zur vorbeugenden Bekämpfung von Straftaten ermächtigt, bei öffentlichen Veranstaltungen ab einer bestimmten Größe Bild- und Tonaufzeichnungen anzufertigen. Bei einer Abwägung der widerstreitenden Interessen – nämlich des Rechts auf informationelle Selbstbestimmung einerseits und dem Schutz der Bevölkerung vor schwerwiegenden Straftaten andererseits – überwiegt hier das Interesse am Schutz der Bevölkerung vor Gefahren für Leib oder Leben.

Die verfassungsrechtlichen Anforderungen an die Ermächtigungsgrundlage richten sich nach dem Gewicht des Eingriffs, das insbesondere von der Art der erfassten Informationen, dem Anlass und den Umständen ihrer Erhebung, dem betroffenen Personenkreis und der Art der möglichen Verwertung der Daten beeinflusst wird (BVerfG, Urteil vom 11. März 2008 – 1 BvR 2074/05, 1 BvR 1254/07 – juris, Rn. 76). Insoweit ist zunächst zu berücksichtigen, dass hier Daten über Personen erhoben werden, die den Eingriff durch ihr Verhalten nicht veranlasst haben. Vielmehr kann jede Person betroffen sein, die an einer größeren Veranstaltung teilnimmt. Datenerhebungen dieser Art sind grundsätzlich von größerer Eingriffsintensität als anlassbezogene. Andererseits darf die Videoüberwachung nur offen und nicht verdeckt erfolgen. Heimliche Grundrechtseingriffe führen zu einer Erhöhung des Gewichts der Freiheitsbeeinträchtigung, was hier nicht der Fall ist. Das Gewicht des Eingriffs wird auch dadurch reduziert, dass nur öffentliche Veranstaltungen überwacht werden dürfen, sodass nur das Verhalten von Personen erfasst wird, das ohnehin für jedermann erkennbar ist. Die Intensität des Eingriffs für den Betroffenen wird schließlich davon beeinflusst, welche über die Informationserhebung hinausgehenden Nachteile ihm aufgrund der Maßnahme drohen. Die erhobenen Daten sind gemäß Absatz 6 Satz 3 unverzüglich zu löschen, soweit sich aus ihnen im Einzelfall nicht konkrete Ermittlungsansätze zur Verfolgung oder Verhütung von Straftaten oder zur Abwehr von in einem überschaubaren Zeitraum drohenden Gefahren für Leib, Leben oder Eigentum einer Person ergeben und die Verwendung der Daten zu diesem Zweck erforderlich ist. In diesem Fall können durch die Informationserhebung jedoch weitere Schlüsse über das Verhalten des Betroffenen gezogen und die gewonnenen Informationen gesammelt und mit weiteren Informationen verknüpft werden, sodass der Grundrechtseingriff in der Gesamtschau nicht nur ganz unerheblich ist.

Eingriffe in das Recht auf informationelle Selbstbestimmung müssen dem Gebot der Verhältnismäßigkeit genügen. Insoweit hat das Bundesverfassungsgericht in seinem Urteil zur automatisierten Kennzeichenerfassung gefordert, dass „der Gesetzgeber die Ausgewogenheit zwischen der Art und Intensität der Grundrechtsbeeinträchtigung einerseits und den zum Eingriff berechtigenden Tatbestandselementen andererseits, wie der Einschreitschwelle, der geforderten Tatsachenbasis und dem Gewicht der geschützten Rechtsgüter, zu wahren hat. Je gewichtiger die drohende oder erfolgte Rechtsgutsbeeinträchtigung und je weniger gewichtig der Grundrechtseingriff ist, um den es sich handelt, desto geringer darf die Wahrscheinlichkeit sein, mit der auf eine drohende oder erfolgte Verletzung des Rechtsguts geschlossen werden kann, und desto weniger fundiert dürfen gegebenenfalls die Tatsachen sein, die dem Verdacht zugrunde liegen. Selbst bei höchstem Gewicht der drohenden Rechtsgutbeeinträchtigung kann allerdings auf das Erfordernis einer hinreichenden Wahrscheinlichkeit nicht verzichtet werden. Grundrechtsein-

greifende Ermittlungen „ins Blaue hinein“ lässt die Verfassung nicht zu“ (BVerfG, a. a. O, juris, Rn. 169).

Nach der neuen Befugnisnorm sind Videoüberwachungsmaßnahmen zur vorbeugenden Bekämpfung von Straftaten zulässig, wenn an einer öffentlichen Veranstaltung oder Ansammlung voraussichtlich mehr als 500 Personen zeitgleich teilnehmen. Wie verschiedene Terroranschläge in der jüngeren Vergangenheit gezeigt haben, sind größere Menschenansammlungen grundsätzlich in besonderem Maße gefährdet, Ziel eines terroristischen Anschlags zu werden. Vor diesem Hintergrund und der hiermit einhergehenden latenten Gefährdung von Leib und Leben einer Vielzahl von Menschen ist es dem Gesetzgeber von Verfassungs wegen nicht verwehrt, Videoüberwachungsmaßnahmen bei Großveranstaltungen unter im Vergleich zur bisherigen Rechtslage erleichterten Voraussetzungen zuzulassen.

Zu Buchstabe b

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Buchstabe c

Zu Doppelbuchstabe aa

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Doppelbuchstabe bb

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Doppelbuchstabe cc

Nach Absatz 3 erlangte Daten sind ebenfalls, wie dies für Bild- und Tonaufzeichnungen nach den Absätzen 1, 2, 4 und 5 gilt, unverzüglich zu löschen, wenn sie nicht für eine zulässige Zweckänderung Verwendung finden sollen. Zulässig ist eine zweckändernde Nutzung der nach Absatz 3 erlangten Daten allerdings nur, wenn sich aus ihnen im Einzelfall konkrete Ermittlungsansätze zur Verfolgung oder Verhütung von Straftaten oder zur Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für Leib, Leben oder Eigentum einer Person ergeben und die Verwendung der Daten zu diesem Zweck erforderlich ist.

Zu Doppelbuchstabe dd

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Buchstabe d

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Buchstabe e

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Nummer 4 (§§ 27 a und 27 b)

§ 27 a (Mobile Bild- und Tonaufzeichnungsgeräte)

Seit dem 1. Juli 2015 wird in Rheinland-Pfalz – gestützt auf § 27 POG – ein Pilotprojekt zum Einsatz von Körperkameras (sog. Bodycams) durchgeführt. Die Kameras kommen als präventiv-polizeiliche Maßnahme in Situationen zum Einsatz, bei denen aufgrund der Gesamtumstände mit einer Gefährdung der Polizeikräfte oder unbeteiligter Dritter zu rechnen ist. Durch den offenen Kameraeinsatz in diesen Fällen soll eine deeskalierende Wirkung auf gewaltbereite Personen erzeugt und die Gefahr gewalttätiger Übergriffe auf Polizeibeamtinnen und Polizeibeamte sowie Dritte verringert werden. Das Pilotprojekt in Rheinland-Pfalz ist wissenschaftlich begleitet worden. Im Ergebnis der Evaluation ist festgestellt worden, dass die Bodycam in einer Reihe von polizeilichen Einsatzsituationen tatsächlich die gewünschte deeskalierende Wirkung erzielen konnte. Die Bodycam hat darüber hinaus eine hohe Akzeptanz bei den Polizeibeamtinnen und Polizeibeamten gefunden und ist auch von der Bevölkerung positiv bewertet worden. Obwohl mit der Regelung in § 27 POG bereits eine Rechtsgrundlage für den Einsatz der Bodycam vorhanden ist, soll hierfür eine bereichsspezifische Ermächtigung geschaffen werden. Grund hierfür ist der Umstand, dass der Einsatz der Bodycam im Vergleich zur stationären Videoüberwachung eine qualifizierte Eingriffstiefe besitzt, da hier einzelne Personen gezielt gefilmt werden. Ferner sind verfahrensrechtliche Regelungen erforderlich, aus denen sich ergibt, wie mit den erhobenen Daten im Anschluss an eine dauerhafte Aufzeichnung zu verfahren ist und wie der Betroffene die ihm zustehenden Rechte geltend machen kann.

Nach Absatz 1 dürfen Bild- und Tonaufnahmen erstellt werden, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz von Polizeibeamtinnen und Polizeibeamten oder Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist. Die Bild- und Tonaufzeichnungen sind ausschließlich in öffentlich zugänglichen Räumen zulässig. Öffentlich zugänglich sind Räume, die entweder dem öffentlichen Verkehr gewidmet sind – wie öffentliche Straßen, Parkanlagen, Wege und Plätze – oder nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden dürfen – wie zum Beispiel Einkaufszentren, Gaststätten, Diskotheken, Geschäfte oder öffentliche Verkehrsmittel. Betriebs- und Geschäftsräume, die der Ausübung von Tätigkeiten von Berufsgeheimnisträgern nach § 53 Abs. 1 StPO dienen, sind nach Absatz 2 Satz 2 ausdrücklich ausgenommen.

Die Aufzeichnung umfasst Bild- und Tonaufzeichnungen. Tonaufzeichnungen sind erforderlich, weil gewalttätigen Übergriffen in der Regel beleidigendes verbales Verhalten vorausgeht. Das deutliche Signal, dass auch entsprechende Äußerungen aufgenommen werden, kann frühzeitig eine gewalttätige Eskalation verhindern. Darüber hinaus erleichtert die Nutzung von Tonaufnahmen die Rekonstruktion eines Geschehensablaufs.

Die Anfertigung von Bild- und Tonaufzeichnungen ist nur zulässig, wenn durch Tatsachen begründete Anhaltspunkte die Annahme rechtfertigen, dass dies zum Schutz eines Polizeibeamten oder eines Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist. Mit dieser Formulierung wird deutlich gemacht, dass Bild- und Tonaufzeichnungen erst dann angefertigt werden dürfen, wenn im konkreten Einsatzgeschehen tatsächliche Anhaltspunkte darauf hindeuten, dass eine Situation einen gewalttätigen Verlauf nehmen kann. Nicht vorausgesetzt wird das Vorliegen einer konkreten Gefahr; auch braucht der gewalttätige Übergriff weder begonnen zu haben noch muss er unmittelbar bevorstehen. Die Aufnahmen sind vielmehr bereits im Vorfeld einer konkreten Gefahr zulässig, wenn es sich um ein Einsatzgeschehen handelt, bei dem die jeweiligen Umstände im Einzelfall den Schluss auf eine mögliche Eskalation zulassen.

Der Einsatz der Bodycam ist nicht nur zum Schutz von Polizeibeamtinnen und Polizeibeamten, sondern auch zum Schutz von Dritten zulässig. Hierbei kann es sich z. B. um Kräfte der Feuerwehr oder des Rettungsdienstes handeln.

Absatz 1 erlaubt ausschließlich den offenen Einsatz der Bild- und Tonaufzeichnungsgeräte. Für die betroffene Person muss daher erkennbar sein, dass aufgezeichnet wird. Verdeckte Aufzeichnungen sind ausgeschlossen.

Absatz 2 Satz 1 stellt klar, dass die Aufzeichnungen auch dann zulässig sind, wenn Dritte unvermeidbar betroffen sind. Aufzeichnungen in einem durch ein Berufsgeheimnis geschützten Vertrauensverhältnis im Sinne des § 53 Abs. 1 StPO und des § 53 a StPO sind nach Absatz 2 Satz 2 ausdrücklich untersagt. Damit dürfen z. B. in Arztpraxen oder Kanzleiräumen keine Aufnahmen angefertigt werden, da anderenfalls in ein geschütztes Vertrauensverhältnis eingegriffen würde. Da Absatz 1 nur den offenen Einsatz der Bodycam erlaubt, legt Absatz 2 Satz 3 fest, dass auf eine Datenerhebung nach Absatz 1 in geeigneter Form hinzuweisen ist. Vor Beginn der Aufzeichnung hat daher regelmäßig ein mündlicher Hinweis der Polizeibeamtin oder des Polizeibeamten zu erfolgen. Darüber hinaus tragen die Polizeikräfte Funktionswesten mit einem auf die Videoaufzeichnung hinweisenden Schriftzug.

Die Verwendung einer Prerecording-Funktion, um schon vor dem Einschaltzeitpunkt der Kamera Daten zu erheben, ist nach Absatz 3 ausgeschlossen.

Absatz 4 enthält verfahrensrechtliche Vorkehrungen zur Aufbewahrung bzw. Löschung der erhobenen Daten. Nach Absatz 4 Satz 1 sind Bild- und Tonaufzeichnungen nach 30 Tagen grundsätzlich zu löschen. Die Aufbewahrungsfrist von 30 Tagen dient dazu, eine Überprüfung der Rechtmäßigkeit von aufgezeichneten polizeilichen Maßnahmen, insbesondere auf Verlangen des Betroffenen, zu ermöglichen. Bei einer 30-tägigen Aufbewahrungsfrist bleibt den Beteiligten ausreichend Zeit, um die Situation nachträglich zu bewerten und zu entscheiden, ob die Rechtmäßigkeit der polizeilichen Maßnahme einer Überprüfung zugeführt werden soll. Eine über 30 Tage hinausgehende Speicherung der Daten ist nur zulässig, soweit die Aufzeichnungen zur Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung, im Einzelfall zur Gefahrenabwehr oder im Einzelfall, insbesondere auf Verlangen des Betroffenen, für die Überprüfung der Rechtmäßigkeit von aufgezeichneten polizeilichen Maßnahmen erforderlich sind. Die damit verbundene Zweckänderung der Daten muss nach Absatz 4 Satz 2 im Einzelfall festgestellt und dokumentiert werden.

§ 27 b (Anlassbezogene Kennzeichenerfassung)

Der neu eingefügte § 27 b POG regelt die Befugnis zur automatisierten Kennzeichenerfassung. Bislang ist die Polizei gehalten, Kraftfahrzeugkennzeichen manuell abzulesen, zu notieren und zu überprüfen. Diese Vorgehensweise bindet jedoch Personal und ist wenig effektiv. Durch den Einsatz technischer Mittel zur anlassbezogenen automatischen Kennzeichenerfassung wird es künftig möglich sein, polizeiliche Kontrollen effizienter zu gestalten. Die automatisierte Kennzeichenfahndung dient der schnellen Erfassung und Identifizierung von Kraftfahrzeugkennzeichen, indem diese von einer Videokamera erfasst und mit polizeilichen Fahndungsdateien abgeglichen werden. Ist das Kennzeichen in den Dateien enthalten, wird eine Treffermeldung ausgegeben, sodass die Polizei Anhaltekontrollen und gegebenenfalls weitere Maßnahmen durchführen kann. Ist das Kennzeichen nicht im Fahndungsbestand enthalten, werden alle Daten unverzüglich gelöscht.

Die Gesetzgebungskompetenz des Landes folgt aus Artikel 70 Abs. 1 GG, da die Zweckrichtung der Maßnahme nicht auf die repressive, strafverfolgende Tätigkeit der Polizei, sondern auf die Verhütung von Straftaten einschließlich der Beseitigung fortdauernder Störungen der öffentlichen Sicherheit ausgerichtet ist. Die automatisierte Kennzeichenerfassung mit dem Ziel, gestohlene Kraftfahrzeuge an den Eigentümer zurückzuführen, ist daher vom präventiven Handeln umfasst.

Die anlassbezogene Kennzeichenerfassung kann die polizeiliche Suche nach zur Fahndung ausgeschriebenen Personen oder Sachen erleichtern. So kann die automatisierte Kennzeichenerfassung insbesondere Fahndungsmaßnahmen bei Terrorlagen und Wohnungseinbruchdiebstählen, die von organisierten Banden begangen werden, wirkungsvoll unterstützen. Mobile Erfassungsgeräte können etwa an einschlägigen Anreisewegen von Einbrecherbanden aufgestellt werden und zuverlässig anzeigen, ob sich verdächtige Fahrzeuge im Fahndungsgebiet befinden.

Die Regelung des § 27 b POG beachtet die Vorgaben aus dem Urteil des Bundesverfassungsgerichts vom 11. März 2008 (1 BvR 2074/05, 1 BvR 1254/07).

Das Bundesverfassungsgericht hat die Befugnis zur automatisierten Kennzeichenerfassung für grundsätzlich zulässig erklärt, wenn die entsprechende Ermächtigungsgrundlage bestimmte Anforderungen erfüllt. So muss eine solche Ermächtigung das im Rechtsstaatsprinzip verankerte Bestimmtheitsgebot sowie das Gebot der Normenklarheit beachten. Hierfür bedarf es einer hinreichend bereichsspezifischen und normenklaren Bestimmung des Anlasses und des Verwendungszwecks der Datenerhebung (BVerfG, a. a. O, juris, Rn. 98). Mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar ist eine anlasslose und flächendeckende automatisierte Erfassung von Kraftfahrzeugkennzeichen (BVerfG, a. a. O, juris, Rn. 172). Die Regelung in § 27 b POG berücksichtigt diese Vorgaben, indem sie ausschließlich eine nur vorübergehende und nicht flächendeckende Kennzeichenerfassung unter engen Begrenzungen der Eingriffsvoraussetzungen erlaubt. Darüber hinaus trifft die Regelung in Absatz 3 Vorkehrungen für einen effektiven Grundrechtsschutz. Das Bundesverfassungsgericht hat festgestellt, dass die automatisierte Kennzeichen-erfassung keinen Eingriff in das Recht auf informationelle Selbstbestimmung gemäß Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes darstellt, wenn die Daten unmittelbar nach der Erfassung technisch wieder spurenlos, anonym und ohne die Möglichkeit, einen Personenbezug herzustellen, ausgesondert werden (BVerfG, a. a. O, juris, Rn. 68). Grundrechtsrelevant sind daher allein die Trefferfälle, für die in Absatz 3 Vorgaben zum Umfang der zu speichernden Daten und zu zulässigen Folgemaßnahmen getroffen werden.

Absatz 1 regelt die Voraussetzungen für die Datenerhebung durch die anlassbezogene automatische Kennzeichenerfassung und bestimmt hierfür mehrere Anwendungsfälle. Diesen ist gemeinsam, dass stets auf einen anlassbezogenen Einsatz der Kennzeichenlesegeräte abgestellt wird, d. h. auf Fälle, in denen eine gegenwärtige Gefahr vorliegt oder eine Straftat unmittelbar bevorsteht. Hierdurch wird ein flächendeckender und anlassloser Einsatz der Geräte ausgeschlossen.

Nach Absatz 1 Nummer 1 wird der Einsatz der Kennzeichenfahndung zur Abwehr gegenwärtiger Gefahren für Leib,

Leben, Freiheit oder Eigentum einer Person erlaubt. Damit kann die Kennzeichenfahndung z. B. auch mit dem Ziel, gestohlene Kraftfahrzeuge aufzufinden und an die Eigentümer zurückzuführen, oder zur Verhinderung von Wohnungseinbruchdiebstählen durchgeführt werden.

Durch die Verweisung in Absatz 1 Nummer 2 auf die polizeiliche Identitätsfeststellung kann die automatisierte Kennzeichenfahndung zur Abwehr einer gegenwärtigen Gefahr anlassbezogen an gefährlichen Orten nach § 10 Abs. 1 Satz 2 Nr. 1 POG eingesetzt werden. Anwendungsbereiche hierfür sind z. B. Einkaufszentren, Geschäfte oder Geldinstitute im Zusammenhang mit Überfallserien. Ähnliches gilt an besonders gefährdeten Objekten (§ 10 Abs. 1 Satz 2 Nr. 2 POG), wie etwa Flughäfen, Bahnhöfen oder militärischen Einrichtungen. Insbesondere mit Blick auf die Gefahren des internationalen Terrorismus können Kontrollen mittels automatisierter Kennzeichenfahndung einen effektiven Schutz dieser Örtlichkeiten bewirken. Schließlich wird die Kennzeichenfahndung in den Fällen des § 10 Abs. 1 Satz 2 Nr. 3 POG erlaubt, also anstelle einer polizeilichen Kontrollstelle zur Verhinderung von schweren Straftaten im Sinne des § 100 a der Strafprozessordnung (StPO) oder des § 27 des Versammlungsgesetzes in der Fassung der Bekanntmachung vom 15. November 1978 (BGBl. I S. 1789), zuletzt geändert durch Artikel 2 des Gesetzes vom 8. Dezember 2008 (BGBl. I. S. 2366). Die Befugnis ermöglicht z. B. die Kennzeichenerfassung zum Zwecke des Abgleichs mit polizeilichen Dateien bekannter Gewalttäter. Zu den schweren Straftaten im Sinne des § 100 a Abs. 2 StPO gehören auch der Bandendiebstahl nach § 244 Abs. 1 Nr. 2 und der schwere Bandendiebstahl gemäß § 244 a des Strafgesetzbuchs (StGB). Der Einsatz der automatisierten Kennzeichenerfassung kommt daher auch zur Verhinderung von Wohnungseinbruchdiebstählen in Betracht, die von Mitgliedern einer Bande begangen werden.

Absatz 1 Nummer 3 knüpft an die Ausschreibung einer Person oder eines Fahrzeugs an. Für den Einsatz der automatisierten Kennzeichenerfassung ist allerdings zusätzlich erforderlich, dass die Begehung der Straftat unmittelbar bevorsteht. Die Kennzeichenerfassung nach Absatz 1 Nummer 3 erleichtert die Arbeit der Polizei beim Auffinden von Personen oder Fahrzeugen, die z. B. gemäß § 32 POG oder vergleichbaren Vorschriften in den Polizeigesetzen anderer Länder zur polizeilichen Beobachtung ausgeschrieben wurden. Personen, von denen die unmittelbar bevorstehende Begehung nicht nur unerheblicher Straftaten zu erwarten ist, können durch diese Methode zielgerichteter aufgespürt werden.

In Absatz 2 werden die polizeilichen Fahndungsbestände bestimmt, mit denen ein Abgleich der erfassten Kennzeichen erfolgen darf. Nach Satz 1 dürfen die erfassten Kennzeichen nur mit den Sachfahndungsdateien des beim Bundeskriminalamt nach den Vorschriften des Bundeskriminalamtgesetzes und des beim Landeskriminalamt nach den Vorschriften dieses Gesetzes geführten polizeilichen Informationssystems abgeglichen werden. Die Sachfahndungsdateien des polizeilichen Informationssystems umfassen auch die nach den Vorschriften des Schengener Durchführungsübereinkommens zulässigen Ausschreibungen von Fahrzeugkennzeichen im Schengener Informationssystem.

Die von den Polizeien des Bundes und der Länder geführten Fahndungsdateien sind – wie nahezu alle polizeilichen Dateien – sogenannte Mischdateien, die sowohl strafprozessualen als auch präventiven Zwecken dienen. Eine Ermächtigung zum Zugriff auf solche Mischdateien widerspricht dem Gebot der Normenbestimmtheit und Normenklarheit nicht, sofern erkennbar ist, ob der Zugriff selbst ausschließlich oder im Schwerpunkt präventiven oder repressiven Zwecken oder beiden dient (BVerfG, a. a. O, juris, Rn. 151). Aufgrund der klaren Zweckbestimmung in Absatz 1 wird deutlich, dass der automatisierte Datenabgleich zu gefahrenabwehrenden Zwecken erfolgt.

Absatz 2 Satz 3 beschreibt den für den Abgleich heranzuziehenden Fahndungsbestand, um den Datenbestand einzugrenzen und auszuschließen, dass sich der Umfang der einbezogenen Datenbestände in nicht vorhersehbarer Weise verändert (vgl. hierzu BVerfG, a. a. O, juris, Rn. 131, 135). Nach Absatz 2 Satz 4 darf der Abgleich nur mit vollständigen Kennzeichen des Fahndungsbestands erfolgen. Würden nämlich zum Fahndungsbestand auch solche Kennzeichen gezählt, bei denen der Polizei nur Teile eines Kennzeichens bekannt sind, nach dem gefahndet wird, würden von der Maßnahme möglicherweise in großer Zahl auch Personen erfasst, die keinen Anlass für die Fahndung gegeben haben (vgl. BVerfG, a. a. O, juris, Rn. 176). Dies wird durch die Vorgabe in Absatz 2 Satz 4 ausgeschlossen.

Absatz 3 Satz 1 regelt die sogenannten Nichttrefferfälle. Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt nicht vor, wenn der Abgleich mit dem Fahndungsbestand unverzüglich vorgenommen wird und negativ ausfällt sowie zusätzlich rechtlich und technisch gesichert ist, dass die Daten anonym bleiben und sofort spurenlos gelöscht werden (BVerfG, a. a. O, juris, Rn. 68). Dementsprechend gibt Absatz 3 Satz 1 vor, dass die erhobenen Daten im Nichttrefferfall sofort nach Durchführung des Datenabgleichs automatisiert zu löschen sind. Damit können sich in einem Nichttrefferfall auch keine weiteren Folgemaßnahmen ergeben. Die spurenlose Löschung der erhobenen Daten wird in der Praxis der Regelfall sein, da einem gesuchten Kennzeichen eine wesentlich höhere Anzahl nicht relevanter Kennzeichen gegenüber steht. Der spurenlosen Löschung von Daten ist eine Verfahrensweise gleichgesetzt, die eine teilweise oder vollständige Rekonstruktion der Daten nach dem aktuellen Stand der Technik unmöglich macht.

Absatz 3 Satz 2 regelt den Umfang der zu speichernden Daten im Trefferfall. Gespeichert werden dürfen das Kennzeichen sowie Angaben zu Ort, Datum, Uhrzeit und Fahrtrichtung. Nach Absatz 3 Satz 3 ist im Trefferfall unverzüglich die Übereinstimmung zwischen den erfassten Daten und den Daten aus dem Fahndungsbestand zu überprüfen. Hierdurch sollen sogenannte unechte Trefferfälle erkannt werden, in denen die Erkennungssoftware des Kennzeichenlesegerätes ein Kennzeichen falsch ausgelesen hat und das falsch erkannte Kennzeichen zufällig im Fahndungsbestand enthalten ist. Durch einen Abgleich des Kennzeichenfotos mit den Daten aus dem Fahndungsbestand können diese unechten Trefferfälle erkannt und die erfassten Daten manuell sofort und spurenlos gelöscht werden.

Nach Absatz 3 Satz 4 dürfen das Fahrzeug und die Insassen im Trefferfall angehalten werden. Über das Anhalten hinausgehende Maßnahmen sind nach Absatz 3 Satz 5 erst zulässig, wenn zuvor die Übereinstimmung zwischen den erfassten Daten und den Daten aus dem Fahndungsbestand festgestellt worden sind. Hierdurch wird sichergestellt, dass weitere Maßnahmen nur bei einem fehlerfreien (echten) Trefferfall erfol-

gen. Absatz 3 Satz 6 und 7 regelt die Weiterverarbeitung der gespeicherten Daten im Trefferfall. Insoweit wird festgelegt, dass Daten im Trefferfall sofort und spurenlos zu löschen sind, wenn die Ausschreibung im Fahndungsbestand nicht im Zusammenhang mit den in Absatz 1 Nr. 1 bis 3 genannten Zwecken steht. Eine weitere Verwendung der Daten ist dann nur zulässig, wenn sie zur Verfolgung einer Straftat von erheblicher Bedeutung benötigt werden.

Zu Nummer 5 (§ 28)

Zu Buchstabe a

Zu Doppelbuchstabe aa

Das Bundesverfassungsgericht hat aus dem Verhältnismäßigkeitsgrundsatz für heimliche Überwachungsmaßnahmen, die tief in die Privatsphäre eingreifen, übergreifende Anforderungen abgeleitet (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 103 ff.). Zwar dürfen solche Maßnahmen auch der Straftatenverhütung dienen und damit bereits im Vorfeld konkreter Gefahren ansetzen. Eine Anknüpfung der Einschreitschwelle an das Vorfeldstadium sei verfassungsrechtlich angesichts der Schwere des Eingriffs jedoch nicht hinnehmbar, wenn „nur relativ diffuse Anhaltspunkte für mögliche Gefahren bestehen“ (BVerfG, a. a. O, Rn. 113). Voraussetzung sei vielmehr eine auf bestimmte Tatsachen und nicht allein auf allgemeine Erfahrungssätze gestützte Prognose, die auf eine konkrete Gefahr bezogen ist. Dazu gehöre, dass ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist (BVerfG, a. a. O, Rn. 112, 164).

Absatz 2 Satz 1 Nr. 2 erlaubt die verdeckte Datenerhebung mit besonderen Mitteln zur Straftatenverhütung über Personen, bei denen durch Tatsachen begründete Anhaltspunkte die Annahme rechtfertigen, dass sie zukünftig Straftaten von erheblicher Bedeutung begehen. Die diesbezüglichen Prognoseanforderungen genügen den dargestellten Anforderungen des Bundesverfassungsgerichts nicht. Mit der Änderung wird die Einschreitschwelle deshalb an Tatsachen geknüpft, die ein konkretisiertes und zeitlich absehbares Geschehen erkennen lassen.

Zu Doppelbuchstabe bb

Das Bundesverfassungsgericht hat in seiner Entscheidung zum Bundeskriminalamtgesetz die in der Rechtsprechung der letzten Jahre entwickelten Kriterien für die Zulässigkeit heimlicher Überwachungsmaßnahmen im Vorfeld von Terrorgefahren präzisiert. So heißt es: „In Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, können Überwachungsmaßnahmen auch dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird. Denkbar ist das etwa, wenn eine Person aus einem Ausbildungslager für Terroristen im Ausland in die Bundesrepublik Deutschland einreist“ (BVerfG,a. a. O, Rn. 112). Mit dieser Prognosemöglichkeit, die nicht an ein konkretes Schadensereignis, sondern an das individuelle Verhalten einer Person anknüpft, will das Bundesverfassungsgericht den Besonderheiten bei Terrorgefahren Rechnung tragen. Oftmals liegen den Sicherheitsbehörden nur Erkenntnisse darüber vor, dass bestimmte Personen Attentate in Deutschland planen; das drohende Schadensereignis selbst kann aber noch nicht konkret beschrieben werden. Anders formuliert: die vorhandenen Tatsachen lassen noch nicht den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zu. In diesen Fällen kann die Prognose statt auf das Ergebnis eines Schadensverlaufs auch auf das Verhalten eines Schädigers – hier eines Terroristen – gerichtet werden. Heimliche Überwachungsmaßnahmen sind dann bereits zulässig, wenn Tatsachen die Annahme rechtfertigen, dass eine Person mit hinreichender Wahrscheinlichkeit terroristische Straftaten begehen wird.

Anknüpfend an diese Rechtsprechung wird in der neu eingefügten Nummer 3 die Möglichkeit geschaffen, besondere Mittel der verdeckten Datenerhebung bereits dann einzusetzen, wenn Hinweise auf das individuelle Verhalten einer Person vorliegen, die die konkrete Wahrscheinlichkeit begründen, dass sie innerhalb eines übersehbaren Zeitraums terroristische Straftaten begehen wird. Nicht vorausgesetzt wird, dass die drohende Straftat bereits ihrer Art nach konkretisiert werden kann. Hinweise, die die konkrete Wahrscheinlichkeit eines terroristischen Anschlags begründen, können sich aus dem Vorverhalten einer Person (z. B. Rückkehr aus einem ausländischen Terror-Camp) oder aus sonstigen Umständen ergeben, die Rückschlüsse auf das individuelle Verhalten zulassen (z. B. glaubwürdige Aussagen eines Zeugen).

Zu Doppelbuchstabe cc

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Buchstabe b

Zu Doppelbuchstaben aa bis cc

Mit der Änderung werden die bislang in der Nummer 2 zusammengefassten technischen Mittel zur Anfertigung von Bildaufzeichnungen sowie zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes in jeweils eigenen Nummern aufgeführt. Grund hierfür ist das unterschiedliche Eingriffsgewicht der Maßnahmen, das eine jeweils unterschiedliche Ausgestaltung der Anordnungskompetenz und der Zulässigkeit einer Zweckänderung zur Folge hat (vgl. BVerfG, a. a. O, Rdn. 172 ff.).

Zu Buchstabe c

Absatz 4 sieht in seiner bisherigen Fassung für die längerfristige Observation und den Einsatz technischer Mittel zur Feststellung des jeweiligen Standortes einer Person oder eines Fahrzeugs keinen Richtervorbehalt vor. Lediglich der Einsatz besonderer Mittel nach dem bisherigen Absatz 2 Nr. 2 bis 4, der länger als sieben Tage durchgeführt werden soll oder durchgeführt wird, bedarf der richterlichen Entscheidung. Hierbei handelt es sich um den verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufzeichnungen sowie zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes, den Einsatz verdeckter Ermittler und den Einsatz von Vertrauenspersonen. Diese Regelung genügt den verfassungsrechtlichen Anforderungen an den Richtervorbehalt nicht.

Das Bundesverfassungsgericht hat mit Blick auf das jeweilige Eingriffsgewicht der besonderen Mittel der verdeckten Datenerhebung entschieden, dass bereits die erstmalige Anordnung einer längerfristigen Observation, das Abhören und Auf-

zeichnen des nicht öffentlich gesprochenen Wortes und der Einsatz von verdeckten Ermittlern oder Vertrauenspersonen unter Richtervorbehalt stehen muss (BVerfG, a. a. O, Rn. 174, 358).

Mit der Regelung in Absatz 4 Satz 1 werden die Vorgaben des Bundesverfassungsgerichts umgesetzt. So wird festgelegt, dass der Einsatz besonderer Mittel nach Absatz 2 Nr. 1, 3 bis 5 bereits bei der erstmaligen Anordnung einer richterlichen Entscheidung bedarf.

Bislang ist in Absatz 4 Satz 2 geregelt, dass die Maßnahme zu befristen ist und wiederholt angeordnet werden kann. Eine Höchstdauer für die Befristung ist nicht vorgesehen. In Konkretisierung des Verhältnismäßigkeitsgrundsatzes wird nunmehr vorgegeben, dass die Anordnung einer längerfristigen Observation und der Einsatz technischer Mittel zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes auf höchstens einen Monat sowie der Einsatz von verdeckten Ermittlern und Vertrauenspersonen auf höchstens drei Monate zu befristen ist. Eine Verlängerung um jeweils nicht mehr als denselben Zeitraum ist nach Absatz 4 Satz 3 zulässig, sofern die Voraussetzungen der Anordnung weiterhin vorliegen. Die Festlegung einer zeitlichen Obergrenze für die Verlängerung der Maßnahmen ist verfassungsrechtlich nicht geboten. Eine solche folgt im Einzelfall aus dem Grundsatz der Verhältnismäßigkeit, da das Eingriffsgewicht mit zunehmender Dauer der Überwachungsmaßnahmen intensiver wird und schließlich dazu führen kann, dass eine weitere Verlängerung verfassungsrechtlich unzulässig ist (vgl. BVerfG, a. a. O, Rn. 171).

Zuständig für die Anordnung der Maßnahmen ist nach Absatz 4 Satz 4 das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat.

Absatz 4 Satz 6 regelt die Anordnungskompetenz der Behördenleitung bzw. eines von ihr besonders beauftragten Beamten mit der Befähigung für das vierte Einstiegsamt bei Gefahr im Verzug. Die richterliche Entscheidung ist unverzüglich nachzuholen.

Zu Buchstabe d

Absatz 5 regelt die Anordnungskompetenz für den Einsatz besonderer Mittel, die kein so großes Eingriffsgewicht haben, dass deren Anordnung durch einen Richter verfassungsrechtlich geboten ist. Hierbei handelt es sich um Bildaufzeichnungen bestimmter Personen, die durchgehend weniger als 24 Stunden oder nicht über einen Zeitraum von mehr als einer Woche angefertigt werden sollen sowie um den Einsatz technischer Mittel zur Feststellung des jeweiligen Standorts einer Person oder eines Fahrzeugs. Wie bislang können diese Maßnahmen durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten mit der Befähigung für das vierte Einstiegsamt angeordnet werden. Die Maßnahme ist zu befristen und kann wiederholt angeordnet werden. Absatz 5 Satz 3 regelt die Anordnung der Maßnahmen bei Gefahr im Verzug.

Zu Buchstabe e

In Absatz 6 Satz 1 und 2 wird eine besondere Kennzeichnungspflicht für Daten aufgenommen, die aus den eingriffsintensiveren Maßnahmen nach Absatz 1 Satz 1 Nr. 1, 3 bis 5 erlangt worden sind. Nur wenn nach der Informationserhebung erkennbar ist, dass die Daten aus entsprechenden Maßnahmen stammen, können der Grundsatz der Zweckbindung und die Grenzen einer zulässigen Zweckänderung gewährleistet werden. Während Satz 1 die Kennzeichnungspflicht für die datenerhebende Behörde festlegt, betrifft Satz 2 die Pflicht zur Aufrechterhaltung der Kennzeichnung im Falle einer Datenübermittlung durch die datenempfangende Behörde.

Das Bundesverfassungsgericht hat in seinem Urteil vom 20. April 2016 klargestellt, dass eine zweckändernde Nutzung von Daten, die aus eingriffsintensiven Maßnahmen stammen, nur dann zulässig ist, wenn die entsprechenden Daten auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln erhoben werden dürften. (BVerfG, a. a. O, Rn. 287). Darüber hinaus müssen sich aus den vorliegenden Informationen im Einzelfall konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter wie die ergeben, zu deren Schutz die entsprechende Datenerhebung zulässig ist (BVerfG, a. a. O, Rn. 290). Die bisherige Regelung in Absatz 5 genügt diesen Anforderungen nicht, da die Zulässigkeit einer zweckändernden Nutzung der Daten hier nicht davon abhängig gemacht wird, dass sich in Bezug auf die Verfolgung oder Verhütung von Straftaten bzw. die Abwehr einer Gefahr bereits ein konkreter Ermittlungsansatz ergibt. Deshalb wird in Absatz 6 Satz 3 für die eingriffsintensiveren Maßnahmen nach Absatz 1 Satz 1 Nr. 1, 3 bis 5 POG festgelegt, dass eine Zweckänderung nur zulässig ist, wenn für eine Nutzung zu anderen Zwecken konkrete Ermittlungsansätze vorliegen. Die Zweck-änderung muss nach Absatz 6 Satz 4 im Einzelfall festgestellt und dokumentiert werden. Hierdurch wird sichergestellt, dass die Zweckänderung nachvollziehbar ist und ihre Zulässigkeit gegebenenfalls überprüft werden kann.

Zu Buchstabe f

Die zweckändernde Nutzung von Daten, die durch die weniger gewichtigen Eingriffe nach Absatz 1 Satz 1 Nr. 2 und 6 erlangt wurden, wird unter im Vergleich zu Absatz 6 erleichterten Voraussetzungen zugelassen. Die Vorgaben orientieren sich an der bisherigen Regelung in Absatz 5.

Zu Buchstabe g

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Nummer 6 (§ 29)

Zu Buchstabe a

Mit der Neufassung des Absatzes 1 werden die Vorgaben des Bundesverfassungsgerichts aus seinem Urteil vom 20. April 2016 umgesetzt. Das Bundesverfassungsgericht hat entschieden, dass die konkrete Ausgestaltung der Ermächtigungen im Bundeskriminalamtgesetz zum Einsatz heimlicher Überwachungsmaßnahmen zur Abwehr von Gefahren des internationalen Terrorismus teilweise unverhältnismäßig ist. Eingriffsbefugnisse, die wie die Wohnraumüberwachung oder die Online-Durchsuchung tief in die Privatsphäre eingreifen, unterliegen als Ausfluss des Verhältnismäßigkeitsgrundsatzes besonders strengen Vorgaben an ihre Ausgestaltung. Diese Maßnahmen dürfen sich unmittelbar nur gegen diejenigen als Zielpersonen richten, die für die Gefahr verantwortlich sind (BVerfG, a. a. O, Rn. 115, 192). Nach der bisherigen Regelung in § 29 Abs. 1 Satz 1 POG darf sich eine Wohnraumüberwachung nicht nur gegen die für die Gefahr Verantwortlichen, sondern auch

gegen Nichtverantwortliche sowie gegen Kontakt- und Begleitpersonen richten. Das ist nach Auffassung des Bundesverfassungsgerichts unverhältnismäßig. Aus diesem Grund wird der Kreis der Adressaten einer Wohnraumüberwachung in Absatz 1 Satz 1 auf die nach den §§ 4 und 5 POG Verantwortlichen beschränkt. Das Bundesverfassungsgericht hat es allerdings als verfassungsrechtlich hinnehmbar bezeichnet, wenn bei einer gegen den Verantwortlichen angeordneten Wohnraumüberwachung auch Dritte miterfasst werden. So könne die Überwachung der Wohnung eines Dritten erlaubt werden, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass sich der Verantwortliche während der Überwachung dort aufhält, für die Ermittlungen relevante Gespräche führen wird und eine Überwachung seiner Wohnung allein zur Erforschung des Sachverhalts nicht ausreicht (BVerfG, a. a. O, Rn. 115, 188). Dementsprechend wird in Absatz 1 Satz 2 festgelegt, dass eine Wohnraumüberwachung unter den vom Bundesverfassungsgericht genannten Voraussetzungen auch in der Wohnung eines Dritten durchgeführt werden darf.

Nach Absatz 1 Satz 6 darf eine Wohnraumüberwachung auch durchgeführt werden, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird. Mit dieser Änderung werden die in der Entscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtgesetz entwickelten Prognosekriterien aufgegriffen. Vgl. dazu die Begründung zu Artikel 1 Nummer 5 Buchstabe a Doppelbuchstabe bb.

Zu Buchstabe b

Zu Doppelbuchstabe aa

Absatz 5 Satz 3 regelt die Zulässigkeit einer Nutzung der aus einer Wohnraumüberwachung erlangten Daten zu anderen Zwecken als denen der ursprünglichen Datenerhebung. In seiner Entscheidung zum Bundeskriminalamtgesetz hat das Bundesverfassungsgericht seine Rechtsprechung zu den Grundsätzen der Zweckbindung und Zweckänderung fortentwickelt. Die Verhältnismäßigkeitsanforderungen für eine zweckändernde Datenverwendung müssen sich am Grundsatz der hypothetischen Datenneuerhebung orientieren. Danach gilt, dass die neue Nutzung der erhobenen Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen können (BVerfG, a. a. O, Rn. 288). Die bisherige Regelung zur Zweckänderung in Absatz 5 Satz 3 entspricht zwar dem Kriterium der hypothetischen Datenneuerhebung, da eine zweckändernde Nutzung der Daten nur zur Verfolgung von besonders schweren Straftaten, die nach der Strafprozessordnung eine Wohnraumüberwachung rechtfertigen bzw. nur zur Abwehr einer dringenden Gefahr zulässig ist. Die Vorschrift gewährleistet aber nicht, dass – wie vom Bundesverfassungsgericht gefordert – nur solche Daten zum Zwecke der Strafverfolgung genutzt werden dürfen, die konkrete Ermittlungsansätze zur Aufdeckung der fraglichen Straftaten erkennen lassen (BVerfG, a. a. O, Rn. 315). Dementsprechend wird in Absatz 5 Satz 3 Nr. 1 festgelegt, dass eine Zweckänderung nur zulässig ist, wenn sich aus den erlangten Daten konkrete Ermittlungsansätze zur Verfolgung von besonders schweren Straftaten ergeben.

Zu Doppelbuchstabe bb

Mit dem neu eingefügten Satz 4 wird klargestellt, dass personenbezogene Daten, die aus einer optischen Wohnraumüberwachung stammen, nicht für Zwecke der Strafverfolgung verwendet werden dürfen. Das Bundesverfassungsgericht hat in seinem Urteil zum Bundeskriminalamtgesetz ausgeführt, dass eine zweckändernde Nutzung von Daten nur zulässig ist, wenn für den neuen Zweck eine entsprechende Datenerhebung nach verfassungsrechtlichen Maßstäben zulässig wäre. Artikel 13 Abs. 3 des Grundgesetzes erlaubt für den Bereich der Strafverfolgung nur die akustische, nicht aber auch die optische Wohnraumüberwachung (vgl. BVerfG, a. a. O, Rn. 317).

Zu Buchstabe c

Es handelt sich um eine Folgeänderung zum neu gestalteten Laufbahnrecht (vgl. die Begründung zu Artikel 1 Nummer 2).

Zu Buchstabe d

Es handelt sich um die Korrektur eines redaktionellen Versehens.

Zu Nummer 7 (§ 31)

Zu Buchstabe a

Nach Absatz 1 Satz 2 darf eine Telekommunikationsüberwachung auch durchgeführt werden, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird. Mit dieser Änderung werden die in der Entscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtgesetz entwickelten Prognosekriterien aufgegriffen. Vgl. dazu die Begründung zu Artikel 1 Nummer 5 Buchstabe a Doppelbuchstabe bb.

Zu Buchstabe b

Auch eine Quellen-Telekommunikationsüberwachung wird – entsprechend der Änderung zur herkömmlichen Telekommunikationsüberwachung in Absatz 1 – bereits dann zugelassen, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird. Vgl. dazu die Begründung zu Artikel 1 Nummer 5 Buchstabe a Doppelbuchstabe bb.

Zu Buchstabe c

Es handelt sich um eine Folgeänderung zum neu gestalteten Laufbahnrecht (vgl. die Begründung zu Artikel 1 Nummer 2).

Zu Buchstabe d

Die bisherige Regelung in Absatz 7 Satz 1 verweist zur Zulässigkeit einer Zweckänderung auf die Regelung in § 29 Abs. 5 POG. Danach dürfen Daten, die durch eine präventive Telekommunikationsüberwachung erlangt wurden, zur Verfolgung von besonders schweren Straftaten, die nach der Strafprozessordnung eine Wohnraumüberwachung rechtfertigen, verwendet werden. Die Beschränkung auf besonders schwere Straftaten im Sinne des § 100 c Abs. 2 StPO entspricht zwar dem Kriterium der hypothetischen Datenneuerhebung, geht aber über das hinaus, was verfassungsrechtlich gefordert ist. Da die Telekommunikationsüberwachung keinen vergleich-

bar schwerwiegenden Eingriff wie eine Wohnraumüberwachung darstellt, ist eine Zweckänderung hier bereits dann verhältnismäßig, wenn sie zur Verfolgung von schweren Straftaten im Sinne des § 100 a Abs. 2 StPO zugelassen wird. Dementsprechend wird statt eines Verweises auf § 29 Abs. 5 POG nunmehr in dem neu eingefügten Absatz 7 eine eigene Zweckänderungsregelung für Daten, die aus einer Telekommunikationsüberwachung erlangt wurden, geschaffen.

Zu Buchstabe e

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Nummer 8 (§ 31 a)

Es handelt sich um eine Folgeänderung zum neu gestalteten Laufbahnrecht (vgl. die Begründung zu Artikel 1 Nummer 2).

Zu Nummer 9 (§ 31 b)

Zu Buchstabe a

Nach dem neu eingefügten Satz 2 dürfen Nutzungsdaten auch abgefragt werden, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird. Mit dieser Änderung werden die in der Entscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtgesetz entwickelten Prognosekriterien aufgegriffen. Vgl. dazu die Begründung zu Artikel 1 Nummer 5 Buchstabe a Doppelbuchstabe bb.

Zu Buchstabe b

Zur Zulässigkeit einer Zweckänderung verweist die bisherige Regelung in Absatz 4 auf § 29 Abs. 5 POG. Danach dürfen Daten, die durch eine Auskunft über Nutzungsdaten erlangt wurden, zur Verfolgung von besonders schweren Straftaten, die nach der Strafprozessordnung eine Wohnraumüberwachung rechtfertigen, verwendet werden. Das Eingriffsgewicht einer Maßnahme nach § 31 b POG ist jedoch geringer als das einer Wohnraumüberwachung und entspricht dem einer Auskunft über Verkehrsdaten nach § 31 POG. Dementsprechend wird nunmehr auf den neu eingefügten § 31 Abs. 7 POG verwiesen.

Zu Nummer 10 (§ 31 c)

Nach geltender Rechtslage kann sich eine Online-Durchsuchung gegen die nach den §§ 4 und 5 Verantwortlichen und gegen Nachrichtenmittler richten. Nachrichtenmittler entstammen zwar dem Umfeld einer Zielperson, sind selbst aber keine Verantwortlichen im Sinne der §§ 4 und 5 POG. Wie das Bundesverfassungsgericht in seiner Entscheidung zum Bundeskriminalamtgesetz deutlich gemacht hat, handelt es sich bei der Online-Durchsuchung um einen so schwerwiegenden Eingriff in die Privatsphäre, dass unmittelbarer Adressat dieser Maßnahme nur derjenige sein darf, der für die Gefahr verantwortlich ist (BVerfG, a. a. O, Rn. 115). In Umsetzung dieser Vorgabe wird deshalb der Nachrichtenmittler aus dem Adressatenkreis herausgenommen. Dass sich die Online-Durchsuchung unmittelbar nur gegen die verantwortliche Zielperson richten darf, schließt nach Auffassung des Bundesverfassungsgerichts allerdings nicht aus, dass durch die Maßnahme, sofern unvermeidbar, auch Dritte miterfasst werden. So dürfe eine Online-Durchsuchung auch auf informationstechnische Systeme Dritter erstreckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass der Verantwortliche dort ermittlungsrelevante Informationen speichert und ein auf sein eigenes informationstechnisches System beschränkter Zugriff zur Erreichung des Ermittlungsziels nicht ausreicht (BVerfG, a. a. O, Rn. 115). Diese Vorgabe wird mit der Regelung in Absatz 1 Satz 3 umgesetzt. Darüber hinaus wird entsprechend den vom Bundesverfassungsgericht entwickelten Prognosekriterien festgelegt, dass eine Online-Durchsuchung auch gegen eine Person zulässig ist, deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird. Vgl. dazu die Begründung zu Artikel 1 Nummer 5 Buchstabe a Doppelbuchstabe bb.

Zu Nummer 11 (§ 31 d)

Es handelt sich um eine Folgeänderung zum neu gestalteten Laufbahnrecht (vgl. die Begründung zu Artikel 1 Nummer 2).

Zu Nummer 12 (§ 31 e)

Zu Buchstabe a

Die Regelung in § 31 e Abs. 1 POG in ihrer bisherigen Fassung lässt offen, wer Adressat einer Funkzellenabfrage sein kann. Insbesondere ist unklar, ob die allgemeinen Adressatenregelungen der §§ 4, 5 und 7 POG gelten sollen oder die spezielle Regelung in § 31 Abs. 1 POG Anwendung findet. Unter dem Aspekt der Normenklarheit und Normenbestimmtheit wird der Adressatenkreis nunmehr explizit geregelt. Da die Funkzellenabfrage ein spezieller Fall der Verkehrsdatenerhebung nach § 31 Abs. 1 POG ist, entspricht der Adressatenkreis demjenigen in § 31 Abs. 1 POG. Auskunft über Verkehrsdaten kann somit über die nach den §§ 4 und 5 POG Verantwortlichen und unter den Voraussetzungen des § 7 POG über die dort genannten Personen sowie über Nachrichtenmittler und Personen verlangt werden, deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen werden. Vgl. dazu die Begründung zu Artikel 1 Nummer 5 Buchstabe a Doppelbuchstabe bb. In Absatz 1 Satz 3 wird klargestellt, dass die Maßnahme auch durchgeführt werden darf, wenn Dritte unvermeidbar betroffen sind, was bei einer Funkzellenabfrage regelmäßig der Fall ist.

Zu Buchstabe b

Zur Zulässigkeit einer Zweckänderung verweist die bisherige Regelung in Absatz 2 Satz 2 Halbsatz 2 auf § 29 Abs. 5 POG. Danach dürfen Daten, die durch eine Funkzellenabfrage erlangt wurden, zur Verfolgung von besonders schweren Straftaten, die nach der Strafprozessordnung eine Wohnraumüberwachung rechtfertigen, verwendet werden. Das Eingriffsgewicht einer Maßnahme nach § 31 e POG entspricht jedoch demjenigen einer Auskunft über Verkehrsdaten nach § 31 POG. Deshalb wird nunmehr auf den neu eingefügten § 31 Abs. 7 POG verwiesen.

Zu Nummer 13 (§ 31 f)

Mit Beschluss vom 24. Januar 2012 (1 BvR 1299/05) hat das Bundesverfassungsgericht die damalige Ausgestaltung des manuellen Auskunftsverfahrens in § 113 des Telekommunikationsgesetzes (TKG) vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 1 und 12 des Gesetzes vom 4. November 2016 (BGBl. I S. 2473), für teilweise verfassungswidrig erklärt und angeordnet, dass die Regelungen, soweit sie den verfassungsrechtlichen Anforderungen nicht genügen, übergangsweise, längstens jedoch bis zum 30. Juni 2013, weiter angewendet werden dürfen.

Gegenstand des Beschlusses war eine Verfassungsbeschwerde, die sich gegen die Vorschriften der §§ 111 bis 113 TKG richtete.

§ 111 TKG verpflichtet die Telekommunikationsunternehmen, die von ihnen vergebenen bzw. bereitgestellten Rufnummern, Anschlusskennungen, Mobilfunkendgerätenummern und Kennungen von elektronischen Postfächern sowie die zugehörigen Daten der Anschlussinhaber wie Namen, Anschrift und Geburtsdaten zu erheben und zu speichern, um diese für die Aufgabenwahrnehmung der Sicherheitsbehörden verfügbar zu halten und die Datenbasis für die in §§ 112 und 113 TKG geregelten automatisierten und manuellen Auskunftsverfahren zu schaffen. Die von § 111 TKG erfassten Daten ermöglichen die individualisierende Zuordnung von Telekommunikationsnummern zu den jeweiligen Anschlussinhabern und damit zu deren potenziellen und typischen Nutzern. Nähere private Daten enthalten diese Daten nicht.

§ 112 TKG regelt die Verwendung der nach § 111 TKG gespeicherten Daten in Form eines automatisierten Auskunftsverfahrens, bei dem die Bundesnetzagentur die Daten auf Ersuchen an die in § 112 Abs. 2 TKG genannten Behörden zu übermitteln hat. Als Rechtsgrundlage für den Datenabruf der um Auskunft ersuchenden Behörde genügt eine schlichte Datenerhebungsgeneralklausel, wie sie sich für die rheinland-pfälzische Polizei als Gefahrenabwehrbehörde in § 26 POG findet.

Etwas anderes gilt für das manuelle Auskunftsverfahren nach § 113 TKG, das eine Datenübermittlungsbefugnis für private Telekommunikationsunternehmen begründet. Auskunftsverlangen der Sicherheitsbehörden können hier nicht auf eine schlichte Datenerhebungsgeneralklausel gestützt werden. Erforderlich ist vielmehr – so das Bundesverfassungsgericht – eine bereichsspezifische Abrufnorm, die eine Verpflichtung der Telekommunikationsdiensteanbieter gegenüber der abrufberechtigten Behörde aus sich heraus normenklar begründet (BVerfG, a. a. O, juris, Rn. 167).

Ferner hat das Bundesverfassungsgericht entschieden, dass auch der Abruf von Bestandsdaten, der nur über die Zuordnung einer dynamischen IP-Adresse möglich ist, einer ausdrücklichen gesetzlichen Regelung bedarf (BVerfG, a. a. O, juris, Rn. 174). Die Deanonymisierung von dynamischen IP-Adressen ist mit einem Eingriff in das Telekommunikationsgeheimnis nach Artikel 10 Abs. 1 des Grundgesetzes verbunden und bedarf einer hinreichend normenklaren Befugnis.

Schließlich hat das Bundesverfassungsgericht gefordert, dass die Sicherheitsbehörden Auskünfte über Daten, die als Zugangssicherungscodes wie Passwörter, PIN und PUK den Zugang zu Endgeräten und Speichereinrichtungen sichern (§ 113 Abs. 1 Satz 2 TKG), nur dann verlangen können, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind (BVerfG, a. a. O, juris, Rn. 185). Wird z. B. eine PIN benötigt, um die auf einem Mobiltelefon abgelegten Daten auszulesen, so muss die Zulässigkeit einer Abfrage der PIN davon abhängig gemacht werden, dass auch die Voraussetzungen für eine Sicherstellung des Mobiltelefons vorliegen.

Wenngleich Gegenstand des Beschlusses des Bundesverfassungsgerichts nur die Regelungen des Telekommunikationsgesetzes waren, lassen sich die Kernaussagen der Entscheidung auf den Abruf von Bestandsdaten nach dem Telemediengesetz (TMG) vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Artikel 1 des Gesetzes vom 21. Juli 2016 (BGBl. I S. 1766), übertragen. Dementsprechend setzen auch Auskunftsersuchen zu Bestandsdaten gegenüber den Anbietern von Telemedien eine bereichsspezifische Ermächtigungsnorm voraus. Die neue Regelung zum Abruf von Bestandsdaten ist daher nicht auf Bestandsdaten nach dem Telekommunikations-gesetz beschränkt, sondern erfasst auch die Bestandsdaten nach dem Telemediengesetz.

Telemedien sind elektronische Informations- und Kommunikationsdienste, soweit sie nicht der Telekommunikation oder dem Rundfunk zuzuordnen sind. Die Abgrenzung kann im Einzelfall schwierig sein. Entscheidend ist letztlich der Gegenstand des Dienstes. Bei Telemediendiensten steht die Bereitstellung von Informationen im Vordergrund. Bei der Telekommunikation kommt es nicht auf die Bereitstellung von Informationen an, sondern auf die Bereitstellung von Datenübertragungsmöglichkeiten (z. B. Telefon). Telemediendienste sind z. B. Online-Angebote von Waren oder Dienstleistungen im Internet, Internet-Suchmaschinen, Telebanking, Online-Computerspiele, Werbe-Mails und wohl auch Messenger-Dienste wie Whatsapp oder Skype.

Die neue Befugnisnorm zur Abfrage von Bestandsdaten im manuellen Auskunftsverfahren legt dem Grundsatz der Normenklarheit folgend fest, unter welchen Voraussetzungen eine Abfrage von Bestandsdaten zulässig ist.

Der Begriff der Bestandsdaten wird in Absatz 5 legaldefiniert. Die Definition deckt sich durch die Bezugnahme auf § 95 TKG mit der Begriffsbestimmung in § 3 Nr. 3 TKG, erweitert um die in § 111 TKG genannten Daten. Bestandsdaten sind danach Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Nicht für betriebliche Zwecke gespeicherte Bestandsdaten gehören dazu, soweit sie in § 111 TKG genannt werden. Erfasst werden danach z. B. Name, Anschrift, Geburtsdatum, E-Mail-Adressen oder Rufnummern und andere Anschlusskennungen. Bestandsdaten nach dem Telemediengesetz sind gem. § 14 Abs. 1 TMG Daten eines Nutzers, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (z. B. Name, Zugangsdaten, Profilname, E-Mail-Adresse).

Für die polizeiliche Gefahrenabwehr sind Bestandsdatenauskünfte vor allem zur Verhinderung von angedrohten Suiziden, zum Auffinden von vermissten und hilflosen Personen sowie zur Verhinderung von angedrohten Straftaten gegen Leib, Leben oder Freiheit einer Person (z. B. Amok- oder Anschlagstaten) von großer Bedeutung.

Die Voraussetzungen der manuellen Bestandsdatenabfrage sind entsprechend der jeweiligen Eingriffstiefe gestaffelt. Während die Eingriffsschwelle bei einer einfachen Bestandsdatenabfrage relativ niedrig ist und lediglich an das Erfordernis einer konkreten Gefahr anknüpft, werden an den Zugriff auf Zugangssicherungscodes und die Zuordnung dynamischer IP-Adressen zu ihren Anschlussinhabern, bei der in den Schutzbereich des Artikel 10 Abs. 1 des Grundgesetzes eingegriffen wird, gesteigerte Anforderungen und Verfahrenssicherungen gestellt.

Absatz 1 Satz 1 regelt die einfache Bestandsdatenabfrage nach § 113 Abs. 1 Satz 1 TKG. Voraussetzung ist das Vorliegen einer konkreten Gefahr für die öffentliche Sicherheit oder Ordnung. Das Bundesverfassungsgericht hat in seinem Beschluss vom 24. Januar 2012 hervorgehoben, dass das rfordernis einer konkreten Gefahr zur Begrenzung der Auskunftsansprüche notwendig, aber – angesichts des begrenzten Informationsgehalts der betreffenden Daten – auch ausreichend ist (BVerfG, a. a. O, juris, Rn. 177). So ermöglichen die von § 111 TKG erfassten Daten allein die individualisierende Zuordnung von Telekommunikationsnummern zu den jeweiligen Anschlussinhabern und damit zu deren potenziellen Nutzern. Sie umfassen aber weder höchstpersönliche Informationen noch ist mit ihnen die Erstellung von Persönlichkeits- oder Bewegungsprofilen möglich (BVerfG, a. a. O, juris, Rn. 39). Zu dem Kreis der Personen, über die Bestandsdaten erhoben werden dürfen, gehören neben den Handlungs- und Zustandsverantwortlichen auch nicht verantwortliche Personen unter den Voraussetzungen des § 7 POG und Nachrichtenmittler.

Absatz 1 Satz 2 erfasst Auskunftsverlangen über Zugangssicherungscodes, wie Passwörter, PIN oder PUK, die den Zugriff auf Endgeräte (z. B. Mobiltelefon, Notebook) oder Speichereinrichtungen (z. B. externe Festplatte, Clouds, E-Mail-Accounts) schützen. Die Kenntnis der durch Zugangssicherungscodes geschützten Daten kann die Polizei in die Lage versetzen, Informationen zu gewinnen, die zur Abwehr einer Gefahr (etwa zum Auffinden einer vermissten Person) erforderlich sind. Die Polizei wird die mithilfe eines abgefragten Zugangscodes gesicherten Daten allerdings nur dann zur Kenntnis nehmen können, wenn der Nutzer die Daten nicht zusätzlich verschlüsselt hat. Entsprechend den Vorgaben des Bundesverfassungsgerichts wird die Erhebung der Zugangsdaten an das Vorliegen der Voraussetzungen für deren Nutzung geknüpft. Dies bedeutet, dass Zugangssicherungscodes nur abgefragt werden dürfen, wenn eine Vorschrift auch die Nutzung der hierdurch erlangten Daten zur Gefahrenabwehr im konkreten Fall erlaubt. Soll etwa die Nutzung des Zugangscodes eine Telekommunikationsüberwachung oder eine Online-Durchsuchung ermöglichen, so müssen bereits für dessen Abfrage die Voraussetzungen des § 31 oder § 31 c POG vorliegen. Sollen demgegenüber mit dem Code nach der Sicherstellung eines Mobiltelefons auf diesem abgelegte Daten ausgelesen werden, so genügen für die Datenabfrage die geringeren Anforderungen einer Sicherstellung nach § 22 POG.

Absatz 2 erlaubt die Identifizierung einer dynamischen IP-Adresse. Auskünfte über die Zuordnung dynamischer IP-Adressen zu ihren Anschlussinhabern sind am Grundrecht des Artikel 10 Abs. 1 des Grundgesetzes zu messen, weil die Telekommunikationsunternehmen für die Identifizierung einer dynamischen IP-Adresse in einem Zwischenschritt die entsprechenden Verbindungsdaten ihrer Kunden sichten und damit auf konkrete Telekommunikationsvorgänge zugreifen müssen (BVerfG, a. a. O, juris, Rn. 116). Das Bundesverfassungsgericht hat betont, dass die Identifizierung von dynamischen IP-Adressen schon vom Umfang, vor allem aber vom Inhalt der Kontakte her, über die sie Auskunft geben kann, eine erheblich größere Persönlichkeitsrelevanz hat als die bloße Identifizierung einer Telefonnummer, weil sie in weitem Umfang eine Deanonymisierung von Kommunikationsvorgängen im Internet ermöglicht (BVerfG, a. a. O, juris, Rn. 174). Aus diesem Grund bedarf es einer hinreichend bestimmten Befugnis in den Fachgesetzen.

Die Eingriffsschwelle orientiert sich an den Voraussetzungen für eine Auskunft über Nutzungsdaten nach § 31 b Abs. 1 POG. So ist die Identifizierung einer dynamischen IP-Adresse nur zulässig, soweit sie zur Abwehr einer konkreten Gefahr für ein hochwertiges Rechtsgut erforderlich ist. Dies kann etwa der Fall sein, wenn zur Verhinderung einer im Internet angekündigten Amoktat der Anschlussinhaber einer bereits ermittelten IP-Adresse ausfindig gemacht werden muss.

Absatz 3 Satz 1 stellt sicher, dass die Abfrage von Zugangssicherungscodes grundsätzlich einer richterlichen Anordnung bedarf. Aus dem Verweis in Satz 2 auf § 31 Abs. 5 POG ergibt sich, dass zuständiges Gericht das Oberverwaltungsgericht Rheinland-Pfalz ist. Die Abfrage von Zugangssicherungscodes kann nach Satz 3 ohne richterliche Anordnung durchgeführt werden, wenn der Betroffene Kenntnis vom Herausgabeverlangen hat oder haben muss. Dies ist dann der Fall, wenn der Betroffene in die Nutzung der Zugangssicherungscodes eingewilligt hat oder er mit deren Nutzung rechnen muss, weil das entsprechende Endgerät bei ihm sichergestellt wurde oder ein Auskunftsverlangen unter Hinweis auf die Möglichkeit der Abfrage beim Provider zuvor an ihn persönlich gerichtet wurde. Ein richterlicher Beschluss ist auch dann entbehrlich, wenn die Nutzung der Zugangssicherungscodes bereits durch eine richterliche Entscheidung gestattet wurde, z. B. durch einen entsprechenden Beschlagnahmebeschluss der gesicherten Daten (vgl. Bundestagsdrucksache 17/12879, Seite 11). Letztlich wird sichergestellt, dass kein heimlicher Zugriff auf Daten des Betroffenen ohne richterliche Zustimmung erfolgt.

Absatz 4 begründet die Pflicht der Diensteanbieter zur unverzüglichen Übermittlung der abgefragten Bestandsdaten an die Polizei. Satz 2 verweist auf § 12 Abs. 5 POG, der die Entschädigung der Diensteanbieter regelt.

Zu Nummer 14 (§ 32)

Zu Buchstabe a

Es handelt sich um eine Folgeänderung zum neu gestalteten Laufbahnrecht (vgl. die Begründung zu Artikel 1 Nummer 2).

Zu Buchstabe b

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Nummer 15 (§ 37)

Zu Buchstabe a

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Buchstabe b

Es handelt sich um eine Folgeänderung zum neu gestalteten Laufbahnrecht (vgl. die Begründung zu Artikel 1 Nummer 2).

Zu Nummer 16 (§ 38)

Zu Buchstabe a

Zu Doppelbuchstabe aa

Nach der bisherigen Regelung in Absatz 3 Satz 2 ist für die Anordnung einer Rasterfahndung das Amtsgericht zuständig, während für andere heimliche Überwachungsmaßnahmen mit hoher Eingriffsintensität die Zuständigkeit des Oberverwaltungsgerichts Rheinland-Pfalz begründet ist.

Da es sich bei der Rasterfahndung um einen verdachtslosen Grundrechtseingriff mit hoher Streubreite und folglich hoher Eingriffsintensität handelt (BVerfG, Beschluss vom 4. April 2006, 1 BvR 518/02, juris, Rn. 117), erscheint es angemessen, die Zuständigkeit auf das Oberverwaltungsgericht zu übertragen.

Zu Doppelbuchstabe bb

Es handelt sich um eine Folgeänderung zum neu gestalteten Laufbahnrecht (vgl. die Begründung zu Artikel 1 Nummer 2).

Zu Buchstabe b

Der neu eingefügte Absatz 4 dient der Umsetzung der Anforderungen des Bundesverfassungsgerichts aus seinem Urteil vom 20. April 2016 zur Zweckänderung. Nach dem Grundsatz der hypothetischen Datenneuerhebung ist eine Zweckänderung zulässig, wenn die neue Nutzung der Daten zum Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten (BVerfG, a. a. O, Rn. 288). Ausreichend, aber für eine Zweckänderung auch erforderlich ist, dass sich aus den erhobenen Daten konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von Gefahren für vergleichbar gewichtige Rechtsgüter ergeben (BVerfG, a. a. O, Rn. 289). Dementsprechend erlaubt Absatz 4 Satz 3 Nr. 1 eine Verwendung der Daten zu Zwecken der Strafverfolgung, wenn sich aus den Daten konkrete Ermittlungsansätze zur Verfolgung von Straftaten von erheblicher Bedeutung ergeben, die nach der Strafprozessordnung eine Rasterfahndung rechtfertigen. Ferner dürfen die Daten nach Absatz 4 Satz 3 Nr. 2 zur Abwehr einer dringenden Gefahr im Sinne des Absatzes 1 Verwendung finden. Damit entspricht die Regelung dem Grundsatz der hypothetischen Datenneuerhebung.

Zu Buchstabe c

Die Änderungen im bisherigen Absatz 4 dienen der Umsetzung der Vorgaben des Bundesverfassungsgerichts aus seinem Urteil vom 20. April 2016 zur Aufbewahrungsfrist von Löschungsprotokollen. Die Frist für ihre Aufbewahrung muss so bemessen sein, dass die Protokolle bei typisierender Betrachtung nach der Benachrichtigung der Betroffenen und im Rahmen der nächsten periodisch anstehenden Kontrolle durch den Datenschutzbeauftragten noch vorliegen (BVerfG, a. a. O, Rn. 273). Dementsprechend wird festgelegt, dass die Dokumentation über die Löschung erst sechs Monate nach der Benachrichtigung nach § 40 Abs. 5 POG zu löschen ist. Ist die Datenschutzkontrolle nach § 41 b noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.

Zu Nummer 17 (§ 39 a)

Mit der Neufassung der Vorschrift werden die Vorgaben aus dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 zum Schutz des Kernbereichs privater Lebensgestaltung umgesetzt.

Absatz 1 Satz 1 und 2 entspricht der bisherigen Regelung. In Absatz 1 Satz 3 wird klargestellt, dass nicht nur die Tatsache der Datenerhebung, sondern auch die Löschung zu dokumentieren ist. Die Dokumentation darf gemäß Absatz 1 Satz 4 ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Die Sätze 5 und 6 dienen der Umsetzung der verfassungsrechtlichen Vorgaben zur Aufbewahrungsfrist der Löschungsprotokolle zwecks effektiver Ausübung der Betroffenenrechte und einer wirksamen Kontrolle durch den Datenschutzbeauftragten (BVerfG, a. a. O, Rn. 205). Dementsprechend wird festgelegt, dass die Dokumentation sechs Monate nach der Benachrichtigung gemäß § 40 Abs. 5 POG zu löschen ist. Sofern die Datenschutzkontrolle nach § 41 b POG noch nicht beendet ist, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.

Absatz 2 regelt – wie bislang – den Kernbereichsschutz bei der Wohnraumüberwachung auf der Erhebungsebene.

Die Regelung zum Kernbereichsschutz in Absatz 3 bei Datenerhebungen nach den §§ 31, 31 b und 31 c POG wird um die besonderen Mittel der Datenerhebung nach § 28 POG ergänzt. Das Bundesverfassungsgericht fordert auch für den Einsatz besonderer Mittel der Datenerhebung eine ausdrückliche gesetzliche Regelung zum Kernbereichsschutz. Dabei habe der Gesetzgeber in normenklarer Weise Schutzvorkehrungen sowohl auf der Ebene der Datenerhebung als auch auf der Ebene der Datenauswertung und Datenverwertung vorzusehen (BVerfG, a. a. O, Rn. 177). Nach Absatz 3 Satz 1 ist daher vor der Durchführung einer Maßnahme nach § 28 POG eine Prognose dahingehend zu treffen, dass mit der Maßnahme nicht allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erhoben werden. Tatsächliche Anhaltspunkte, die für die Annahme sprechen, dass allein kernbereichsrelevante Daten erfasst werden, können sich z. B. aus der Art der zu überwachenden Räumlichkeiten und dem Verhältnis der zu überwachenden Personen zueinander ergeben. Schützenswert ist insbesondere die nicht öffentliche Kommunikation mit engen Vertrauenspersonen, wie z. B. mit Ehepartnern, Geschwistern oder Verwandten gerader Linie. Gespräche über bevorstehende Straftaten sind jedoch auch unter engen Vertrauenspersonen nicht vom Kernbereichsschutz umfasst.

Absatz 4 Satz 1 enthält das Gebot der unverzüglichen Unterbrechung der Maßnahme, sofern sich während der Durchführung einer Wohnraumüberwachung nach § 29 POG tatsächliche Anhaltspunkte ergeben, dass Inhalte erfasst werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Bestehen in dieser Lage über den höchstvertraulichen Charakter – etwa aus sprachlichen Gründen – Zweifel oder gibt es konkrete Anhaltspunkte, dass im Zusammenhang mit dem Austausch höchstprivater Gedanken auch Straftaten besprochen werden, kann – wie das Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 deutlich gemacht hat – die Überwachung in Form einer automatischen Aufzeichnung fortgeführt werden (BVerfG, a. a. O, Rn. 199). Dementsprechend legt Absatz 4 Satz 2 fest, dass in Zweifelsfällen eine automatische Aufzeichnung fortgesetzt werden darf. Dies impliziert, dass die unmittelbare Kenntnisnahme der möglicherweise kernbereichsrelevanten Daten durch die ermittelnden Stellen ausgeschlossen ist.

Absatz 4 Satz 3 setzt die Vorgabe des Bundesverfassungsgerichts um, wonach die Sichtung der Ergebnisse der Wohnraumüberwachung durch eine unabhängige Stelle vorzunehmen und eine Beschränkung nur auf Zweifelsfälle verfassungsrechtlich unzulässig ist (BVerfG, a. a. O, Rn. 200). Eine unabhängige Sichtung aller Aufzeichnungen aus einer Wohnraumüberwachung vor der Verwendung durch die Polizei dient der verfahrensrechtlichen Absicherung des Kernbe-

reichsschutzes in der Auswertungsphase. Nach Absatz 4 Satz 3 sind daher nicht nur automatische Aufzeichnungen in Zweifelsfällen, sondern alle Erkenntnisse, die durch eine Wohnraumüberwachung erlangt worden sind, dem Oberverwaltungsgericht Rheinland-Pfalz unverzüglich zur Entscheidung über die Verwertbarkeit oder Löschung vorzulegen.

Absatz 4 Satz 4 bis 7 macht von der durch das Bundesverfassungsgericht eröffneten Möglichkeit Gebrauch, die notwendigen Regelungen zu treffen, um der Polizei für Ausnahmefälle bei Gefahr im Verzug auch kurzfristig erste Handlungsmöglichkeiten einzuräumen (BVerfG, a. a. O, Rn. 204). Bei Gefahr im Verzug, wenn eine gerichtliche Entscheidung nach Absatz 4 Satz 3 nicht rechtzeitig eingeholt werden kann, kann die Behördenleitung oder ein von ihr besonders beauftragter Beamter mit der Befähigung für das vierte Einstiegsamt im Benehmen mit dem behördlichen Datenschutzbeauftragten über die Verwertung der Erkenntnisse entscheiden. Bei der Sichtung der Daten kann sich die Behördenleitung bzw. der besonders beauftragte Beamte der technischen Unterstützung von zwei weiteren Bediensteten der zuständigen Polizeibehörde bedienen, von denen einer die Befähigung zum Richteramt haben muss. Die Bediensteten sind – entsprechend den Vorgaben des Bundesverfassungsgerichts – zur Verschwiegenheit über ihnen bekannt werdende Erkenntnisse, die nicht verwertet werden dürfen, verpflichtet (BVerfG, a. a. O, Rn. 224). Nach Absatz 4 Satz 7 ist die gerichtliche Entscheidung unverzüglich nachzuholen.

Absatz 4 Satz 8 legt fest, dass eine Wohnraumüberwachung, die nach Absatz 4 Satz 1 unterbrochen wurde, unter den Voraussetzungen des Absatzes 2 Satz 1 fortgeführt werden darf.

Absatz 5 regelt den Kernbereichsschutz in der Durchführungs- bzw. Auswertungsphase beim Einsatz besonderer Mittel nach § 28 POG und bei der Telekommunikationsüberwachung gemäß § 31 POG. Wie bei der Wohnraumüberwachung ist die unmittelbare Kenntnisnahme einer Maßnahme nach § 28 Abs. 2 Nr. 1 bis 3 und Nr. 6 POG und § 31 POG zu unterbrechen, wenn sich unerwartet tatsächliche Anhaltspunkte ergeben, dass Inhalte aus dem Kernbereich privater Lebensgestaltung erfasst werden. Bestehen insoweit Zweifel, darf nur eine automatische Aufzeichnung fortgesetzt werden.

Das Bundesverfassungsgericht hat dargelegt, dass der Gesetzgeber nicht in jedem Fall eine Sichtung der Daten durch eine unabhängige Stelle vorsehen muss. Je verlässlicher schon auf der ersten Stufe die Erfassung kernbereichsrelevanter Inhalte vermieden wird, umso eher könne auf der Stufe der Auswertung und Verwertung auf die Sichtung durch eine unabhängige Stelle verzichtet werden (BVerfG, a. a. O, Rn. 241). Die Regelung zum Kernbereichsschutz auf der Erhebungsebene in Absatz 3 entspricht vergleichbaren Vorgaben im Bundeskriminalamtgesetz, die das Bundesverfassungsgericht nicht beanstandet hat. Die Erfassung kernbereichsrelevanter Inhalte wird daher bereits auf der Erhebungsebene hinreichend verlässlich ausgeschlossen. Aus diesem Grund ist es zulässig, dass eine Sichtung der erhobenen Daten durch das Oberverwaltungsgericht Rheinland-Pfalz nach Absatz 5 Satz 2 nur für automatische Aufzeichnungen in Zweifelsfällen vorgesehen ist. In diesen Fällen entscheidet das Gericht, ob die Daten verwertet werden können oder zu löschen sind.

Absatz 5 Satz 3 verweist auf Absatz 4 Satz 4 bis 7. Daraus folgt, dass die Behördenleitung oder ein von ihr besonders beauftragter Beamter mit der Befähigung für das vierte Einstiegsamt bei Gefahr in Verzug anstelle des Gerichts über die Verwertbarkeit der Inhalte automatischer Aufzeichnungen in Zweifelsfällen entscheiden kann und die gerichtliche Entscheidung unverzüglich nachholen muss.

Absatz 5 Satz 4 regelt den Kernbereichsschutz während der Durchführungsphase in den Fällen, in denen gem. § 28 Abs. 2 Nr. 4 und 5 POG verdeckte Ermittler oder Vertrauenspersonen zum Einsatz kommen. Ergeben sich während der Durchführung der Maßnahmen tatsächliche Anhaltspunkte dafür, dass kernbereichsrelevante Inhalte erfasst werden, ist die Maßnahme zu unterbrechen, sobald dies ohne Gefährdung des verdeckten Ermittlers oder der Vertrauensperson möglich ist.

Absatz 5 Satz 5 regelt, dass eine unterbrochene Maßnahme fortgeführt werden darf, wenn die Voraussetzungen des Absatzes 3 Satz 1 vorliegen.

Absatz 6 enthält Vorgaben zum Kernbereichsschutz auf der Auswertungsebene bei der Online-Durchsuchung gemäß § 31 c POG. Das Bundesverfassungsgericht hat darauf hingewiesen, dass der Zugriff auf ein informationstechnisches System typischerweise die Gefahr einer Erfassung auch höchstvertraulicher Daten in sich trägt, da der Zugriff mittels eines Ausforschungsprogramms erfolgt, das auf alle Daten zugreift, ohne dass kernbereichsrelevante Daten vor oder bei der Datenerhebung ausgesondert werden können (BVerfG, a. a. O, Rn. 218). Der Schwerpunkt des Kernbereichsschutzes liege daher auf der Aus- und Verwertungsebene. Entscheidende Bedeutung komme dabei einer Sichtung der Daten durch eine unabhängige Stelle zu, die kernbereichsrelevante Informationen vor ihrer Kenntnisnahme und Nutzung durch die Polizei herausfiltert (BVerfG, a. a. O, Rn. 220). In Umsetzung dieser Vorgabe legt Absatz 6 Satz 1 fest, dass alle Erkenntnisse, die durch eine Online-Durchsuchung erlangt worden sind, unverzüglich dem Oberverwaltungsgericht Rheinland-Pfalz zur Entscheidung über die Verwertbarkeit oder Löschung vorzulegen sind. Absatz 6 Satz 2 verweist auf Absatz 4 Satz 4 bis 7 und trifft damit die notwendigen Regelungen, um der Polizei bei Gefahr im Verzug noch vor einer gerichtlichen Entscheidung kurzfristige Handlungsmöglichkeiten einzuräumen.

Zu Nummer 18 (§ 41 b)

Die neu aufgenommene Regelung dient der Umsetzung der Vorgaben aus dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 im Hinblick auf die Gewährleistung einer wirksamen aufsichtlichen Kontrolle. Angesichts des schwach ausgestalteten Individualrechtsschutzes bei verdeckten Überwachungsmaßnahmen kommt der regelmäßigen Durchführung datenschutzaufsichtlicher Kontrollen nach Auffassung des Gerichts eine besondere Bedeutung zu. Entsprechende Kontrollen seien in angemessenen Abständen – deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten dürfe – durchzuführen (BVerfG, aaO, Rn. 141). Dementsprechend ist in § 41 b POG vorgesehen, dass der Landesbeauftragte für den Datenschutz und die Informationsfreiheit mindestens alle zwei Jahre Kontrollen bezüglich der Datenerhebungen nach den §§ 27 b, 28, 29, 31, 31 b, 31 c, 31 e und 38 durchführt.

Zu Nummer 19 (§ 99 a)

Mit der neuen Regelung wird ein Ordnungswidrigkeitentatbestand für vorsätzliche oder fahrlässige Verstöße gegen bestimmte vollziehbare Anordnungen eingeführt. Erfasst werden Verstöße gegen eine Meldeauflage gemäß § 12 a POG, ein Platzverweis gemäß § 13 Abs. 1 POG, eine Wohnungsverweisung gemäß § 13 Abs. 2 POG, ein Aufenthaltsverbot gemäß § 13 Abs. 3 Satz 1 Nr. 1 POG, ein Rückkehrverbot gemäß § 13 Abs. 4 Nr. 1 POG oder ein Annäherungsverbot gemäß § 13 Abs. 4 Nr. 3 POG. Ziel der Regelung ist es, entsprechenden Anordnungen durch eine Bußgeldbewehrung mehr Nachdruck zu verleihen. Da sich aus der Missachtung dieser Anordnungen erhebliche Nachteile für wichtige Gemeinschaftsinteressen ergeben, besteht die Notwendigkeit für die Schaffung einer entsprechenden Bußgeldbestimmung.

Zwar enthält § 37 Abs. 1 Nr. 3 des Brand- und Katastrophenschutzgesetzes (LBKG) vom 2. November 1981 (GVBl. S. 247), zuletzt geändert durch Gesetz vom 8. März 2016 (GVBl. S. 173), BS 2013-50, einen Ordnungswidrigkeitentatbestand für die Fälle, in denen eine Person vorsätzlich oder leichtfertig entgegen § 29 LBKG Rettungseinsätze behindert oder den Anweisungen des Einsatzleiters, der Polizei, der Feuerwehrangehörigen oder der Helfer der anderen Hilfsorganisationen nicht nachkommt. Der neu geschaffene Ordnungswidrigkeitentatbestand im Polizei- und Ordnungsbehördengesetz geht hierüber jedoch hinaus, da er nicht auf Anordnungen im Rahmen von Rettungseinsätzen beschränkt ist, sondern generell vollziehbare Platzverweise, Aufenthaltsverbote, Wohnungsverweisungen und Näherungsverbote erfasst. Soweit im Einzelfall die Tatbestandsvoraussetzungen des § 37 Abs. 1 Nr. 3 LBKG erfüllt sind, geht dieser Ordnungswidrigkeitentatbestand als lex specialis der Regelung in § 13 a POG vor. Dementsprechend wird in Absatz 1 Satz 2 darauf hingewiesen, dass § 37 LBKG unberührt bleibt.

Nach Absatz 2 kann die Ordnungswidrigkeit mit einer Geldbuße bis zu 5 000 Euro geahndet werden.

Absatz 3 legt fest, welche Behörde zur Verfolgung und Ahndung der Ordnungswidrigkeit zuständig ist.

Zu Nummer 20

Die Vorgabe verweist darauf, dass die Inhaltsübersicht entsprechend den vorstehenden Bestimmungen zu ändern ist.

Zu Artikel 2

Mit der Regelung wird dem in Artikel 19 Abs. 1 Satz 2 des Grundgesetzes enthaltenen Zitiergebot Rechnung getragen.

Zu Artikel 3

Die Vorschrift regelt das Inkrafttreten des Gesetzes.

Für die Fraktion der SPD:
Martin Haller

Für die Fraktion der FDP:
Marco Weber

Für die Fraktion BÜNDNIS 90/DIE GRÜNEN
Pia Schellhammer