LANDTAG RHEINLAND-PFALZ
15. Wahlperiode

Drucksache 15/4879
18. 08. 2010

Gesetzentwurf

der Landesregierung

…tes Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes

A. Problem und Regelungsbedürfnis

Die Landesregierung verfolgt mit diesem Gesetzentwurf das Ziel, ein modernes und effizientes Polizei- und Ordnungsbehördengesetz zu schaffen, um die Sicherheit der Bürgerinnen und Bürger weiterhin gewährleisten zu können. Im Einklang mit der Verfassung und der aktuellen Verfassungsrechtsprechung werden unter Berücksichtigung der rechtsstaatlichen Grundsätze vor allem die erforderlichen polizeilichen Befugnisse geschaffen oder bestehende Ermächtigungen angepasst, um technische Entwicklungen zur Gefahrenabwehr und vorbeugenden Verbrechensbekämpfung berücksichtigen zu können.

Der Gesetzentwurf setzt zudem Folgerungen aus aktuellen Entscheidungen des Bundesverfassungsgerichts zum Gefahrenabwehrrecht um.

Weiterhin werden Entwicklungen in der Gesetzgebung und des Datenschutzes beachtet.

B. Lösung

Mit den beabsichtigten Änderungen nimmt das Polizei- und Ordnungsbehördengesetz moderne technische Entwicklungen auf und entspricht den verfassungsrechtlichen Anforderungen.

C. Alternativen

Keine.

D. Kosten

Die Kosten, die durch den Gesetzentwurf für den Haushalt des Landes verursacht werden, können derzeit nicht genau beziffert werden. Dies betrifft insbesondere die Ausgaben zur Telekommunikationsüberwachung und Online-Durchsuchung. Im Hinblick auf die erforderlichen Ausgaben zur Durchführung solcher Maßnahmen ist zu berücksichtigen, dass die Telekommunikationsüberwachung in Rheinland-Pfalz insgesamt neu gestaltet werden soll. Deshalb wurden im Doppelhaushalt 2009/2010 beim Landeskriminalamt Ausgaben für die Informations- und Kommunikationstechnik mit einem jährlichen Haushaltsvolumen von jeweils 4,3 Millionen EUR etatisiert.

Des Weiteren können die gestiegenen Anforderungen zum Schutz des unantastbaren Kernbereichs privater Lebensgestaltung höhere Personalkosten verursachen. Bereits derzeit sind entsprechende Schutzanforderungen bei der Durchführung der Wohnraumüberwachung zu beachten. Nach dem Gesetzentwurf soll dieser Kernbereich nunmehr auch bei anderen sehr grundrechtsintensiven Maßnahmen wie der Telekommunikationsüberwachung und der Online-Durchsuchung besonders geschützt

Druck: Landtag Rheinland-Pfalz, 25. August 2010

werden. Die Gesetzesänderung ist bedingt durch die aktuelle Rechtsprechung des Bundesverfassungsgerichts. Zudem wird angenommen, dass solche Maßnahmen aufgrund der restriktiven Anforderungen der Ermächtigungen nur selten angewendet werden.

Ferner kann die Einführung der polizeilichen Ermächtigung zur körperlichen Untersuchung zu Mehrkosten für den Landeshaushalt führen. Diese Kosten werden allerdings auch als gerechtfertigt angesehen, da die Maßnahmen dazu dienen, Gefahren für Leib oder Leben von Personen abzuwehren.

Insgesamt werden die anfallenden Kosten für den Landeshaushalt als angemessen eingeschätzt.

E. Zuständigkeit

Federführend ist das Ministerium des Innern und für Sport.

Der Ministerpräsident des Landes Rheinland-Pfalz
Mainz, den 17. August 2010

An den
Herrn Präsidenten
des Landtags Rheinland-Pfalz

55116 Mainz

Entwurf eines … ten Landesgesetzes zur Änderung des Polizei- und Ordnungsbehördengesetzes

Als Anlage übersende ich Ihnen den von der Landesregierung beschlossenen Gesetzentwurf.

Ich bitte Sie, die Regierungsvorlage dem Landtag zur Beratung und Beschlussfassung vorzulegen.

Federführend ist der Minister des Innern und für Sport.

Kurt Beck

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

Der Landtag Rheinland-Pfalz hat das folgende Gesetz beschlossen:

Artikel 1

Das Polizei- und Ordnungsbehördengesetz in der Fassung vom 10. November 1993 (GVBl. S. 595), zuletzt geändert durch Gesetz vom 25. Juli 2005 (GVBl. S. 320), BS 2012-1, wird wie folgt geändert:

1. § 1 wird wie folgt geändert:
   a) In Absatz 1 Satz 3 werden die Worte „und für die Verfolgung von Straftaten vorzusorgen“ gestrichen.
   b) Nach Absatz 6 wird folgender neue Absatz 7 eingefügt:

      „(7) Die Polizei ist zuständig für die Sicherstellung von Sachen, sofern deren Beschlagnahme zum Zweck des Verfalls oder der Einziehung in einem Strafverfahren aufgehoben worden ist.“
   c) Die bisherigen Absätze 7 und 8 werden Absätze 8 und 9.

2. § 9 a wird wie folgt geändert:
   a) Absatz 3 wird wie folgt geändert:
      aa) Folgende neue Sätze 2 und 3 werden eingefügt:

         „Dies gilt nicht, soweit die Auskunft zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person unerlässlich ist. Eine in § 53 Abs. 1 oder § 53 a Abs. 1 der Strafprozessordnung genannte Person ist auch in den Fällen des Satzes 2 zur Verweigerung der Auskunft berechtigt.“
      bb) Folgender Satz 5 wird angefügt:

         „Auskünfte, die gemäß Satz 2 erlangt wurden, dürfen nur für den dort bezeichneten Zweck verwendet werden.“
   b) In Absatz 4 wird das Wort „Kraftfahrzeuge“ durch die Worte „Fahrzeuge (§ 19 Abs. 1 Nr. 6)“ ersetzt.

3. In § 10 Abs. 2 Satz 4 werden die Worte „von ihm mitgeführten Sachen“ durch die Worte „Sachen, auf die er Zugriff hat,“ ersetzt.

4. § 11 a wird wie folgt geändert:
   a) Absatz 2 wird wie folgt geändert:
      aa) Satz 2 erhält folgende Fassung:

         „§ 81 f Abs. 2 und § 81 g Abs. 2 Satz 2 der Strafprozessordnung gelten entsprechend.“
      bb) Folgender Satz 3 wird angefügt:

         „Die entnommenen Körperzellen sind unverzüglich nach der Durchführung der molekulargenetischen Untersuchung zu vernichten; die gewon-

nenen und gespeicherten DNA-Identifizierungsmuster sind unverzüglich zu löschen, sobald sie zur Identitätsfeststellung nach Absatz 1 nicht mehr benötigt werden."

b) Absatz 3 wird wie folgt geändert:

aa) In Satz 1 werden nach dem Wort „Untersuchungen" die Worte „an dem durch Maßnahmen nach Absatz 1 Satz 1 Nr. 2 erlangten Material" eingefügt.

bb) Satz 3 erhält folgende Fassung:

„§ 21 Abs. 1 Satz 3 gilt entsprechend."

5. In § 12 Abs. 5 werden die Wörter „Gesetz über die Entschädigung von Zeugen und Sachverständigen in der Fassung vom 1. Oktober 1969 (BGBl. I S. 1756), zuletzt geändert durch Artikel 1 Abs. 5 des Gesetzes vom 22. Februar 2002 (BGBl. I S. 981)" durch die Worte „Justizvergütungs- und -entschädigungsgesetz vom 5. Mai 2004 (BGBl. S. 718 –776–), zuletzt geändert durch Artikel 7 Abs. 3 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2449)" ersetzt.

6. Nach § 12 wird folgender § 12 a eingefügt:

„§ 12 a
Meldeauflagen

Die Polizei kann gegenüber einer Person anordnen, sich an bestimmten Tagen zu bestimmten Zeiten bei einer bestimmten Polizeidienststelle zu melden (Meldeauflage), wenn Tatsachen die Annahme rechtfertigen, dass die Person eine Straftat begehen wird und die Meldeauflage zur vorbeugenden Bekämpfung der Straftat erforderlich ist. Die Meldeauflage ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als denselben Zeitraum ist zulässig, sofern die Voraussetzungen der Anordnung weiterhin vorliegen. Die Verlängerung der Maßnahme bedarf der richterlichen Entscheidung. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. § 21 Abs. 1 Satz 3 gilt entsprechend."

7. § 13 wird wie folgt geändert:

a) In Absatz 3 Satz 1 werden die Worte „Die allgemeinen Ordnungsbehörden und die Polizei können" durch die Worte „Die Polizei kann" ersetzt.

b) In Absatz 4 Satz 1 wird nach dem Wort „kann" das Wort „insbesondere" eingefügt und werden die Worte „gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person oder für bedeutende Sach- und Vermögenswerte" durch die Worte „dringenden Gefahr" ersetzt.

8. § 15 Abs. 2 Satz 2 erhält folgende Fassung:

„Das Verfahren richtet sich nach dem Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit vom 17. Dezember 2008 (BGBl. I S. 2586 –2587–), zuletzt geändert durch Artikel 2 des Gesetzes vom 31. Juli 2009 (BGBl. I S. 2512)."

9. Nach § 16 werden folgende §§ 16 a und 16 b eingefügt:

„§ 16 a
Nicht polizeiliche Gewahrsamseinrichtung

Der Gewahrsam nach § 14 kann auch in einer hierfür geeigneten und vom fachlich zuständigen Ministerium bestimmten nicht polizeilichen Einrichtung des Landes vollzogen werden (nicht polizeiliche Gewahrsamseinrichtung). Die nicht polizeiliche Gewahrsamseinrichtung hat die Sicherheit und Ordnung in ihrer Einrichtung, den ordnungsgemäßen Vollzug des Gewahrsams sowie die Rechte der festgehaltenen Person zu gewährleisten.

§ 16 b
Datenerhebung
durch den Einsatz technischer Mittel
in polizeilichen Gewahrsamseinrichtungen

(1) Die Polizei kann in polizeilichen Gewahrsamseinrichtungen personenbezogene Daten durch den offenen Einsatz technischer Mittel zur Bildübertragung erheben, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass diese Maßnahme zum Schutz von Personen erforderlich ist. Der Schutz der Intimsphäre der festgehaltenen Person ist, soweit möglich, zu wahren. Die Datenerhebung ist durch ein optisches oder akustisches Signal anzuzeigen.

(2) Die zur Anordnung einer Maßnahme nach Absatz 1 in Gewahrsamsräumen führenden tatsächlichen Anhaltspunkte sowie Beginn und Ende einer solchen Maßnahme sind zu dokumentieren.

(3) Die Absätze 1 und 2 gelten für nicht polizeiliche Gewahrsamseinrichtungen nach § 16 a entsprechend."

10. § 18 wird wie folgt geändert:

a) In der Überschrift werden nach dem Wort „Durchsuchung" die Worte „und Untersuchung" eingefügt.

b) Absatz 2 wird wie folgt geändert:

aa) In Nummer 5 wird nach dem Wort „genommen" das Wort „oder" durch ein Komma ersetzt.

bb) Der Nummer 6 wird nach dem Wort „verbracht" das Wort „oder" angefügt.

cc) Folgende Nummer 7 wird eingefügt:

„7. zur Verkehrskontrolle einschließlich der Kontrolle der Verkehrstüchtigkeit und zu Verkehrserhebungen angehalten und kontrolliert (§ 36 Abs. 5 der Straßenverkehrs-Ordnung)".

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

„(3) Die Polizei darf zur Abwehr einer Gefahr für Leib oder Leben eine Person körperlich untersuchen. Zu diesem Zweck sind Entnahmen von Blutproben oder andere körperliche Eingriffe, die von einem Arzt nach den Regeln der ärztlichen Kunst zu Untersuchungszwecken vorgenommen werden, ohne Einwilligung des Betroffenen zulässig, wenn kein Nachteil für seine

Gesundheit zu befürchten ist. Die körperliche Untersuchung bedarf der richterlichen Entscheidung. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. § 21 Abs. 1 Satz 3 gilt entsprechend. Bei Gefahr im Verzug darf die Maßnahme durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes angeordnet werden; die richterliche Entscheidung ist unverzüglich nachzuholen. Die bei der Untersuchung erhobenen personenbezogenen Daten dürfen für einen anderen Zweck nur zur Abwehr von schwerwiegenden Gesundheitsgefährdungen oder zur Verfolgung von Straftaten von erheblicher Bedeutung (§ 28 Abs. 3) verwendet werden. Sind die durch die Maßnahme erlangten personenbezogenen Daten nicht mehr erforderlich, sind sie unverzüglich zu löschen."

d) Der bisherige Absatz 3 wird Absatz 4 und wie folgt geändert:

aa) In Halbsatz 1 werden nach dem Wort „durchsucht" die Worte „oder untersucht" eingefügt.

bb) In Halbsatz 2 werden nach dem Wort „Durchsuchung" die Worte „oder Untersuchung" eingefügt.

e) Der bisherige Absatz 4 wird Absatz 5.

11. § 21 Abs. 1 wird wie folgt geändert:

a) In Satz 1 wird das Wort „dürfen" durch das Wort „bedürfen" und werden die Worte „nur durch den Richter angeordnet werden" durch die Worte „der richterlichen Entscheidung" ersetzt.

b) In Satz 3 werden die Worte „über die" durch die Worte „über das Verfahren in Familiensachen und in den" ersetzt.

12. In § 25 Abs. 3 Satz 1 werden die Worte „und Verwahrung" durch die Worte „, Verwahrung, Unbrauchbarmachung und Vernichtung" ersetzt.

13. § 27 wird wie folgt geändert:

a) In Absatz 4 wird die Angabe „Nr. 1 bis 6" durch die Angabe „Nr. 1 bis 7" ersetzt.

b) Absatz 5 wird gestrichen.

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

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

bb) In Satz 2 werden die Worte „, spätestens nach zwei Monaten" gestrichen.

d) Der bisherige Absatz 7 wird Absatz 6.

e) Folgender Absatz 7 wird angefügt:

„(7) Die örtliche Ordnungsbehörde hat eine Datenerhebung nach Absatz 1 spätestens zwei Wochen vor deren Durchführung der Landesordnungsbehörde und dem Landesbeauftragten für den Datenschutz anzuzeigen. Für die Polizei besteht eine entsprechende An-

zeigepflicht gegenüber dem Landesbeauftragten für den Datenschutz bei einer Datenerhebung nach den Absätzen 1 und 3.“

14. § 28 wird wie folgt geändert:

a) Absatz 4 wird gestrichen.

b) Der bisherige Absatz 5 wird Absatz 4 und in Satz 5 wird das Wort „Polizeibehörde“ durch das Wort „Polizeidienststelle“ ersetzt.

c) Die bisherigen Absätze 6 und 7 werden Absätze 5 und 6.

15. § 29 wird wie folgt geändert:

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

„Die Datenerhebung ist nur zulässig unter den in § 39 a Abs. 2 bezeichneten Voraussetzungen.“

b) Absatz 2 Nr. 1 wird wie folgt geändert:

aa) Folgender neue Buchstabe e wird eingefügt:

„e) Verbreitung, Erwerb und Besitz kinderpornografischer Schriften in den Fällen des § 184 b Abs. 3,“.

bb) Die bisherigen Buchstaben e bis l werden Buchstaben f bis m.

c) Die Absätze 3 bis 6 werden gestrichen.

d) Der bisherige Absatz 7 wird Absatz 3 und wie folgt geändert:

aa) In Satz 1 wird das Wort „Anordnung“ durch das Wort „Entscheidung“ ersetzt.

bb) In Satz 2 wird vor dem Wort „schriftlichen“ das Wort „dieser“ durch das Wort „der“ ersetzt.

cc) In Satz 4 werden die Worte „soweit die in den Absätzen 1 und 3 bezeichneten Voraussetzungen“ durch die Worte „sofern die Voraussetzungen der Anordnung weiterhin“ ersetzt.

e) Der bisherige Absatz 8 wird Absatz 4 und wie folgt geändert:

Die Sätze 3 und 4 werden gestrichen.

f) Der bisherige Absatz 9 wird Absatz 5.

g) Der bisherige Absatz 10 wird Absatz 6 und wie folgt geändert:

aa) In Satz 1 werden die Worte „Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat“ durch die Worte „Oberverwaltungsgericht Rheinland-Pfalz“ ersetzt.

bb) Satz 2 erhält folgende Fassung:

„Das Oberverwaltungsgericht entscheidet nach Maßgabe der Verwaltungsgerichtsordnung.“

h) Der bisherige Absatz 11 wird Absatz 7.

i) Der bisherige Absatz 12 wird Absatz 8 und wie folgt geändert:

In Satz 1 wird die Verweisung „Absatz 1 und 11“ durch die Verweisung „den Absätzen 1 und 7“ ersetzt.

16. § 31 wird durch folgende §§ 31 bis 31 e ersetzt:

„§ 31
Datenerhebung durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation, Auskunft über die Telekommunikation

(1) Die Polizei kann personenbezogene Daten durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation sowie durch Auskünfte über die Telekommunikation 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, erheben 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.

Die Datenerhebung ist nur zulässig, soweit sie zwingend erforderlich ist und die Voraussetzungen des § 39 a Abs. 3 vorliegen. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Die Datenerhebung nach Absatz 1 kann sich auf die Inhalte der Telekommunikation und auf Verkehrsdaten beziehen. Die Erhebung von Verkehrsdaten kann sich auch auf Zeiträume vor deren Anordnung erstrecken.

(3) 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, darf die Überwachung und Aufzeichnung der Telekommunikation ohne Wissen des Betroffenen in der Weise erfolgen, dass mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und
2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

§ 31 c Abs. 2 und 4 gilt entsprechend. Im Übrigen bleibt § 31 c unberührt.

(4) Die Datenerhebung bedarf der richterlichen Entscheidung. In der schriftlichen Anordnung sind insbesondere

1. Voraussetzungen und wesentliche Abwägungsgesichtspunkte,

2. die Person, gegen die sich die Datenerhebung richtet, soweit möglich mit Name und Anschrift,
3. Art, Umfang und Dauer der Datenerhebung unter Benennung des Endzeitpunkts,
4. soweit möglich die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist, und
5. im Fall des Absatzes 3 möglichst genau das informationstechnische System, in das zur Datenerhebung eingegriffen werden soll, sowie das technische Mittel

zu bestimmen. Die Maßnahme ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, sofern die Voraussetzungen der Anordnung weiterhin vorliegen.

(5) Zuständiges Gericht im Sinne dieser Vorschrift ist das Oberverwaltungsgericht Rheinland-Pfalz. Das Oberverwaltungsgericht entscheidet nach Maßgabe der Verwaltungsgerichtsordnung. Bei Gefahr im Verzug kann die Maßnahme vorläufig durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes angeordnet werden; die richterliche Entscheidung ist unverzüglich nachzuholen.

(6) Aufgrund der Anordnung hat jeder, der geschäftsmäßig Telekommunikationsdienstleistungen erbringt oder daran mitwirkt, unverzüglich der Polizei die Überwachung oder Aufzeichnung der Telekommunikation zu ermöglichen sowie Auskünfte über Verkehrsdaten zu erteilen. Von der Auskunftspflicht sind auch Verkehrsdaten erfasst, die nach der Anordnung anfallen. Ob und in welchem Umfang dafür Vorkehrungen zu treffen sind, richtet sich nach dem Telekommunikationsgesetz und den auf seiner Grundlage erlassenen Rechtsverordnungen zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen. § 12 Abs. 5 gilt entsprechend.

(7) § 29 Abs. 5 findet entsprechende Anwendung. Soweit sich die Datenerhebung auf die Inhalte der Telekommunikation bezieht, gilt § 29 Abs. 8 entsprechend.

§ 31 a
Identifizierung und Lokalisierung von mobilen Telekommunikationsendgeräten

(1) Die Polizei kann durch den verdeckten Einsatz technischer Mittel spezifische Kennungen, insbesondere die Geräte- und Kartennummer von mobilen Telekommunikationsendgeräten, oder den Standort eines mobilen Telekommunikationsendgeräts ermitteln von

1. den Verantwortlichen nach den §§ 4 und 5 und unter den Voraussetzungen des § 7 von den dort genannten Personen, soweit die Datenerhebung zur Abwehr einer Gefahr für Leib oder Leben erforderlich ist,
2. Personen, bei denen durch Tatsachen begründete Anhaltspunkte die Annahme rechtfertigen, dass sie zukünftig Straftaten von erheblicher Bedeutung begehen (§ 28 Abs. 3) und die Datenerhebung zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist, und
3. Kontakt- und Begleitpersonen (§ 26 Abs. 3 Satz 2), so-

weit die Datenerhebung zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist.

(2) Personenbezogene Daten Dritter dürfen anlässlich einer Maßnahme nach Absatz 1 nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist. Über den Datenabgleich zur Ermittlung der spezifischen Kennung oder des Standorts eines mobilen Telekommunikationsendgeräts hinaus dürfen sie nicht verwendet werden.

(3) Die Datenerhebung nach Absatz 1 bedarf der richterlichen Entscheidung. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. § 21 Abs. 1 Satz 3 und § 31 Abs. 4 Satz 2 bis 4 gelten entsprechend. Bei Gefahr im Verzug kann die Maßnahme durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes angeordnet werden; mit Ausnahme einer Datenerhebung nach Absatz 1 Nr. 1 zur Ermittlung des Aufenthaltsortes einer vermissten, suizidgefährdeten oder sonstigen hilflosen Person ist die richterliche Entscheidung unverzüglich nachzuholen.

(4) Unter den Voraussetzungen des Absatzes 1 hat jeder, der geschäftsmäßig Telekommunikationsdienstleistungen erbringt oder daran mitwirkt, unverzüglich der Polizei Auskunft über spezifische Kennungen, insbesondere die Geräte- und Kartennummer von mobilen Telekommunikationsendgeräten, oder den Standort des mobilen Telekommunikationsendgeräts zu erteilen. Absatz 3 und § 31 Abs. 6 Satz 2 bis 4 gelten entsprechend.

(5) Die erlangten personenbezogenen Daten dürfen für einen anderen Zweck verwendet werden, soweit dies zur Verfolgung von Straftaten von erheblicher Bedeutung (§ 28 Abs. 3), zur Abwehr einer dringenden Gefahr oder zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist. Die Zweckänderung der Daten muss im Einzelfall festgestellt und dokumentiert werden.

§ 31 b
Auskunft über Nutzungsdaten

(1) Die Polizei kann Auskünfte über Nutzungsdaten (§ 15 Abs. 1 des Telemediengesetzes) verlangen 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, 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.

Die Datenerhebung ist nur zulässig, soweit sie zwingend erforderlich ist und die Voraussetzungen des § 39 a Abs. 3 vorliegen. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Die Auskunft kann auch über zukünftige Nutzungsdaten angeordnet werden.

(2) Aufgrund der Anordnung hat jeder, der geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang vermittelt, unverzüglich der Polizei Auskunft über die Nutzungsdaten zu erteilen. § 31 Abs. 4 und 5 gilt entsprechend.

(3) Die Daten sind unverzüglich auf dem von der Polizei bestimmten Weg durch den Verpflichteten nach Absatz 2 Satz 1 zu übermitteln. § 12 Abs. 5 gilt entsprechend.

(4) § 29 Abs. 5 findet entsprechende Anwendung.

§ 31 c
Datenerhebung durch den Einsatz technischer Mittel in informationstechnischen Systemen

(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, 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.

Die Maßnahme ist nur zulässig, soweit die Aufgabenerfüllung nach Satz 1 auf andere Weise nicht möglich erscheint oder wesentlich erschwert wäre und die Voraussetzungen des § 39 a Abs. 3 vorliegen. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) Unter den Voraussetzungen des Absatzes 1 dürfen technische Mittel eingesetzt werden, um zur Vorbereitung einer Maßnahme nach Absatz 1 die erforderlichen Daten, wie insbesondere spezifische Kennungen, sowie den Standort eines informationstechnischen Systems zu ermitteln. Personenbezogene Daten Dritter dürfen dabei nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist.

(4) Bei jedem Einsatz des technischen Mittels sind zu protokollieren:

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach Absatz 1 rechtmäßig durchgeführt worden ist. Sie sind unverzüglich zu löschen, soweit sie für den in Satz 2 genannten Zweck nicht mehr erforderlich sind.

(5) Die Datenerhebung bedarf der richterlichen Entscheidung. In der schriftlichen Anordnung sind insbesondere
1. Voraussetzungen und wesentliche Abwägungsgesichtspunkte,
2. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Name und Anschrift,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunkts und
4. möglichst genau das informationstechnische System, in das zur Datenerhebung eingegriffen werden soll, sowie das technische Mittel

zu bestimmen. Zuständiges Gericht ist das Oberverwaltungsgericht Rheinland-Pfalz. Das Oberverwaltungsgericht entscheidet nach Maßgabe der Verwaltungsgerichtsordnung. Die Maßnahme ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, sofern die Voraussetzungen der Anordnung weiterhin vorliegen.

(6) § 29 Abs. 5 und 8 findet entsprechende Anwendung.

§ 31 d
Unterbrechung oder Verhinderung der Telekommunikation

(1) Die Polizei kann durch den Einsatz technischer Mittel Telekommunikationsverbindungen 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, unterbrechen oder verhindern von
1. den Verantwortlichen nach den §§ 4 und 5 und unter den Voraussetzungen des § 7 von den 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.

Die Maßnahme darf auch durchgeführt werden, wenn Telekommunikationsverbindungen Dritter unvermeidbar unterbrochen oder verhindert werden.

(2) Die Polizei kann unter den Voraussetzungen des Absatzes 1 Telekommunikationsverbindungen auch ohne Kenntnis der Rufnummer oder einer anderen Kennung des betreffenden Anschlusses oder des Endgeräts unterbrechen oder verhindern, sofern anderenfalls die Erreichung des Zwecks der Maßnahme nach Absatz 1 erheblich erschwert wäre.

(3) Die Maßnahme bedarf der richterlichen Entscheidung. In der schriftlichen Anordnung sind insbesondere

1. Voraussetzungen und wesentliche Abwägungsgesichtspunkte,
2. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Name und Anschrift,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunkts,
4. soweit möglich die Rufnummer oder eine andere Kennung des Anschlusses oder des Endgeräts, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist, und
5. im Fall des Absatzes 2 die möglichst genaue räumliche und zeitliche Bezeichnung der Telekommunikationsverbindungen, die unterbrochen oder verhindert werden sollen,

zu bestimmen. Zuständiges Gericht ist das Oberverwaltungsgericht Rheinland-Pfalz. Das Oberverwaltungsgericht entscheidet nach Maßgabe der Verwaltungsgerichtsordnung. Bei Gefahr im Verzug kann die Maßnahme vorläufig durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes angeordnet werden; die richterliche Entscheidung ist unverzüglich nachzuholen. Die Maßnahme ist auf höchstens 24 Stunden zu befristen. Eine Verlängerung um jeweils nicht mehr als denselben Zeitraum ist zulässig, sofern die jeweiligen Voraussetzungen der Anordnung weiterhin vorliegen.

§ 31 e
Funkzellenabfrage

(1) Die Polizei kann unter den Voraussetzungen des § 31 Abs. 1 von jedem, der geschäftsmäßig Telekommunikationsdienstleistungen erbringt oder daran mitwirkt, Auskunft über Verkehrsdaten ohne Kenntnis der Rufnummer oder einer anderen Kennung des zu überwachenden Anschlusses oder des Endgeräts verlangen, sofern anderenfalls die Erreichung des Zwecks der Maßnahme erheblich erschwert wäre.

(2) § 31 Abs. 4 gilt entsprechend mit der Maßgabe, dass abweichend von § 31 Abs. 4 Satz 2 Nr. 4 in der richterlichen Anordnung möglichst genau die Telekommunikation räumlich und zeitlich zu bestimmen ist, über die Verkehrsdaten erhoben werden soll. Im Übrigen gelten § 31 Abs. 5 und 6 Satz 2 bis 4 entsprechend; § 29 Abs. 5 findet entsprechende Anwendung."

17. § 32 wird wie folgt geändert:

a) In Absatz 2 werden die Worte „Kontakt- und Begleitpersonen (§ 26 Abs. 3 Satz 2)" durch die Worte „etwaige Begleiter" ersetzt.

b) Absatz 3 wird wie folgt geändert:

aa) In Satz 2 werden die Worte „und kann wiederholt angeordnet werden" gestrichen.

bb) Nach Satz 2 werden folgende Sätze angefügt:

„Eine Verlängerung der Maßnahme um jeweils nicht mehr als denselben Zeitraum ist zulässig, sofern die Voraussetzungen der Anordnung weiter-

hin vorliegen. Die Verlängerung der Maßnahme bedarf der richterlichen Entscheidung. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. § 21 Abs. 1 Satz 3 gilt entsprechend."

c) Absatz 4 wird gestrichen.

d) Der bisherige Absatz 5 wird Absatz 4 und wie folgt geändert:

Die Angabe „Abs. 6" wird durch die Angabe „Abs. 5" ersetzt.

18. § 33 wird wie folgt geändert:

a) Dem Absatz 6 wird folgender Satz angefügt:

„Werden innerhalb dieser gesetzlichen Fristen weitere personenbezogene Daten über dieselbe Person gespeichert, so gilt für alle Speicherungen einheitlich der Prüfungstermin, der als letzter eintritt, oder die Aufbewahrungsfrist, die als letzte endet."

b) In Absatz 7 Satz 3 wird die Verweisung „§§ 29 und 31" durch die Verweisung „§§ 29, 31 und 31 c" ersetzt.

19. Dem § 34 Abs. 7 wird folgender Satz angefügt:

„Satz 1 gilt für die Polizei entsprechend, soweit von einer Person eine Gefahr für Leib, Leben oder Freiheit anderer Personen ausgeht."

20. In § 37 Abs. 2 Satz 1 werden nach dem Wort „Fahndungsbestand" die Worte „zum Zweck der Gefahrenabwehr" eingefügt.

21. § 38 wird wie folgt geändert:

a) In Absatz 1 werden die Worte „erheblichen Gefahr oder zur vorbeugenden Bekämpfung von besonders schwerwiegenden Straftaten (§ 29 Abs. 2)" durch die Worte „Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person" ersetzt.

b) Absatz 3 erhält folgende Fassung:

„(3) Die Maßnahme bedarf der richterlichen Entscheidung. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. § 21 Abs. 1 Satz 3 gilt entsprechend. Der Landesbeauftragte für den Datenschutz ist unverzüglich zu unterrichten. Bei Gefahr im Verzug kann die Maßnahme vorläufig durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes angeordnet werden; die richterliche Entscheidung ist unverzüglich nachzuholen."

c) In Absatz 4 Satz 1 wird das Wort „schwerwiegender" durch das Wort „schwerer" ersetzt.

22. § 39 wird wie folgt geändert:

a) Absatz 2 wird wie folgt geändert:

aa) In Nummer 3 wird der Schlusspunkt durch ein Komma ersetzt.

bb) Folgende Nummer 4 wird eingefügt:

„4. sie für den der Anordnung ihrer verdeckten Erhebung zugrunde liegenden Zweck nicht mehr erforderlich sind."

cc) Folgende Sätze 2 und 3 werden angefügt:

„Über die Löschung personenbezogener Daten, die verdeckt erhoben wurden, ist eine Niederschrift zu fertigen. Die Löschung von durch Maßnahmen nach den §§ 29, 31, 31 b und 31 c erhobenen personenbezogenen Daten erfolgt unter Aufsicht des behördlichen Datenschutzbeauftragten."

b) Nach Absatz 3 wird folgender Absatz 4 angefügt:

„(4) Die Bestimmungen über die Zweckänderung von personenbezogenen Daten bleiben unberührt."

23. Nach § 39 werden folgende §§ 39 a und 39 b eingefügt:

„§ 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 ist zu dokumentieren.

(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 § 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) Das Oberverwaltungsgericht Rheinland-Pfalz besitzt die Sachleitung über die Auswertung von Daten, die durch Maßnahmen nach den §§ 29, 31, 31 b und 31 c erhoben wurden. Zwei Bedienstete der zuständigen Polizeibehörde, von denen einer die Befähigung zum Richteramt haben muss, und der behördliche Datenschutzbeauftragte haben Daten, die durch Maßnahmen nach den §§ 29 und 31 c erhoben wurden, auf kernbereichsrelevante Inhalte durchzusehen.

(5) Die unmittelbare Kenntnisnahme einer Maßnahme nach den §§ 29, 31 und 31 c ist unverzüglich zu unterbrechen, sofern sich tatsächliche Anhaltspunkte ergeben, dass Inhalte, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erhoben werden. Automatische

Aufzeichnungen hierüber sind unverzüglich dem Oberverwaltungsgericht Rheinland-Pfalz zur Entscheidung über die Verwertbarkeit oder Löschung vorzulegen. Ist die Datenerhebung nach Satz 1 unterbrochen worden, darf sie im Fall des § 29 unter den Voraussetzungen des Absatzes 2 Satz 1 und in den Fällen der §§ 31 und 31 c unter denen des Absatzes 3 Satz 1 fortgeführt werden.

§ 39 b
Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger

(1) Verdeckte Datenerhebungen in einem durch ein Berufsgeheimnis geschützten Vertrauensverhältnis im Sinne des § 53 Abs. 1 und des § 53 a Abs. 1 der Strafprozessordnung sind unzulässig. Dennoch erlangte Daten sind unverzüglich zu löschen. Erkenntnisse hierüber dürfen nicht verwertet werden. Die Tatsache der Datenerhebung ist zu dokumentieren.

(2) Absatz 1 gilt nicht, sofern Tatsachen die Annahme rechtfertigen, dass die zeugnisverweigerungsberechtigte Person für die Gefahr verantwortlich ist.“

24. § 40 Abs. 5 wird wie folgt geändert:

a) In Satz 2 wird die Verweisung „§ 29“ durch die Verweisung „den §§ 29 und 31 c“ ersetzt.

b) In Satz 8 wird das Wort „Polizeibehörde“ durch das Wort „Polizeidienststelle“ ersetzt.

c) Folgender Satz wird angefügt:

„Sind mehrere verdeckte Datenerhebungen in einem zeitlichen und sachlichen Zusammenhang durchgeführt worden, erfolgt die Unterrichtung des Betroffenen nach dieser Bestimmung nach Abschluss der letzten Maßnahme; Entsprechendes gilt für die Berechnung der Frist zur Einholung der richterlichen Zustimmung für jede weitere Zurückstellung der Unterrichtung.“

25. § 41 Abs. 2 Satz 1 Nr. 11 erhält folgende Fassung:

„11. die in § 41 a genannten technischen und organisatorischen Maßnahmen des Datenschutzes sowie“.

26. Nach § 41 wird folgender § 41 a eingefügt:

„§ 41 a
Technische und organisatorische Maßnahmen des Datenschutzes

(1) Die Polizeibehörden und -einrichtungen haben die nach § 9 des Landesdatenschutzgesetzes erforderlichen Maßnahmen zu treffen, um die Ausführung der Bestimmungen dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu gewährleisten. Dabei ist insbesondere sicherzustellen, dass nur befugte Personen auf Verfahren und personenbezogene Daten Zugriff nehmen können (Vertraulichkeit) und personenbezogene Daten unversehrt, zurechenbar und vollständig bleiben (Integrität).

(2) Die nach Absatz 1 zu treffenden technischen und organisatorischen Maßnahmen sind auf der Grundlage einer

Schutzbedarfsfeststellung und einer Risikoanalyse in einem IT-Sicherheits- und Datenschutzkonzept festzulegen und in angemessenen Abständen oder bei Verfahrensänderung auf ihre Eignung zu überprüfen und zu dokumentieren.

(3) Zur Verbesserung des Datenschutzes und der Datensicherheit sollen die Polizeibehörden und -einrichtungen die von ihnen eingesetzten Verfahren zur automatisierten Verarbeitung personenbezogener Daten sowie die dabei genutzten technischen Einrichtungen durch unabhängiges und fachkundiges Personal prüfen und bewerten lassen (IT-Sicherheits- und Datenschutzaudit). Die Prüfergebnisse sowie deren Unterlagen dürfen bei dienstlichem Interesse Dritten in geeigneter Form zugänglich gemacht oder veröffentlicht werden. Verfahren und technische Einrichtungen, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem Verfahren nach Satz 1 geprüft wurde, sollen von den Polizeibehörden und -einrichtungen vorrangig eingesetzt werden.

(4) Verfahren der Polizeibehörden und -einrichtungen zur automatisierten Verarbeitung personenbezogener Daten unterliegen der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Zuständig für die Vorabkontrolle ist der behördliche Datenschutzbeauftragte. Dieser wendet sich in Zweifelsfällen an den Landesbeauftragten für den Datenschutz. Das Ergebnis der Vorabkontrolle ist zu dokumentieren."

27. In § 58 Abs. 5 Satz 1 werden die Worte „der Bundesgrenzschutz" und die Worte „den Bundesgrenzschutz" jeweils durch die Worte „die Bundespolizei" ersetzt.

28. In § 79 Abs. 3 werden nach dem Wort „Straftaten" die Worte „oder die Aufgabe der Gefahrenabwehr" eingefügt.

29. § 86 Abs. 3 erhält folgende Fassung:

„(3) Die Absätze 1 und 2 gelten für Polizeibeamte des Bundes entsprechend. Das Gleiche gilt für Bedienstete ausländischer Polizeidienststellen, wenn völkerrechtliche Vereinbarungen dies vorsehen oder das fachlich zuständige Ministerium Amtshandlungen dieser ausländischen Polizeidienststellen allgemein oder im Einzelfall zustimmt."

30. In § 95 Abs. 3 Halbsatz 1 wird das Wort „Hilfsbeamte" durch das Wort „Ermittlungspersonen" ersetzt.

31. § 100 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) Satz 1 erhält folgende Fassung:

„Die Landesregierung berichtet dem Landtag über die Wirksamkeit der Maßnahmen nach den §§ 29, 31, 31 b, 31 c, 31 e und 38 in der Zeit vom … *(ersten Tag des zweiten auf die Verkündung folgenden Kalendermonats einsetzen)* bis zum Ablauf des … *(letzten Tag des ersten auf die Verkündung folgenden Kalendermonats zuzüglich fünf Jahre einsetzen).*"

bb) In Satz 2 wird die Verweisung „§ 29 Abs. 7“ durch die Verweisung „§ 29 Abs. 8“ ersetzt.

b) Nach Absatz 1 wird folgender neue Absatz 2 eingefügt:

„(2) Die Anfertigung des Berichts der Landesregierung erfolgt unter Mitwirkung einer Stelle, die eine wissenschaftlich fundierte Überprüfung der Maßnahmen gewährleistet.“

c) Der bisherige Absatz 2 wird Absatz 3.

32. Die Inhaltsübersicht wird entsprechend den vorstehenden Bestimmungen geändert.

Artikel 2

Die Grundrechte auf körperliche Unversehrtheit (Artikel 2 Abs. 2 Satz 1 des Grundgesetzes), Wahrung des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes), Freizügigkeit (Artikel 11 des Grundgesetzes) und Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) werden nach Maßgabe dieses Gesetzes eingeschränkt.

Artikel 3

Dieses Gesetz tritt am Tage nach der Verkündung in Kraft.

Begründung

A. Allgemeines

Zentrale Aufgabe der allgemeinen Ordnungsbehörden und der Polizei ist es, die Sicherheit der Bürgerinnen und Bürger in Rheinland-Pfalz zu gewährleisten. Für den Gesetzgeber folgt daraus die laufende Verpflichtung, gesetzliche Instrumentarien zu schaffen, die zum einen im Einklang mit der Verfassung stehen und zum anderen in tatsächlicher Hinsicht zur Erfüllung des gesetzlichen Auftrages ausreichend und geeignet sind.

Die Notwendigkeit zur erneuten Novellierung des Polizei- und Ordnungsbehördengesetzes (POG) in der Fassung vom 10. November 1993 (GVBl. S. 595), zuletzt geändert durch Gesetz vom 25. Juli 2005 (GVBl. S. 320), BS 2012-1, ergibt sich aufgrund technischer Fortschritte, die der Polizei neue Möglichkeiten zur Optimierung ihrer Tätigkeit eröffnen. Dies gilt insbesondere im Hinblick auf die Abwehr von Gefahren durch terroristische Vereinigungen oder der organisierten Kriminalität. Diese Gruppen nutzen im hohen Maß für ihre Zwecke die Möglichkeiten der neuen Informations- und Kommunikationstechnik. Ihre Netzwerke sind geprägt durch weltweite Verknüpfungen und hohe Konspirativität. Herkömmliche kriminalpolizeiliche Ermittlungsmethoden sind nicht mehr ausreichend, um diesen Entwicklungen wirksam begegnen zu können. Vor diesem Hintergrund sollen die polizeilichen Befugnisse dem technischen Fortschritt angepasst werden. Die Polizei soll unter engen rechtsstaatlichen Voraussetzungen zum verdeckten Zugriff auf informationstechnische Systeme (sogenannte Online-Durchsuchung) und zur Unterbrechung und Verhinderung der Telekommunikation ermächtigt werden. Zudem sollen die Befugnis zur Telekommunikationsüberwachung differenzierter ausgestaltet und technische Entwicklungen berücksichtigt werden.

Die Gesetzesänderungen sind auch nicht im Hinblick auf das Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008 (BGBl. I S. 3083) entbehrlich. Durch dieses Gesetz hat das Bundeskriminalamt (BKA) zwar erstmals präventive Befugnisse im Kampf gegen den internationalen Terrorismus erhalten. Die Befugnisse der Länder zur Gefahrenabwehr bleiben jedoch gemäß § 4 a Abs. 2 Satz 1 des Bundeskriminalamtgesetzes (BKAG) vom 7. Juli 1997 (BGBl. I S. 1650), zuletzt geändert durch Artikel 2 des Gesetzes vom 6. Juni 2009 (BGBl. I S. 1226), davon unberührt. Die neuen Befugnisse des BKA treten also zu denen der Länder hinzu, sodass eine Doppelzuständigkeit in diesem Aufgabenbereich entstanden ist.

Die Notwendigkeit zur Gesetzesänderung ergibt sich ferner aus aktuellen Entscheidungen des Bundesverfassungsgerichts zum Gefahrenabwehrrecht, die rechtliche Konsequenzen für das rheinland-pfälzische Polizei- und Ordnungsbehördengesetz haben. So wird die polizeiliche Ermächtigung zur Rasterfahndung unter Beachtung verfassungsrechtlicher Vorgaben restriktiver gefasst. Die Befugnisnorm zum automatisierten Kfz-Kennzeichenabgleich, die den Vorgaben des Bundesverfassungsgerichts nicht entspricht, wird aufgehoben. Ferner wird in Umsetzung der Verfassungsrechtsprechung der Schutz des unantastbaren Kernbereichs privater Lebensgestaltung verbessert. Der Schutz der zeugnisverweigerungsberechtigten Berufsgeheimnisträgerinnen und Berufsgeheimnisträger bei Durchführung verdeckter Maßnahmen wird einheitlich geregelt.

Daneben werden die Belange des Datenschutzes durch materielle und verfahrensrechtliche Bestimmungen noch stärker als bislang berücksichtigt.

Zudem sollen durch diese Novelle die polizeilichen Befugnisse zur Gefahrenabwehr nochmals ergänzt und an Rechtsentwicklungen und aktuelle Gesetzesänderungen angepasst werden. Neben redaktionellen Änderungen sieht der Gesetzentwurf deshalb folgende wesentliche Änderungen und Ergänzungen des Polizei- und Ordnungsbehördengesetzes vor:

1. Die polizeiliche Aufgabe, für die Verfolgung von Straftaten vorzusorgen, wird aufgehoben (§ 1 Abs. 1 Satz 3 POG).
2. Die ausschließliche Zuständigkeit der Polizei für die Sicherstellung von Sachen, sofern deren Beschlagnahme zum Zweck der Vermögensabschöpfung in einem Strafverfahren aufgehoben worden sind, wird begründet (§ 1 Abs. 7 POG).
3. Das bisherige Recht zur Verweigerung der Auskunft wird eingeschränkt. Die Einschränkung gilt nicht für zeugnisverweigerungsberechtigte Berufsgeheimnisträgerinnen und Berufsgeheimnisträger nach § 53 Abs. 1 und § 53 a Abs. 1 der Strafprozessordnung – StPO – (§ 9 a Abs. 3 POG).
4. Die Regelung zur molekulargenetischen Untersuchung wird an die geänderten Bestimmungen der Strafprozessordnung angepasst (§ 11 a POG).
5. Die Polizei wird ausdrücklich zum Erlass von Meldeauflagen zur vorbeugenden Bekämpfung von Straftaten befugt (§ 12 a POG).
6. Die Befugnis zur Anordnung eines Aufenthaltsverbots wird ausschließlich der Polizei zugewiesen (§ 13 Abs. 3 Satz 1 POG).
7. Die Begrenzung des Anwendungsbereichs der Aufenthalts-, Kontakt- und Näherungsverbote auf Fälle der Gewalt in engen sozialen Beziehungen wird aufgehoben und die Gefahrenschwelle wird auf eine dringende Gefahr herabgesenkt (§ 13 Abs. 4 Satz 1 POG).
8. Die Zulässigkeit der Durchführung des polizeilichen Gewahrsams in sonstigen Einrichtungen des Landes wird geregelt (§ 16 a POG).
9. Die Polizei wird zur Datenerhebung durch den offenen Einsatz technischer Mittel zur Bildübertragung in polizeilichen Gewahrsamseinrichtungen ermächtigt (§ 16 b POG).
10. Die Eigensicherung der Polizeibeamtinnen und Polizeibeamten wird verbessert (§ 18 Abs. 2 und § 27 Abs. 4 POG).

11. Die polizeiliche Befugnis zur körperlichen Untersuchung einer Person zur Abwehr einer Gefahr für Leib oder Leben wird eingeführt (§ 18 Abs. 3 POG).

12. Es erfolgt die Klarstellung, dass die polizeirechtlich verantwortliche Person auch die Kosten der Vernichtung oder Unbrauchbarmachung einer sichergestellten Sache zu tragen hat (§ 25 Abs. 3 Satz 1 POG).

13. Bei Datenerhebungen durch den Einsatz technischer Mittel wird die bisherige zeitliche Begrenzung der Löschungsverpflichtung gestrichen. Ferner wird eine Anzeigepflicht der örtlichen Ordnungsbehörden gegenüber der Landesordnungsbehörde und der oder dem Landesbeauftragten für den Datenschutz eingeführt. Eine entsprechende Anzeigepflicht gegenüber der oder dem Landesbeauftragten für den Datenschutz gilt für die Polizei bei Datenerhebungen nach den Absätzen 1 und 3 (§ 27 Abs. 5 Satz 2 und Abs. 7 POG).

14. Die Ermächtigung zum automatisierten Kennzeichenabgleich in § 27 Abs. 5 POG wird aufgehoben.

15. Die Zuständigkeit der Amtsgerichte wird einheitlich geregelt. Während sich die Zuständigkeit der Amtsgerichte bislang in vielen Fällen entweder nach dem Sitz der Polizeidienststelle oder dem Sitz der Polizeibehörde richtet, soll künftig grundsätzlich das Amtsgericht zuständig sein, in dessen Bezirk die Polizeidienststelle ihren Sitz hat (§ 28 Abs. 4 Satz 5 und § 40 Abs. 5 Satz 8 POG).

16. Für die Entscheidung über die Anordnung verdeckter Ermittlungsmaßnahmen nach den §§ 29, 31, 31 b, 31 c, 31 d und 31 e POG tritt an die Stelle der bisherigen Zuständigkeit des Amtsgerichts die Zuständigkeit des Oberverwaltungsgerichts Rheinland-Pfalz (§ 29 Abs. 6 Satz 1, § 31 Abs. 5 Satz 1, § 31 b Abs. 2 Satz 2, § 31 c Abs. 5 Satz 3, § 31 d Abs. 3 Satz 3 und § 31 e Abs. 2 Satz 2 POG).

17. Die bisherige Befugnis zur Telekommunikationsüberwachung wird unter Beachtung der Verfassungsrechtsprechung und technischer Entwicklungen neu und differenzierter gefasst. Insbesondere wird eine bereichsspezifische Ermächtigung zur Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten eingeführt. Im Einzelnen sei auf folgende Änderungen besonders hingewiesen:

    – Die Befugnis zur Telekommunikationsüberwachung wird um die Tatbestandsalternative „zur Abwehr einer gegenwärtigen Gefahr für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt“ ergänzt. Weiterhin wird der Kreis der Verantwortlichen um den „Nachrichtenmittler“ erweitert (§ 31 Abs. 1 POG).

    – Ausdrücklich wird die polizeiliche Befugnis zum verdeckten, technischen Zugriff auf ein informationstechnisches System zum Zweck der Telekommunikationsüberwachung (sogenannte Quellen-Telekommunikationsüberwachung) aufgenommen (§ 31 Abs. 3 POG).

    – Die Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten werden in einer eigenen Ermächtigung unter erleichterten Voraussetzungen zugelassen (§ 31 a POG).

18. Die Polizei wird zur Erlangung von Auskünften über Nutzungsdaten nach § 15 Abs. 1 des Telemediengesetzes (TMG) vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Gesetz vom 31. Mai 2010 (BGBl. I S. 692), befugt (§ 31 b POG).

19. Die Polizei erhält die Befugnis zum verdeckten Zugriff auf informationstechnische Systeme, um personenbezogene Daten zu erheben (§ 31 c POG).

20. Die Polizei wird zur Unterbrechung oder Verhinderung der Telekommunikation befugt (§ 31 d POG).

21. Die Funkzellenabfrage wird ausdrücklich geregelt (§ 31 e POG).

22. Bei polizeilichen Beobachtungen erhält die Polizei die Befugnis zur Übermittlung von Erkenntnissen über Begleitpersonen (§ 32 Abs. 2 POG).

23. Die Anordnung der Verlängerung einer polizeilichen Beobachtung nach Ablauf von zwölf Monaten wird unter Richtervorbehalt gestellt (§ 32 Abs. 3 Satz 4 POG).

24. Bei Mehrfachspeicherungen von personenbezogenen Daten werden einheitliche Prüfungstermine und Aufbewahrungsfristen festgelegt (§ 33 Abs. 6 Satz 2 POG).

25. Die Öffentlichkeitsfahndung zum Zwecke der Ermittlung der Identität oder des Aufenthaltsortes wird auch in den Fällen zugelassen, in denen von einer Person eine Gefahr für Leib, Leben oder Freiheit anderer Personen ausgeht (§ 34 Abs. 7 Satz 2 POG).

26. Es erfolgt die gesetzliche Klarstellung, dass ein Datenabgleich mit dem Fahndungsbestand nur zum Zweck der Gefahrenabwehr zulässig ist (§ 37 Abs. 2 Satz 1 POG).

27. Die Rasterfahndung wird nur zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person zugelassen und unter Richtervorbehalt gestellt (§ 38 POG).

28. Eine bereichsspezifische Verpflichtung zur Löschung von durch verdeckte Datenerhebungen gewonnenen Daten wird aufgenommen. Ferner werden allgemeine Verfahrensanforderungen für die Löschung solcher Daten festgelegt (§ 39 Abs. 2 POG).

29. Der Schutz des unantastbaren Kernbereichs privater Lebensgestaltung bei verdeckten Maßnahmen wird in einer eigenen Norm geregelt und näher ausgestaltet. Besondere Anforderungen gelten bei Durchführung von besonders grundrechtsintensiven Maßnahmen (§ 39 a POG).

30. Der Schutz der zeugnisverweigerungsberechtigten Berufsgeheimnisträgerinnen und Berufsgeheimnisträger bei verdeckten Maßnahmen wird einheitlich in einer eigenen Norm geregelt (§ 39 b POG).

31. Die Verpflichtung, sonstige betroffene Personen von einer verdeckten Datenerhebung zu unterrichten, wird um den Tatbestand des verdeckten Zugriffs auf informationstechnische Systeme ergänzt (§ 40 Abs. 5 Satz 2 POG).

32. Die Unterrichtung betroffener Personen bei Durchführung mehrerer verdeckter Maßnahmen wird neu geregelt (§ 40 Abs. 5 Satz 9 POG).

33. Die Gewährleistung der Datensicherheit bei der polizeilichen Datenverarbeitung wird bereichsspezifisch geregelt (§ 41 a POG).

34. Die Zuständigkeit des Landeskriminalamtes wird um die Fälle der Gefahrenabwehr erweitert (§ 79 Abs. 3 POG).

35. Die Zulässigkeit von Amtshandlungen der Bediensteten ausländischer Polizeidienststellen wird erweitert (§ 86 Abs. 3 POG).

36. Die Ermächtigungen zur Wohnraumüberwachung gemäß § 29 POG, zur Telekommunikationsüberwachung gemäß § 31 POG, zur Auskunft über Nutzungsdaten gemäß § 31 b POG, zur Online-Durchsuchung gemäß § 31 c POG, zur Funkzellenabfrage gemäß § 31 e POG und zur Rasterfahndung gemäß § 38 POG sollen evaluiert werden (§ 100 Abs. 1 Satz 1 POG).

37. Die Anfertigung des Evaluationsberichts erfolgt unter Mitwirkung einer Stelle, die eine wissenschaftlich fundierte Überprüfung der Maßnahmen gewährleistet (§ 100 Abs. 2 POG).

Es bedurfte keiner Gesetzesfolgenabschätzung, die über die bei allen Gesetzentwürfen erfolgende Prüfung der Notwendigkeit der Maßnahmen und ihrer Auswirkungen hinausgeht. Es handelt sich nicht um ein Gesetzesvorhaben mit großer Wirkungsbreite oder erheblichen Auswirkungen. Zum einen werden durch den Gesetzentwurf polizeiliche Befugnisse aufgrund der aktuellen Verfassungsrechtsprechung eingeschränkt. Zum anderen werden bereits bestehende Ermächtigungen, die sich in der Praxis im Grundsatz bewährt haben, wegen technischer Entwicklungen geändert oder ergänzt, sodass sich folglich weder die Frage nach der Notwendigkeit der Regelung als solcher noch nach Regelungsalternativen stellt. Die neu geschaffenen Befugnisse werden voraussichtlich aufgrund der hohen rechtsstaatlichen Anforderungen nur selten bei besonderen Gefahrenlagen angewendet werden. Eine große Wirkungsbreite oder erhebliche Auswirkungen werden ihnen somit in der tatsächlichen Lebenswirklichkeit nicht zukommen.

Das Konnexitätsprinzip gemäß § 1 des Konnexitätsausführungsgesetzes vom 2. März 2006 (GVBl. S. 53, BS 2020-5) wird durch diesen Gesetzentwurf nicht berührt.

Unterschiedliche Auswirkungen auf die spezifische Lebenssituation von Frauen und Männer sind durch dieses Landesgesetz nicht zu erwarten.

Die Verwendung einer geschlechtsgerechten Rechtssprache im Polizei- und Ordnungsbehördengesetz bleibt einem Neuerlass des Gesetzes vorbehalten.

B. Zu den einzelnen Bestimmungen

Zu Artikel 1

Zu Nummer 1 (§ 1)

Zu Buchstabe a

In Absatz 1 Satz 3 wird die „Vorsorge für die Verfolgung von Straftaten“ aus dem Aufgabenbereich der Polizei gestrichen. Damit wird dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 (1 BvR 668/04) zur polizeilichen Telekommunikationsüberwachung nach den Bestimmungen des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (Nds. SOG) Rechnung getragen. Das Bundesverfassungsgericht hat in dem Urteil die polizeiliche Befugnis zur Durchführung von Telekommunikationsüberwachungen zum Zweck der Vorsorge für die Verfolgung von Straftaten wegen fehlender Gesetzgebungskompetenz für nichtig erklärt. Danach gehört die Vorsorge für die Verfolgung noch nicht begangener, sondern in ungewisser Zukunft bevorstehender Straftaten zum gerichtlichen Verfahren (BVerfG, a. a. O., Absatz Nr. 97) und somit gemäß Artikel 74 Abs. 1 Nr. 1 des Grundgesetzes zur konkurrierenden Gesetzgebung. Eine solche Verfolgungsvorsorge hat der Bundesgesetzgeber abschließend in der Strafprozessordnung geregelt. Damit fehlt dem Landesgesetzgeber die Regelungskompetenz für diesen Aufgabenbereich.

Durch die Streichung dieser Regelung entstehen keine praktischen Auswirkungen für die Polizeiarbeit, da bis auf die begriffliche Aufgabenbestimmung für die Polizei in § 1 POG der Landesgesetzgeber der Polizei ausdrücklich keine Aufgabe zur „Vorsorge für die Verfolgung von Straftaten“ zugewiesen hat. Zwar wird dieser Begriff in der Bestimmung zur Zuständigkeit des Landeskriminalamtes gemäß § 79 POG verwendet. Diese Norm stellt jedoch eine polizeiliche Zuständigkeitsregelung und keine originäre Aufgabenzuweisung an die Polizei dar. Von der Streichung unberührt bleibt die Aufgabe der Polizei, im Rahmen der Gefahrenabwehr auch weiterhin Straftaten zu verhüten. Hierzu hat das Bundesverfassungsgericht in dem Urteil ausgeführt, dass die Verhütung einer Straftat in der Gesetzgebungskompetenz der Länder liegt, und zwar auch dann, wenn sie vorbeugend für den Zeitraum vor dem Beginn einer konkreten Straftat vorgesehen wird. Das Tatbestandsmerkmal der Verhütung von Straftaten erfasst Maßnahmen, die drohende Rechtsgutverletzungen von vornherein und in einem Stadium verhindern sollen, in dem es noch nicht zu strafwürdigem Unrecht gekommen ist (BVerfG, a. a. O., Absatz Nr. 94 und Absatz Nr. 96).

Zu Buchstabe b

Der neu eingefügte Absatz 7 begründet die ausschließliche Zuständigkeit der Polizei zur Sicherstellung einer Sache, sofern deren Beschlagnahme zum Zweck der Vermögensabschöpfung in einem Strafverfahren aufgehoben worden ist. In den letzten Jahren hat die Vermögensabschöpfung im Strafverfahren eine immer größere Bedeutung erlangt. Die Instrumente der Vermögensabschöpfung sind jedoch an enge gesetzliche Anforderungen gebunden, die im Verfahren nicht immer nachgewiesen werden können. Ist ein solcher Nachweis nicht möglich, kann unter bestimmten Voraussetzungen die Sicherstellung der Sache zum Zweck der Gefahrenabwehr in Betracht kommen. Um diese Möglichkeiten zu verbessern und das Verfahren einer solchen Sicherstellung effizienter zu gestalten, wird eine ausschließliche polizeiliche Zuständigkeit für solche Sicherstellungen festgelegt, deren Beschlagnahme zum Zweck der Vermögensabschöpfung in einem Strafverfahren aufgehoben worden ist.

Die Instrumente der Vermögensabschöpfung im Strafverfahren sind der Verfall gemäß § 73, die Einziehung gemäß § 74 und der erweiterte Verfall gemäß § 73 d des Strafgesetzbuchs (StGB).

Zur Sicherstellung von Verfalls- und Einziehungsgegenständen wird gemäß § 111 b Abs. 1 StPO die Beschlagnahme angeordnet, wenn Gründe für die Annahme vorhanden sind,

dass die Voraussetzungen für ihren Verfall oder ihre Einziehung vorliegen. Wird im Verfahren festgestellt, dass die Sache keiner konkreten rechtswidrigen Tat zugeordnet werden kann, sind die Voraussetzungen des Verfalls gemäß § 73 StGB oder der Einziehung gemäß § 74 StGB nicht gegeben. Liegen ebenso die Voraussetzungen des erweiterten Verfalls gemäß § 73 d StGB nicht vor, ist die Anordnung der Beschlagnahme gemäß § 111 b Abs. 3 StPO aufzuheben und die Sache an die gewahrsamsberechtigte Person herauszugeben. In den Fällen, in denen die Sache von der betroffenen Person offensichtlich nicht rechtmäßig erlangt wurde, kann sie unter bestimmten Voraussetzungen nach § 22 POG sichergestellt werden. Einer solchen Sicherstellung stehen die Bestimmungen der Strafprozessordnung nicht entgegen. Trotz der Freigabe der beschlagnahmten Sachen im Strafverfahren kann es ein öffentliches Interesse an der Sicherstellung zu Zwecken der Gefahrenabwehr geben (vgl. zur Zulässigkeit einer solchen Sicherstellung Beschluss des Niedersächsischen Oberverwaltungsgerichts vom 19. Oktober 2006, 5 B 284/06). Die Befugnisse des Strafprozessrechts und Polizeirechts schließen sich nicht gegenseitig aus, da sie unterschiedlichen Zielsetzungen dienen.

Nach der derzeitigen Zuständigkeitsverteilung gemäß § 1 POG sind für Sicherstellungen die allgemeinen Ordnungsbehörden originär zuständig. Die Zuständigkeit der Polizei ist nur bei Gefahr im Verzug gemäß dem bisherigen § 1 Abs. 7 POG gegeben. Um die Möglichkeiten der oben genannten Sicherstellungen effektiver nutzen zu können, ist jedoch ein abgestimmtes Zusammenwirken zwischen der zuständigen Staatsanwaltschaft, dem zuständigen Gericht und der anordnenden Sicherheitsbehörde erforderlich. Die Polizei kann als Ermittlungsbehörde bereits bestehende Informationen und Kontakte nutzen. Wegen der Sachnähe der Polizei zu diesen Verfahren wird deren ausschließliche Zuständigkeit als sachgerecht angesehen.

Handelt es sich um Sachen, die nicht zuvor in einem Strafverfahren zum Zweck der Vermögensabschöpfung beschlagnahmt worden sind, bleibt es bei der bisherigen Zuständigkeitsregelung. Dies gilt etwa für die Sicherstellung einer Sache, deren Beschlagnahme zum Zweck der Vermögensabschöpfung in einem Ordnungswidrigkeitsverfahren aufgehoben worden ist.

Zu Buchstabe c

Redaktionelle Folgeänderung zu der Änderung in Buchstabe b.

Zu Nummer 2 (§ 9 a)

Zu Buchstabe a

Zu Doppelbuchstabe aa

Das bisherige Recht zur Auskunftsverweigerung wird zu Zwecken der Gefahrenabwehr eingeschränkt. Wie bisher bleiben jedoch zeugnisverweigerungsberechtigte Berufsgeheimnisträgerinnen und Berufsgeheimnisträger nach § 53 Abs. 1 und § 53 a Abs. 1 StPO zur Verweigerung der Auskunft berechtigt.

Der neu eingefügte Satz 2 schränkt das bestehende Recht zur Auskunftsverweigerung ein, sofern die geforderte Auskunft zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person unerlässlich ist. Eine Güterabwägung macht es in diesen Fällen erforderlich, dem Schutz hochrangiger Rechtsgüter im Interesse einer effektiven Gefahrenabwehr grundsätzlich Vorrang vor dem Interesse des Einzelnen auf Auskunftsverweigerung einzuräumen. Diese Einschränkung der Auskunftsverweigerungsrechte ist auch im Vergleich zum umfassenden Schutz nach der Strafprozessordnung gemäß den §§ 52 bis 55 StPO gerechtfertigt, da das Gefahrenabwehrrecht dazu dient, Gefahren abzuwehren. Damit soll der Eintritt des Schadens verhindert werden.

Nach Satz 3 gilt diese Pflicht zur Auskunft hingegen nicht für zeugnisverweigerungsberechtigte Berufsgeheimnisträgerinnen und Berufsgeheimnisträger gemäß § 53 Abs. 1 und § 53 a Abs. 1 StPO. Die Norm gewährt den Betroffenen einen absoluten Schutz ihres Auskunftsverweigerungsrechts. Der privilegierte Personenkreis ist begrifflich durch Rechtsprechung und Lehre ausreichend bestimmt. Daraus ergibt sich u. a., dass von dem Zeugnisverweigerungsrecht nur Geistliche der öffentlich-rechtlichen Religionsgemeinschaften erfasst werden, und dies auch nur insoweit, als sie im konkreten Fall seelsorgerisch tätig werden.

Der Schutz von Geistlichen, Strafverteidigerinnen und Strafverteidigern sowie Abgeordneten nach § 53 Abs. 1 Satz 1 Nr. 1, 2 und 4 StPO ist bereits aufgrund ihrer besonderen verfassungsrechtlichen Bedeutung geboten. Das Bundesverfassungsgericht hat dies hinsichtlich des seelsorgerischen Gesprächs mit Geistlichen sowie des Gesprächs mit Strafverteidigerinnen oder Strafverteidigern mit Blick auf die Menschenwürde angenommen (BVerfG, Urteil vom 3. März 2004, 1 BvR 2378/98; 1 BvR 1084/99, Absatz Nr. 148). Darüber hinaus ist bei Geistlichen zu berücksichtigen, dass diese nach § 139 Abs. 2 StGB nicht verpflichtet sind anzuzeigen, was ihnen in ihrer Eigenschaft als Seelsorgerinnen oder Seelsorger anvertraut worden ist. Geistliche bleiben also straffrei, wenn sie schwere Straftaten nicht anzeigen, soweit ihnen diese Straftaten in ihrer Eigenschaft als Seelsorgerinnen oder Seelsorger bekannt geworden sind. Dem absoluten Schutz des Beicht- und Seelsorgegeheimnisses soll auch weiterhin im Gefahrenabwehrrecht Rechnung getragen werden.

Der Schutz von Parlamentsabgeordneten ist ebenso verfassungsrechtlich geboten. Das für sie bestehende Zeugnisverweigerungsrecht und das korrespondierende Beschlagnahmeverbot stehen unter dem verfassungsrechtlichen Schutz des Artikels 47 des Grundgesetzes, des Artikels 95 der Verfassung für Rheinland-Pfalz und vergleichbarer Regelungen in anderen Landesverfassungen.

Der absolute Schutz der Vertrauensverhältnisse von Berufsgruppen gemäß § 53 Abs. 1 Satz 1 Nr. 3 bis 3 b und Nr. 5 StPO, wie beispielweise Rechtsanwältinnen und Rechtsanwälten oder Ärztinnen und Ärzten, ist zwar nicht verfassungsrechtlich geboten, an deren Tätigkeit besteht aber ein hohes öffentliches Interesse. Um das Bestehen solcher Vertrauensverhältnisse zwischen der Berufsgeheimnisträgerin oder dem Berufsgeheimnisträger und demjenigen, der dies in Anspruch nimmt, zu schützen, steht diesen Personen ein uneingeschränktes Recht zur Verweigerung der Auskunft zu.

Das Recht zur Auskunftsverweigerung gilt auch für Hilfspersonen gemäß § 53 a Abs. 1 StPO. Dadurch soll verhindert werden, dass das Recht zur Auskunftsverweigerung für die Berufsgruppen nach § 53 Abs. 1 StPO auf dem Umweg über die Hilfspersonen umgangen wird. Vorausgesetzt wird des-

halb stets ein unmittelbarer Zusammenhang zwischen der Tätigkeit der Berufshelferin oder des Berufshelfers und der Tätigkeit der Hauptberufsträgerin oder des Hauptberufsträgers gemäß § 53 StPO Abs. 1 StPO.

Zu Doppelbuchstabe bb

Nach Satz 5 unterliegen die gemäß Satz 2 erlangten Auskünfte einer strengen Zweckbindung und dürfen nur zur Abwehr der jeweiligen Gefahr verwendet werden. Eine Verwendung zum Zweck der Strafverfolgung ist somit unzulässig. Das bedeutet, dass aufgrund einer Auskunft, die zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben von einer gemäß den §§ 52 bis 55 StPO zeugnis- oder auskunftsverweigerungsberechtigen Person erlangt wurde, kein Strafverfahren eingeleitet werden darf.

Zu Buchstabe b

In der Regelung wird der Begriff „Kraftfahrzeuge“ durch den Begriff „Fahrzeuge“ im Sinne des § 19 Abs. 1 Nr. 6 POG ersetzt, um den Anwendungsbereich der Bestimmung zu erweitern. Bislang war die Ermächtigung zu Kontrollen im öffentlichen Verkehrsraum begrenzt auf die Inaugenscheinnahme von Kraftfahrzeugen. Gemäß § 1 Abs. 2 des Straßenverkehrsgesetzes sind darunter nur Landfahrzeuge zu verstehen. Damit auch andere Fahrzeuge wie beispielsweise Schiffe kontrolliert werden können, ist die Erweiterung der Norm erforderlich. Ein Anwendungsfall der Befugnis kann nunmehr die Inaugenscheinnahme von Schiffen zur Bekämpfung der Schleuserkriminalität sein.

Zu Nummer 3 (§ 10 Abs. 2 Satz 4)

Nach Absatz 2 Satz 4 in seiner geltenden Fassung können die oder der Betroffene sowie die von ihr oder ihm mitgeführten Sachen unter den Voraussetzungen des Satz 3 durchsucht werden. Die sprachliche Neuformulierung der „mitgeführten Sachen“ in „Sachen, auf die er Zugriff hat“ dient der Klarstellung. Eine inhaltliche Änderung ist damit nicht verbunden. Durch die Formulierung „Sachen, auf die er Zugriff hat“ soll klargestellt werden, dass auch solche Sachen von der oder dem Betroffenen mitgeführt und unter den entsprechenden Voraussetzungen durchsucht werden dürfen, die sich in ihrem oder seinem faktischen Einwirkungsbereich befinden. Wirft etwa die Beifahrerin oder der Beifahrer, deren oder dessen Identität festgestellt werden soll, ihren oder seinen Personalausweis in das Fahrzeuginnere, so darf auch das Fahrzeug als eine Sache, auf die die Beifahrerin oder der Beifahrer Zugriff hat, durchsucht werden. Diese Möglichkeit besteht zwar auch nach der geltenden sprachlichen Fassung der Vorschrift, durch die Neuformulierung werden jedoch etwaige Unsicherheiten bei der Auslegung des Begriffs der von der betroffenen Person „mitgeführten Sachen“ vermieden.

Zu Nummer 4 (§ 11 a)

Zu Buchstabe a

Zu Doppelbuchstabe aa

Die Regelung fasst bisherige Verweisungen auf Bestimmungen zur Durchführung von molekulargenetischen Untersuchungen nach der Strafprozessordnung in einer Norm zusammen. Dabei wird auch berücksichtigt, dass das Gesetz zur Novellierung der forensischen DNA-Analyse vom 12. August 2005 (BGBl. I S. 2360) die Durchführung solcher Untersuchungen nunmehr zusammengefasst in § 81 f Abs. 2 StPO regelt. Der Regelungsgehalt des aufgehobenen § 81 f Abs. 1 Satz 3 StPO wurde in § 81 f Abs. 2 Satz 1 StPO aufgenommen. Der Verweis im bisherigen § 11 a Abs. 3 Satz 3 POG auf § 81 f Abs. 1 Satz 3 StPO ist somit gegenstandslos. Ferner entfällt der Verweis auf § 81 g Abs. 2 Satz 1 StPO, da die Bestimmung hierzu eigene Regelungen trifft. So regelt Absatz 2 Satz 1 bereits derzeit die Zweckbestimmung für molekulargenetische Untersuchungen und für die Speicherung von DNA-Identifizierungsmustern zu Zwecken der Gefahrenabwehr. Absatz 2 Satz 3 führt zudem eine eigene Vernichtungsregelung für die entnommenen Körperzellen ein.

Zu Doppelbuchstabe bb

Die Bestimmung verpflichtet zur unverzüglichen Vernichtung der entnommenen Körperzellen nach der Durchführung der molekulargenetischen Untersuchung. Ferner sind die gewonnenen und gespeicherten DNA-Identifizierungsmuster unverzüglich zu löschen, wenn sie zur Identitätsfeststellung nach Absatz 1 nicht mehr benötigt werden. Eine Zweckänderung der erhobenen Daten ist somit nicht zulässig.

Zu Buchstabe b

Zu Doppelbuchstabe aa

Absatz 3 regelt die Anpassung an die modifizierten Bestimmungen der Strafprozessordnung über den Richtervorbehalt für molekulargenetische Untersuchungen von Spuren. Durch das Gesetz zur Novellierung der forensischen DNA-Analyse wurde § 81 f StPO dahingehend geändert, dass auf den Richtervorbehalt für die molekulargenetische Untersuchung von Spuren verzichtet wurde.

Im Gefahrenabwehrrecht ist es ebenso gerechtfertigt, den Richtervorbehalt aufzuheben, wenn lediglich Spurenmaterial zu untersuchen ist. Im Zeitpunkt der molekulargenetischen Untersuchung einer Spur steht naturgemäß die Spurenverursacherin oder der Spurenverursacher noch nicht fest. Diese oder dieser kann vielmehr erst durch eine vergleichende Untersuchung, die ihrerseits die Entnahme von Körperzellen bei einer bestimmten Person voraussetzt, ermittelt werden. Den Belangen der Grundrechtsträgerin oder des Grundrechtsträgers, von dem das Spurenmaterial stammt, wird dadurch ausreichend Rechnung getragen, dass die Entnahme von Körperzellen und deren molekulargenetische Untersuchung auch zukünftig unter Richtervorbehalt stehen. Die vorherige richterliche Anordnung erfolgt damit dort, wo dies als präventiver Schutz des Grundrechts auf informationelle Selbstbestimmung gemäß Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes angemessen ist.

Ferner entfällt bei molekulargenetischen Untersuchungen von Toten die derzeit erforderliche richterliche Entscheidung. Durch diese Gesetzesänderung erfolgt die Anpassung an die entsprechende Bestimmung zur Strafverfolgung gemäß § 88 StPO. Das Gesetz zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung und zur Änderung anderer Vorschriften vom 27. Dezember 2003 (BGBl. I S. 3007) stellte klar, dass zum Zweck der Identitätsfeststellung bei einer aufgefundenen Leiche auch eine DNA-Analyse

durchgeführt werden darf. Einen Richtervorbehalt sieht § 88 StPO für diese Maßnahme nicht vor.

Zu Doppelbuchstabe bb

Mit der Änderung des § 81 f StPO durch das Gesetz zur Novellierung der forensischen DNA-Analyse ist der Verweis auf § 81 f Abs. 1 Satz 3 StPO gegenstandslos geworden. Der Verweis auf § 81 f Abs. 2 StPO ist nunmehr in Absatz 2 Satz 2 enthalten.

Zu Nummer 5 (§ 12)

Absatz 5 berücksichtigt die geänderte Rechtslage durch das Kostenrechtsmodernisierungsgesetz vom 5. Mai 2004 (BGBl. I S. 718), das das Gesetz über die Entschädigung von Zeugen und Sachverständigen in der Fassung vom 1. Oktober 1969 (BGBl. I S. 1756) aufhob und das Gesetz über die Vergütung von Sachverständigen, Dolmetscherinnen, Dolmetschern, Übersetzerinnen und Übersetzern sowie die Entschädigung von ehrenamtlichen Richterinnen, ehrenamtlichen Richtern, Zeuginnen, Zeugen und Dritten (Justizvergütungs- und -entschädigungsgesetz) vom 5. Mai 2004 (BGBl. I S. 718 –776–) am 1. Juli 2004 in Kraft setzte.

Zu Nummer 6 (§ 12 a)

Die neu geschaffene Ermächtigung befugt die Polizei zum Erlass von Meldeauflagen, um Straftaten zu verhindern. Meldeauflagen sind bereits bislang auf der Grundlage der Generalklauseln der Polizeigesetze der Länder zulässig, um im Einzelfall Gefahren für die öffentliche Sicherheit oder Ordnung abzuwehren (vgl. Urteil des Bundesverwaltungsgerichts vom 25. Juli 2007, 6 C 39.06). In Rheinland-Pfalz wurden Meldeauflagen insbesondere im Zusammenhang mit der Fußballweltmeisterschaft im Jahr 2006 erlassen, um die Begehung von Straftaten bei den sportlichen, kulturellen und gesellschaftlichen Veranstaltungen zu verhindern. Die neue Ermächtigung soll nunmehr die Voraussetzungen der Meldeauflage konkretisieren sowie die Zuständigkeit zum Erlass einer solchen Verfügung grundsätzlich auf die Polizei übertragen. Nach der derzeitigen Zuständigkeitsverteilung gemäß § 1 POG sind die allgemeinen Ordnungsbehörden für den Erlass von Meldeauflagen originär zuständig, sofern nicht Gefahr im Verzug gemäß dem bisherigen § 1 Abs. 7 POG vorliegt. Die Tatsachen zum Erlass einer solchen Meldeauflage beruhen jedoch regelmäßig auf polizeilichen Erkenntnissen. Zu nennen ist beispielsweise die in das polizeiliche Informationssystem einbezogene Verbunddatei „Gewalttäter Sport“, in der Täterinnen und Täter gespeichert werden, die durch Gewaltstraftaten im Zusammenhang mit sportlichen Ereignissen in Erscheinung getreten sind, wie beispielsweise Hooligans. Da die Polizei über die relevanten Daten und Erkenntnisse zum Erlass solcher Meldeauflagen verfügt, ist es auch sachgerecht, dass sie die Maßnahme erlässt.

Die Meldeauflagen dienen der Gefahrenabwehr. Die Befugnis regelt nunmehr die Meldeauflagen bereichsspezifisch, indem der Gefahrenbestand durch den Bezug auf die vorbeugende Bekämpfung von Straftaten näher konkretisiert wird.

Satz 1 befugt die Polizei zum Erlass von Meldeauflagen gegenüber einer Person, sofern Tatsachen die Annahme rechtfertigen, dass die Person eine Straftat begehen wird. Die Meldeauflagen haben das Ziel, insbesondere Großveranstaltungen wie Fußballspiele oder Versammlungen vor Gewalttäterinnen und Gewalttätern zu schützen. Inhalt der Meldeauflage ist die Pflicht, sich an bestimmten Tagen zu bestimmten Zeiten bei einer bestimmten Polizeidienststelle zu melden. Dadurch soll verhindert werden, dass die Verantwortlichen an gewalttätigen Auseinandersetzungen am Veranstaltungsort teilnehmen. Dabei ist es nicht entscheidend, ob die zu erwartende Straftat im Inland oder Ausland stattfindet. Behördliche Befugnisse wie beispielsweise Ausreisebeschränkungen oder Platzverweise bleiben durch diese Bestimmung unberührt und können zum Schutz der Veranstaltungen neben den Meldeauflagen angeordnet werden.

Meldeauflagen greifen in den Schutzbereich der allgemeinen Handlungsfreiheit gemäß Artikel 2 Abs. 1 des Grundgesetzes und in das Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes ein. Zudem wird die verantwortliche Person regelmäßig in ihrer Freizügigkeit gemäß Artikel 11 Abs. 1 des Grundgesetzes eingeschränkt. Meldeauflagen sind deshalb nur gerechtfertigt, wenn Tatsachen auf die Begehung von Straftaten hindeuten. Die Norm setzt damit eine auf Tatsachen beruhende Prognose voraus und verlangt, dass von der Adressatin oder dem Adressaten der Meldeauflage die Begehung von Straftaten droht. Die Ermächtigung lässt hingegen keine Meldeauflagen im Vorfeld einer Gefahr zu.

Satz 2 bestimmt als besondere Ausformung des Grundsatzes der Verhältnismäßigkeit, dass die Meldeauflage auf höchstens einen Monat zu befristen ist.

Nach Satz 3 ist eine Verlängerung der Maßnahme um jeweils nicht mehr als denselben Zeitraum zulässig, sofern die Voraussetzungen der Anordnung vorliegen. Aufgrund der mit der Verlängerung einhergehenden Eingriffsintensität der Maßnahme besteht nach Satz 4 für die Anordnung der Verlängerung ein Richtervorbehalt.

Zu Nummer 7 (§ 13)

Zu Buchstabe a

Nach Absatz 3 Satz 1 in seiner bisherigen Fassung können sowohl die Polizei als auch die allgemeinen Ordnungsbehörden einer Person verbieten, einen bestimmten Ort oder ein bestimmtes Gebiet zu betreten oder sich dort aufzuhalten, soweit Tatsachen die Annahme rechtfertigen, dass diese Person dort eine Straftat begehen wird. Ziel der Maßnahme ist demnach die vorbeugende Bekämpfung von Straftaten.

Nach § 1 Abs. 1 Satz 3 POG liegt die Zuständigkeit für die vorbeugende Bekämpfung von Straftaten ausschließlich bei der Polizei. Dem widerspricht die in Absatz 3 Satz 1 enthaltene Befugnis der allgemeinen Ordnungsbehörden, zum Zwecke der Straftatenverhütung ein Aufenthaltsverbot auszusprechen. Um die Aufgabenzuweisung in § 1 Abs. 1 Satz 3 POG mit der Befugnisnorm in Absatz 3 zu harmonisieren, wird die Ermächtigung zur Anordnung eines Aufenthaltsverbotes allein der Polizei übertragen.

Zu Buchstabe b

In Absatz 4 Satz 1 wird der Anwendungsbereich der polizeilichen Befugnis zu Aufenthalts-, Kontakt- und Näherungsverboten erweitert und deren Gefahrenschwelle herabgesenkt.

Das Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes und anderer Gesetze vom 2. März 2004 (GVBl. S. 202) führte diese polizeiliche Befugnis zusammen mit dem Wohnungsverweis zum Schutz der Opfer von Gewalt in engen sozialen Beziehungen ein. Die entsprechenden Gesetzesänderungen konnten damals bestehende Rechtsschutzlücken, die bis zum Erlass der zivilgerichtlichen Entscheidung nach dem Gewaltschutzgesetz vom 11. Dezember 2001 (BGBl. I S. 3513) bestanden, schließen. Im Gegensatz zum Gewaltschutzgesetz wurde die polizeiliche Befugnis zu Aufenthalts-, Kontakt- und Näherungsverboten auf die Fälle der Gewalt in engen sozialen Beziehungen begrenzt, da darin der wesentliche Anwendungsbereich des Gewaltphänomens gesehen wurde.

Diese Ermächtigung hat eine wichtige Bedeutung zum Schutz der betroffenen Opfer erlangt, da sie insbesondere die Befugnis zum Wohnungsverweis der verantwortlichen Person ergänzt. Die polizeilichen Erfahrungen zeigen allerdings, dass sich auch zunehmend Opfer von Gewalt an die Polizei wenden, die nicht in einer engen sozialen Beziehung zur verantwortlichen Person stehen. Auch diese Opfer bedürfen des polizeilichen Schutzes. Das Gesetz zur Strafbarkeit beharrlicher Nachstellungen vom 22. März 2007 (BGBl. I S. 354) gewährt diesen Opfern bereits einen verbesserten strafrechtlichen Schutz, indem bestehende Strafbarkeitslücken geschlossen wurden. Dieses Gesetz hat insbesondere den Straftatbestand der Nachstellung gemäß § 238 StGB in das Strafgesetzbuch eingeführt. Damit wird ein Verhalten unter Strafe gestellt, das unter der Bezeichnung Stalking bekannt geworden ist. Dieser Begriff ist aus der englischen Sprache entlehnt und bedeutet im Wortlaut sich anschleichen, heranpirschen. Das Phänomen des Stalkings kann somit als nachhaltige Beeinträchtigung einer Person durch Verfolgen, Auflauern, Ausspionieren, Bedrohen oder andere Arten der Kontaktaufnahme umschrieben werden.

Im Interesse eines umfassenden Opferschutzes ist es erforderlich, die Opfer bereits vor der Begehung einer Straftat zu schützen. Es ist deshalb notwendig, die bestehenden polizeilichen Ermächtigungen zur Gefahrenabwehr zu ergänzen. Entscheidend ist dabei auch, dass den Opfern durch die polizeilichen Anordnungen ein zeitnaher Schutz gewährt werden kann.

Die Gesetzesänderung hebt die Eingrenzung auf Fälle der Gewalt in engen sozialen Beziehungen auf. Durch die Einfügung des Wortes „insbesondere“ wird klargestellt, dass Gewalt in engen sozialen Beziehungen zwar ein bedeutsamer, jedoch nicht der einzige Anwendungsfall dieser Norm ist. Entscheidend ist ausschließlich das Vorliegen der gesetzlichen Gefahrenlage.

Ferner wird die Gefahrenschwelle zum polizeilichen Einschreiten auf das Vorliegen einer dringenden Gefahr herabgesenkt. Dringende Gefahr setzt eine Gefahr für hochrangige Rechtsgüter voraus. Damit werden zwar hohe Anforderungen an die zu schützenden Rechtsgüter gestellt, um der Eingriffsintensität der Maßnahmen Rechnung zu tragen. Eine besondere zeitliche Nähe zum Schadenseintritt wird hingegen nicht mehr gefordert.

Derzeit wird bei Gewalt in engen sozialen Beziehungen zur Abwehr der zeitlich unmittelbar bevorstehenden Gefahr häufig ein Wohnungsverweis gegenüber der verantwortlichen Person ausgesprochen. Diese Maßnahme zielt auf die Abwehr der akuten Gefahrensituation. Darüber hinaus ist es erforderlich, weitere Gefahrenlagen für das Opfer zu verhindern. Die Opfer von Gewalt leben regelmäßig in einer Dauergefahr, die vor allem durch ein Treffen oder Kontakt mit der Gewalttäterin oder dem Gewalttäter in eine akute Gefahrensituation umschlagen kann. Dabei steigert sich die Gewalteinwirkung vielfach im Laufe der Zeit. Durch die Gesetzesänderung soll nun unter erleichterten Anforderungen ein Aufenthalts-, Kontakt- und Näherungsverbot zulässig sein, um diesen Gefahrenlagen besser begegnen zu können. Dem Opfer soll damit auch die Möglichkeit gegeben werden, in Ruhe Entscheidungen über die künftige Lebensgestaltung zu treffen.

Zu Nummer 8 (§ 15 Abs. 2 Satz 2)

Die Gesetzesänderung berücksichtigt die geänderte Rechtslage durch das FGG-Reformgesetz vom 17. Dezember 2008 (BGBl. I S. 2586), zuletzt geändert durch Artikel 8 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2449). Die Bestimmung wird dahingehend geändert, dass nunmehr auf das Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit verwiesen wird. Dieses Gesetz, das durch das FGG-Reformgesetz am 1. September 2009 in Kraft gesetzt wurde, regelt in Buch 7 das Verfahren in Freiheitsentziehungssachen. Das Gesetz über das gerichtliche Verfahren bei Freiheitsentziehungen vom 29. Juni 1956 (BGBl. I S. 599) wurde durch Artikel 112 des FGG-Reformgesetzes aufgehoben.

Zu Nummer 9 (§§ 16 a und 16 b)

§ 16 a (Nicht polizeiliche Gewahrsamseinrichtung)

Nach dieser Vorschrift kann der Gewahrsam gemäß § 14 POG auch in einer hierfür geeigneten und vom fachlich zuständigen Ministerium bestimmten nicht polizeilichen Gewahrsamseinrichtung vollzogen werden. Eine nicht polizeiliche Einrichtung ist nach Satz 2 zum Vollzug des Gewahrsams geeignet, wenn die Sicherheit und Ordnung in der Einrichtung, der ordnungsgemäße Vollzug des Gewahrsams und die Rechte der festgehaltenen Personen gewährleistet werden. Für die Durchführung dieser Ingewahrsamnahmen gelten grundsätzlich die entsprechenden Bestimmungen zum polizeilichen Gewahrsam. § 16 POG sowie die Gewahrsamsordnung für die Polizei des Landes Rheinland-Pfalz vom 8. März 2003 (MinBl. S. 292; 2008 S. 326) sind damit analog anzuwenden. Abweichend hiervon kann allerdings in der Landeseinrichtung eine eigene, die polizeiliche Gewahrsamsordnung verdrängende Gewahrsamsordnung gelten, sofern diese in vergleichbarer Weise die Sicherheit und Ordnung in der Gewahrsamseinrichtung und die Rechte der festgehaltenen Personen gewährleistet.

Im Rahmen eines Modellversuchs besteht bereits derzeit durch Erlass des Ministeriums des Innern und für Sport vom 4. Dezember 2007 die Möglichkeit, den polizeilichen Gewahrsam in der Gewahrsamseinrichtung für Ausreisepflichtige (GfA) in Ingelheim durchzuführen. In der Einrichtung wurden zehn Gewahrsamsplätze eingerichtet, die von den rheinland-pfälzischen Polizeibehörden in Anspruch genommen werden können. Nachdem die Erfahrungen positiv sind, soll die Durchführung des polizeilichen Gewahrsams in der GfA fortgeführt werden. Die neu eingefügte Bestimmung schafft nunmehr die

gesetzlichen Grundlagen, den Modellversuch in den Regelbetrieb zu überführen.

§ 16 b (Datenerhebung durch den Einsatz technischer Mittel in polizeilichen Gewahrsamseinrichtungen)

Die Regelung ermächtigt die Polizei zur Datenerhebung durch den Einsatz technischer Mittel in polizeilichen Gewahrsamseinrichtungen. Bislang ist die Videoüberwachung in polizeilichen Gewahrsamseinrichtungen in Nummer 3.5 der Gewahrsamsordnung für die Polizei des Landes Rheinland-Pfalz geregelt. Da Videoüberwachungen gegenüber den Betroffenen einen Eingriff in den Schutzbereich des Grundrechts auf informationelle Selbstbestimmung gemäß Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes darstellen, ist die erforderliche gesetzliche Rechtsgrundlage zu schaffen. Die Vorschrift findet Anwendung, wenn Personen in polizeilichen Gewahrsamseinrichtungen aufgrund des § 14 POG in Gewahrsam genommen werden oder ihnen aufgrund anderer Rechtsvorschriften die Freiheit vorübergehend entzogen wird.

Absatz 1 Satz 1 befugt zur offenen Überwachung von polizeilichen Gewahrsamseinrichtungen mittels Bildübertragung. Eine Bildaufzeichnung gemäß § 27 Abs. 1 Satz 2 POG ist nach dieser Ermächtigung nicht zulässig.

Die offenen Videoübertragungen sollen Personen, die sich in der Gewahrsamseinrichtung aufhalten, vor Gefahrensituationen schützen. Diese können daraus resultieren, dass die Personen, die von der Polizei in Gewahrsam genommen werden müssen, häufig betrunken, medikamenten- oder rauschgiftabhängig sind. Während des Gewahrsamsaufenthalts kann es damit immer wieder zu Unfällen, Eigenverletzungen, Suizidversuchen oder zur Begehung von Straftaten kommen. Die Datenerhebung setzt keine konkrete Gefahrenlage voraus, sondern es reichen tatsächliche Anhaltspunkte, die die Annahme rechtfertigen, dass die Maßnahme zum Schutz von Personen erforderlich ist. Bloße Vermutungen genügen jedoch nicht, um eine Bildübertragung zu rechtfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die eine Gefahrenprognose tragen. Tatsächliche Anhaltspunkte, die die Annahme rechtfertigen, dass die Videoüberwachung zum Schutz von Personen erforderlich ist, können sich etwa aus dem Verhalten der festgehaltenen Person bei ihrer Einlieferung oder bei ihrer Begleitung zu Sanitäreinrichtungen, zu Aufenthalten im Freien oder zu Vernehmungsterminen ergeben. Die Videoüberberwachung ist dann beispielsweise in den Fluren, Vorräumen, Aufenthaltsräumen oder im Freien zulässig. Die Möglichkeit einer Gefährdung der festgehaltenen Person kann insbesondere auch in den Gewahrsamsräumen bestehen. Zwar sind Personen, die erkennbar geistig verwirrt sind und/oder Suizidabsichten hegen oder so stark unter der Einwirkung von Rauschmitteln stehen, dass hierdurch lebensbedrohliche Zustände eintreten können, nicht gewahrsamsfähig, sodass die Unterbringung in einer geschlossenen psychiatrischen Einrichtung oder in einem Krankenhaus angezeigt ist. Dennoch können auch bei Personen, die nach dem äußeren Eindruck gewahrsamsfähig sind, auto- oder fremdaggressive Verhaltensweisen auftreten. Um insbesondere Gefahren für Leib oder Leben der festgehaltenen Person auszuschließen, umfasst die Ermächtigung zur offenen Videoüberwachung auch die Gewahrsamsräume.

Nach Absatz 1 Satz 2 ist der Schutz der Intimsphäre der festgehaltenen Person, soweit möglich, zu wahren. Das bedeutet, dass sie insbesondere auf den Umstand der Videoüberwachung hinzuweisen und ihr die Möglichkeit zu eröffnen ist, auf Wunsch eine Toilette außerhalb des Gewahrsamsraums aufzusuchen.

Absatz 1 Satz 3 bestimmt, dass die Datenerhebung durch ein optisches oder akustisches Signal anzuzeigen ist.

Nach Absatz 2 sind die zur Anordnung führenden tatsächlichen Anhaltspunkte der optisch-elektronischen Beobachtung in Gewahrsamsräumen sowie Beginn und Ende der Bildübertragung zu dokumentieren. Die Dokumentationspflicht dient der Nachvollziehbarkeit und datenschutzrechtlichen Kontrolle von Videoüberwachungsmaßnahmen in Gewahrsamsräumen.

Nach Absatz 3 gelten die Absätze 1 und 2 für nicht polizeiliche Gewahrsamseinrichtungen gem. § 16 a POG entsprechend.

Zu Nummer 10 (§ 18)

Zu Buchstabe a

Redaktionelle Änderung.

Zu Buchstabe b

Zu Doppelbuchstabe aa und bb

Redaktionelle Folgeänderungen.

Zu Doppelbuchstabe cc

Die polizeiliche Ermächtigung zur Durchsuchung von Personen zu Zwecken der Eigensicherung wird erweitert, um den Schutz der Polizeibeamtinnen und Polizeibeamten oder Dritten bei der täglichen Polizeiarbeit zu verbessern. Der Anwendungsbereich dieser polizeilichen Befugnis ist auf die in der Norm abschließend genannten Standardmaßnahmen begrenzt. Dieser abschließende Katalog wird nunmehr um die Kontrollen im öffentlichen Verkehrsraum gemäß § 36 Abs. 5 der Straßenverkehrs-Ordnung (StVO) ergänzt. Damit wird der Tatsache Rechnung getragen, dass eine Vielzahl von polizeilichen Kontrollen auf Grundlage des § 36 Abs. 5 StVO durchgeführt werden und sich hieraus stets gefahrenträchtige Situationen entwickeln können.

Zu Buchstabe c

Die Bestimmung schafft die Rechtsgrundlage für körperliche Untersuchungen zur Abwehr von Gefahren für Leib oder Leben. Die körperliche Untersuchung ist darauf gerichtet, den Zustand und die Beschaffenheit des Körpers sowie seiner Bestandteile für die Zwecke der Gefahrenabwehr festzustellen. Die Ermächtigung befugt hingegen nicht zu medizinischen Behandlungsmaßnahmen.

Das Land besitzt die Gesetzgebungskompetenz für diese Ermächtigung zu Zwecken der Gefahrenabwehr. Zwar hat der Bund die konkurrierende Gesetzgebungskompetenz nach Artikel 74 Abs. 1 Nr. 19 des Grundgesetzes für „Maßnahmen gegen gemeingefährliche oder übertragbare Krankheiten“. Darunter sind alle Infektionskrankheiten zu verstehen, sodass alle Krankheiten im Sinne des § 2 Nr. 3 des Infektionsschutz-

gesetzes vom 20. Juli 2000 (BGBl. I S. 1045), zuletzt geändert durch Artikel 2 a des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091), erfasst werden. Mit dem Infektionsschutzgesetz hat der Bund im Sinne des Artikels 72 Abs. 1 des Grundgesetzes von seiner Gesetzgebungszuständigkeit Gebrauch gemacht. Der Bundesgesetzgeber hat jedoch die Blutentnahme zur Gefahrenabwehr (Individualprophylaxe), verbunden mit einer entsprechend klar definierten Datenweitergabe, bisher nicht spezialgesetzlich geregelt. Er hat somit in dieser speziellen Frage von seiner Gesetzgebungszuständigkeit nicht abschließend Gebrauch gemacht, sodass das Infektionsschutzgesetz einer landesrechtlichen Regelung nicht entgegensteht.

Die Innenministerkonferenz betonte in ihrem Beschluss vom 18./19. November 2004 die dringende Notwendigkeit, angesichts der Opfersituation von vergewaltigten Personen, insbesondere Frauen und Kindern, sowie berufsbedingt betroffenen Personengruppen (Ärztinnen und Ärzte sowie Krankenpflegepersonal, Strafvollzugs- und Polizeibedienstete) eine gesetzliche Regelung für die Entnahme von Blutproben zum Zweck der Gefahrenabwehr zu schaffen.

Satz 1 fordert als Voraussetzung für körperliche Untersuchungen das Vorliegen einer Gefahr für Leib oder Leben. Ein wesentlicher Anwendungsfall dieser Norm ist die körperliche Untersuchung zur Abwehr von Infektionsgefahren. Kommen Opfer von Gewaltdelikten oder Polizeibeamtinnen oder Polizeibeamte im Rahmen ihres Einschreitens mit möglicherweise infektiösen Körperflüssigkeiten der Verursacherin oder des Verursachers in Kontakt, beispielsweise durch Stichverletzungen an einer Spritze bei einer Durchsuchung oder eine Bisswunde, kann die Entnahme einer Blutprobe und ihre Untersuchung Sicherheit über das Infektionsrisiko geben und gegebenenfalls schnell eine gezielte Behandlung des Opfers eingeleitet werden. Dabei muss die Behandlung zeitnah zur möglichen Übertragung der Krankheitserreger begonnen werden, um ihren Erfolg nicht zu gefährden. Bei Verdacht auf eine HIV-Infektion ist beispielsweise ein Behandlungsbeginn innerhalb der ersten zwei bis vier Stunden optimal. Die Notwendigkeit der Einleitung medizinischer Maßnahmen beim Opfer ist durch eine Ärztin oder einen Arzt zu bewerten.

Sollte das Ergebnis der Blutuntersuchung nicht zeitgerecht vorliegen, kann entsprechend der ärztlichen Beratung mit einer Behandlung begonnen werden. Da die Behandlung mit gravierenden Nebenwirkungen einhergeht, ist auch nach Beginn der Behandlung eine schnellstmögliche Verifizierung einer Infektion unabdingbar, um für den Fall, dass keine übertragbare Krankheit vorliegt, unverzüglich die Behandlung abzubrechen. In der gleichen Weise ist zu verfahren, wenn zwar die Blutuntersuchung der verantwortlichen Person ein negatives Ergebnis ergibt, allerdings nicht ausgeschlossen werden kann, dass bei ihr eine frische Infektion vorliegt, die im Blut noch nicht nachweisbar ist.

Die Untersuchung des Verursacherbluts kann in diesen Fällen notwendige Erkenntnisse für die ärztliche Entscheidungsfindung bringen.

Die Regelung kommt allen Personen zugute, die aus ärztlicher Sicht einer Infektionsgefährdung ausgesetzt waren, insbesondere Opfern von Gewaltdelikten, aber auch beispielsweise medizinischem Personal oder Polizeibeamtinnen und Polizeibeamten. Ein weiterer Anwendungsbereich kann gegebenenfalls in der Untersuchung von gefährdeten Personen selbst liegen. Körperliche Untersuchungseingriffe ohne oder gegen den Willen der Betroffenen können im Einzelfall zum Schutz von Leib und Leben und damit zu dessen Rettung, beispielsweise bei einer konkreten Vergiftungsgefahr, erforderlich werden.

Satz 2, der § 81 a Abs. 1 Satz 2 StPO entspricht, regelt, dass Entnahmen von Blutproben und andere körperliche Eingriffe nur von einer Ärztin oder einem Arzt nach den Regeln der ärztlichen Kunst vorgenommen werden dürfen. Unter einem körperlichen Eingriff ist alles zu verstehen, was zu einer auch noch so geringfügigen Verletzung des Körpers führt oder führen kann. Vor einem körperlichen Eingriff hat deshalb eine Ärztin oder ein Arzt mit entsprechenden Fachkenntnissen festzustellen, dass kein Nachteil für die Gesundheit der Betroffenen zu befürchten ist.

Satz 3 bestimmt für die körperliche Untersuchung einen Richtervorbehalt. Satz 4 regelt die Zuständigkeit des Amtsgerichts. Satz 5 verweist im Hinblick auf das Verfahren auf § 21 Abs. 1 Satz 3 POG, der wiederum auf das Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit Bezug nimmt. Bei Gefahr im Verzug kann nach Satz 6 die Anordnung durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes erfolgen.

Satz 7 begrenzt die Zulässigkeit der Zweckänderung der erhobenen personenbezogenen Daten auf die Fälle zur Abwehr schwerwiegender Gesundheitsgefährdungen oder zur Verfolgung von Straftaten von erheblicher Bedeutung gemäß § 28 Abs. 3 POG. Damit soll ein vergleichbarer Maßstab wie bei der Erhebung dieser Daten angelegt werden. Die Verwertung der Daten für Beweiszwecke in einem Strafverfahren wegen einer Straftat von erheblicher Bedeutung soll ausdrücklich ermöglicht werden. Dies gilt insbesondere für die Fälle, in denen die Gefahrenlage durch eine Straftat der verantwortlichen Person gegen Leib, Leben oder körperliche Integrität des Opfers verursacht wurde. Satz 8 gibt den allgemeinen Grundsatz des Datenschutzes wieder, wonach die erlangten personenbezogenen Daten unverzüglich zu löschen sind, wenn sie nicht mehr erforderlich sind.

Zu Buchstabe d

Zu Doppelbuchstabe aa und bb

Der Inhalt des bisherigen Absatzes 3 geht in den neuen Absatz 4 ein, der um Regelungen zur körperlichen Untersuchung ergänzt wird. Danach darf eine körperliche Untersuchung nur von Personen des gleichen Geschlechts oder Ärztinnen und Ärzten körperlich durchgeführt werden. Zwar sind körperliche Untersuchungen bereits nach § 18 Abs. 3 Satz 2 POG stets von Ärztinnen oder Ärzten vorzunehmen, sofern die Maßnahme mit einem körperlichen Eingriff verbunden ist. In der Mehrzahl der körperlichen Untersuchungen wird diese Voraussetzung gegeben sein. In den Fällen, in denen kein körperlicher Eingriff vorliegt und die Polizei die Maßnahme selbstständig durchführen darf, ist nunmehr nach Absatz 4 zwingend zu beachten, dass diese nur Personen des gleichen Geschlechts durchführen dürfen. Solche körperlichen Untersuchungen können Augenscheinnahmen der Körperoberfläche zwecks Auffindens bestimmter Körpermerkmale (z. B. Leberflecken oder Tätowierungen) oder Verletzungen (Kratz- und Injektionsspuren, Blutspritzer auf der Haut) sein, sofern es sich nicht um Auffälligkeiten handelt, die sich offen dar-

bieten. Nach dem Halbsatz 2 der Regelung gilt etwas anderes nur dann, wenn die sofortige körperliche Untersuchung zur Abwehr der Gefahr für Leib oder Leben erforderlich ist.

Zu Buchstabe e

Redaktionelle Folgeänderung.

Zu Nummer 11 (§ 21 Abs. 1)

Zu Buchstabe a

Redaktionelle Änderung.

Zu Buchstabe b

Redaktionelle Anpassung an die geänderte Gesetzesbezeichnung.

Zu Nummer 12 (§ 25 Abs. 3 Satz 1)

Durch die Änderung der Regelung wird klargestellt, dass neben den Kosten der Sicherstellung und Verwahrung einer Sache auch die Kosten deren Unbrauchbarmachung und Vernichtung von der verantwortlichen Person zu erstatten sind.

Zu Nummer 13 (§ 27)

Zu Buchstabe a

Die Befugnis zum Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen in öffentlich zugänglichen Räumen zum Zweck der Eigensicherung von Polizeibeamtinnen und Polizeibeamten oder Dritten wird erweitert. Durch den Verweis auf den neu eingefügten § 18 Abs. 2 Nr. 7 POG wird die Bestimmung um Kontrollen im öffentlichen Verkehrsraum gemäß § 36 Abs. 5 StVO ergänzt. Damit wird die Polizei nunmehr auch bei solchen Kontrollen zu Bild- und Tonaufzeichnungen zum Zweck der Eigensicherung befugt. Ziel der Gesetzesänderung ist die Verbesserung der Eigensicherung bei der täglichen Polizeiarbeit, die stets mit Gefahren verbunden sein kann.

Zu Buchstabe b

Die in Absatz 5 enthaltene Befugnis zum automatisierten Kfz-Kennzeichenabgleich, von der bislang kein Gebrauch gemacht wurde, wird aufgehoben. Das Bundesverfassungsgericht hat mit Urteil vom 11. März 2008 (1 BvR 2074/05; 1 BvR 1254/07) entschieden, dass die Ermächtigungen der Länder Hessen und Schleswig-Holstein zum automatisierten Kfz-Kennzeichenabgleich insbesondere wegen Verstößen gegen den Bestimmtheits- und Verhältnismäßigkeitsgrundsatz nichtig sind. Da die rheinland-pfälzische Bestimmung im Wesentlichen der schleswig-holsteinischen Ermächtigung entspricht, genügt die Norm den verfassungsrechtlichen Anforderungen nicht und ist aufzuheben.

Zu Buchstabe c

Zu Doppelbuchstabe aa

Redaktionelle Folgeänderung.

Zu Doppelbuchstabe bb

Die Verpflichtung zur Löschung von angefertigten Bild- und Tonaufzeichnungen sowie daraus gefertigten Unterlagen wird restriktiver gefasst. Die Einschränkung der Löschungsverpflichtung, wonach die erhobenen Daten spätestens zwei Monate nach der Feststellung, dass die Daten oder Unterlagen nicht mehr erforderlich sind, zu löschen oder zu vernichten sind, entfällt. Nach der Neufassung sind personenbezogene Daten oder Unterlagen, die durch Maßnahmen nach § 27 POG erhoben worden sind, unverzüglich zu löschen oder zu vernichten, soweit diese nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung, zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten oder zur Behebung einer bestehenden Beweisnot, erforderlich sind. Diese Bestimmung entspricht den Belangen des Datenschutzes und steht nicht im Widerspruch zu den Interessen der Gefahrenabwehr.

Zu Buchstabe d

Redaktionelle Folgeänderung.

Zu Buchstabe e

Nach Absatz 7 Satz 1 haben die örtlichen Ordnungsbehörden Datenerhebungen nach § 27 Abs. 1 POG spätestens zwei Wochen vor deren Durchführung sowohl gegenüber der Landesordnungsbehörde als auch gegenüber der oder dem Landesbeauftragten für den Datenschutz anzuzeigen. Die Anzeigepflicht dient der frühzeitigen Information und Überprüfung entsprechender Videomaßnahmen.

Die Landesordnungsbehörde soll damit die Möglichkeit erhalten, frühzeitig die rechtlichen Voraussetzungen der Maßnahme zu überprüfen und auf einen einheitlichen Vollzug der Vorschrift hinzuwirken. Da die Landesordnungsbehörde landesweit zuständig ist, erhält sie durch die Anzeigepflicht auch einen Gesamtüberblick über die Videomaßnahmen der örtlichen Ordnungsbehörden im Land.

Da Datenerhebungen nach § 27 Abs. 1 POG insbesondere in das Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes eingreifen, sind sie ebenfalls gegenüber der oder dem Landesbeauftragten für den Datenschutz anzuzeigen. Nach Absatz 7 Satz 2 gilt eine entsprechende Anzeigepflicht für die Polizei bei Datenerhebungen nach den Absätzen 1 und 3. Die oder der Landesbeauftragte für den Datenschutz überwacht als unabhängige oberste Landesbehörde die Einhaltung des Landesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz durch die öffentlichen Stellen des Landes.

Die Anzeigepflicht beinhaltet dabei keinen Genehmigungsvorbehalt, sodass die Verantwortung für die Anordnung und Durchführung der Maßnahme bei der örtlichen Ordnungsbehörde bzw. der Polizei verbleibt.

Zu Nummer 14 (§ 28)

Zu Buchstabe a

Der bisherige Absatz 4 entfällt, da sein Regelungsinhalt nunmehr im neu eingefügten § 39 b POG, der den Schutz von zeugnisverweigerungsberechtigten Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern im Sinne des § 53 Abs. 1 und des § 53 a Abs. 1 StPO bei verdeckten Maßnahmen regelt, aufgenommen wird.

Zu Buchstabe b

Die Zuständigkeit der Amtsgerichte für die Anordnung besonderer Mittel der Datenerhebung wird neu geregelt. Entsprechend der Regelung in anderen Fällen – wie etwa der Anordnung molekulargenetischer Untersuchungen nach § 11 a Abs. 3 Satz 2 POG – soll auch hier das Amtsgericht zuständig sein, in dessen Bezirk die Polizeidienststelle ihren Sitz hat.

Zu Buchstabe c

Redaktionelle Folgeänderungen.

Zu Nummer 15 (§ 29)

Die Änderung des § 29 POG ist darin gegründet, dass der Schutz des unantastbaren Kernbereichs privater Lebensgestaltung sowie der Schutz von zeugnisverweigerungsberechtigten Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern im Sinne des § 53 Abs. 1 und des § 53 a Abs. 1 StPO jeweils in eigenen Bestimmungen gemäß § 39 a und § 39 b POG geregelt werden. Damit sind die bisherigen bereichsspezifischen Bestimmungen zu streichen.

Zu Buchstabe a

Satz 2 stellt klar, dass die Anforderungen zum Schutz des unantastbaren Kernbereichs privater Lebensgestaltung nach dem neu eingefügten § 39 a Abs. 2 POG zu beachten sind.

Zu Buchstabe b

Zu Doppelbuchstabe aa

Die in Absatz 2 Nr. 1 aufgezählten besonders schweren Straftaten werden um den Tatbestand der Verbreitung, des Erwerbs und den Besitz kinderpornografischer Schriften in den Fällen des § 184 b Abs. 3 StGB erweitert. Damit erfolgt eine Angleichung an die entsprechende Vorschrift des § 100 c Abs. 2 StPO, die in Absatz 2 Nr. 1 Buchst. e im Falle des § 184 b Abs. 3 StGB ebenfalls von einer besonders schweren Straftat ausgeht.

Zu Doppelbuchstabe bb

Redaktionelle Änderungen.

Zu Buchstabe c

Die bisherigen Absätze 3 bis 6 entfallen, da ihre Regelungsinhalte nunmehr in § 39 Abs. 2 Satz 2 und den §§ 39 a und 39 b POG enthalten sind.

Zu Buchstabe d

Der bisherige Absatz 7 wird zu Absatz 3.

Zu Doppelbuchstabe aa und bb

Redaktionelle Änderungen.

Zu Doppelbuchstabe cc

Satz 4 wird sprachlich neu gefasst, ohne dass damit eine inhaltliche Änderung verbunden ist.

Zu Buchstabe e

Der bisherige Absatz 8 wird zu Absatz 4. Die Sätze 3 und 4 werden gestrichen, da ihre Regelungsinhalte nunmehr von § 39 a Abs. 4 Satz 1 und Abs. 5 Satz 2 POG mit umfasst werden.

Zu Buchstabe f

Redaktionelle Änderung.

Zu Buchstabe g

Zu Doppelbuchstabe aa

Absatz 6 Satz 1 legt fest, dass das für die nach Absatz 3 erforderliche richterliche Anordnung zuständige Gericht das Oberverwaltungsgericht Rheinland-Pfalz ist. Entscheidungen über die Anordnung verdeckter Ermittlungsmaßnahmen nach den §§ 29, 31, 31 b, 31 c, 31 d und 31 e POG haben besonders grundrechtsintensive Sachverhalte zum Gegenstand. Für diese Fälle soll durch die Verlagerung der bisherigen Zuständigkeit der Amtsgerichte auf das Oberverwaltungsgericht Rheinland-Pfalz die Wirksamkeit des Richtervorbehalts akzentuiert werden, da für die richterliche Beurteilung derart intensiver Grundrechtseingriffe profunde Kenntnisse des Verfassungs- und Verwaltungsrechts sowie entsprechende Erfahrungen förderlich sind. Dieser Zielsetzung trägt die Übertragung von Entscheidungen über die Anordnung verdeckter Ermittlungsmaßnahmen nach Maßgabe der vorbezeichneten Vorschriften an die Verwaltungsgerichtsbarkeit Rechnung. In Anlehnung an die in dem Koalitionsvertrag auf Bundesebene zwischen CDU, CSU und FDP getroffene Vereinbarung, dass künftig für die Entscheidung über die Anordnung der verdeckten Ermittlungsmaßnahmen nach dem Abschnitt zur Gefahrenabwehr gegen den internationalen Terrorismus im Bundeskriminalamtgesetz zur Verstärkung der Rechtsstaatlichkeit der Entscheidung nicht mehr eine Richterin oder ein Richter des Amtsgerichts am Sitz des BKA, sondern eine Richterin oder ein Richter am Bundesgerichtshof durch Vermittlung der Generalbundesanwältin oder des Generalbundesanwalts zuständig sein soll, wird die Anordnungsbefugnis nach Absatz 6 Satz 1 für die nach Absatz 3 erforderliche richterliche Anordnung ebenfalls nicht einem erstinstanzlichen Gericht, sondern dem höchsten (Landes-)Gericht des Gerichtszweiges zugewiesen.

Zu Doppelbuchstabe bb

Das gerichtliche Verfahren für die Entscheidungen des Oberverwaltungsgerichts Rheinland-Pfalz über die Anordnung verdeckter Ermittlungsmaßnahmen nach den §§ 29, 31, 31 b bis 31 e POG richtet sich nach der Verwaltungsgerichtsordnung. Da die Entscheidung über die Anordnung besonders grundrechtsrelevanter Maßnahmen der Polizei durch das Oberverwaltungsgericht Rheinland-Pfalz getroffen wird, ist es folgerichtig, wenn das Gericht, wie auch in sonstigen polizeirechtlichen Streitigkeiten, nach Maßgabe der Verwaltungsgerichtsordnung entscheidet. Die Anwendung der Verwaltungsgerichtsordnung schafft auch Klarheit darüber, dass das Oberverwaltungsgericht letztinstanzlich entscheidet.

Zu den Buchstaben h und i

Redaktionelle Änderungen.

Zu Nummer 16 (§§ 31 bis 31 e)

§ 31 (Datenerhebung durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation, Auskunft über die Telekommunikation)

Die polizeiliche Ermächtigung zur Überwachung und Aufzeichnung der Telekommunikation sowie zur Erhebung von Verkehrsdaten wird neu gefasst.

Das Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes und anderer Gesetze vom 2. März 2004 (GVBl. S. 202) schuf eine umfassende Ermächtigung zur polizeilichen Telekommunikationsüberwachung, die seit dieser Zeit eine wichtige Bedeutung für die Aufgabe der Gefahrenabwehr erlangt hat. Die Berichte der Landesregierung über inhaltliche Telekommunikationsüberwachungen (vgl. Landtagsdrucksachen 15/114, 15/1502, 15/2236, 15/3438) zeigen, dass solche Maßnahmen zwar nur in seltenen Fällen angewendet werden. Sie sind jedoch bei besonderen Gefahrenlagen zur Abwehr von Gefahren für hochrangige Rechtsgüter unerlässlich. Standortfeststellungen zur Rettung von Suizidgefährdeten oder hilflosen Personen, beispielsweise gebrechlichen Personen und Kindern, stellen polizeiliche Standardmaßnahmen der Lebensrettung dar, die in einer Vielzahl von Fällen durchgeführt werden. Angesichts aktueller Anforderungen der Verfassungsrechtsprechung und technischer Entwicklungen ist es nunmehr erforderlich, die Bestimmung zu überarbeiten.

Im Rahmen der Neufassung wird die bisherige Befugnis zu Standortfeststellungen einer Telekommunikationsteilnehmerin oder eines Telekommunikationsteilnehmers und Feststellungen der Polizei nicht bekannter Telekommunikationsanschlüsse bereichsspezifisch in einer eigenen Norm gemäß § 31 a POG geregelt. Ferner wird die Rechtsprechung des Bundesverfassungsgerichts zur sogenannten Quellen-Telekommunikationsüberwachung (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07 und 1 BvR 595/07) durch eine Ermächtigung in Absatz 3 berücksichtigt. Die bisherigen bereichsspezifischen Bestimmungen zum Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträgerinnen und Berufsgeheimnisträger gemäß § 53 Abs. 1 und § 53 a Abs. 1 StPO und zur Löschung erlangter Unterlagen werden in diese Bestimmung nicht übernommen, da ihre Regelungsinhalte nunmehr in § 39 Abs. 2 Satz 1 Nr. 4 und Satz 2 und 3 sowie § 39 b POG enthalten sind.

Absatz 1 formuliert die materiellen Anforderungen und orientiert sich dabei am bisherigen Absatz 1. Wie bislang soll die Maßnahme grundsätzlich nur zur Abwehr einer gegenwärtigen Gefahr zulässig sein. Lediglich im Fall der Quellen-Telekommunikationsüberwachung nach Absatz 3 genügt eine konkrete Gefahr für hochwertige Rechtsgüter. In Satz 1 wird die Befugnis in Anlehnung an die neu geschaffenen Ermächtigungen gemäß den §§ 31 b, 31 c und 31 d POG um die Tatbestandsalternative „zur Abwehr einer Gefahr für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt“ ergänzt. Neben hochrangigen Individualrechtsgütern sollen damit zukünftig ebenso die Schutzgüter der Allgemeinheit geschützt werden. Im Hinblick auf diese neue Tatbestandsalternative wird auf die Erläuterung zu § 31 c POG verwiesen.

Weiterhin wird der Kreis der Verantwortlichen um den „Nachrichtenmittler“ erweitert. Insbesondere zur Abwehr von Gefahren der organisierten Kriminalität und des internationalen Terrorismus kann es notwendig sein, auch gegen diese Personen entsprechende Maßnahmen durchzuführen. Die Änderung orientiert sich an den bestehenden Bestimmungen zur Telekommunikationsüberwachung gemäß § 100 a Abs. 3 StPO und § 20 l Abs. 1 Satz 1 Nr. 3 BKAG.

Satz 2 übernimmt die Regelung des bisherigen § 31 Abs. 1 POG, wonach die Datenerhebung zwingend sein muss. Ferner stellt dieser Satz klar, dass die Anforderungen gemäß § 39 a Abs. 3 POG an den Schutz des Kernbereichs privater Lebensgestaltung bei der Anordnung einer Telekommunikationsüberwachung einzuhalten sind. Satz 3 entspricht der Regelung im bisherigen § 31 Abs. 2 Satz 1 POG.

Absatz 2 Satz 1 bestimmt, auf welche Art von Daten sich die Maßnahme nach Absatz 1 beziehen darf und enthält zwei Alternativen. Nach der ersten Alternative wird die Polizei wie bislang zur Überwachung von Inhalten der Telekommunikation ermächtigt. Die zweite Alternative umfasst die Erhebung von Verkehrsdaten. Der Begriff der Verkehrsdaten ersetzt den bisherigen Begriff „nähere Umstände der Telekommunikation“, wodurch eine Anpassung an den Sprachgebrauch des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. I S. 3198) erfolgt. Verkehrsdaten sind nach § 3 Nr. 30 des Telekommunikationsgesetzes (TKG) vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 2 des Gesetzes vom 17. Februar 2010 (BGBl. I S. 78), Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Die Regelung ist technikoffen formuliert, um zukünftigen technischen Entwicklungen Rechnung tragen zu können. § 96 Abs. 1 TKG konkretisiert diesen Begriff, indem er die Verkehrsdaten aufzählt, die der Telekommunikations-Diensteanbieter erheben und verwenden darf. Zu den Verkehrsdaten zählen u. a. die Teilnehmerkennung, Beginn und Ende der Verbindung einschließlich Datum und Uhrzeit.

Unter den Begriff der Verkehrsdaten fallen ebenso die Standortdaten eines Mobilfunkendgeräts und die Kartennummer von mobilen Telekommunikationsendgeräten (IMEI-Nummer: International Mobilstation Equipment Identity). Die Erhebung solcher Daten und Auskunft darüber werden nunmehr allerdings bereichsspezifisch in § 31 a POG geregelt, sodass insoweit § 31 POG verdrängt wird.

Die Neufassung übernimmt nicht die Nummern 3 und 4 des bisherigen § 31 Abs. 2 Satz 1 POG, da ihr Regelungsinhalt vom Begriff der Verkehrsdaten mit umfasst wird.

Ebenso entfällt die Regelung im bisherigen § 31 Abs. 2 Satz 2 POG, da ihr kein eigener Regelungsgehalt zukommt. Die Bestimmung, welche Telekommunikationsanschlüsse überwacht werden können, ergibt sich ausschließlich aus der Regelung zur Inanspruchnahme der verantwortlichen Personen gemäß Absatz 1 Satz 1.

Absatz 2 Satz 2 entspricht inhaltlich dem bisherigen § 31 Abs. 2 Satz 3 POG. Die Regelung wird jedoch konkretisiert, indem klargestellt wird, dass sich die Datenerhebung auf Ver-

kehrsdaten, die zeitlich vor der Anordnung der Maßnahme erhoben und dann gespeichert worden sind, erstrecken kann. Unter Anordnung ist entweder die gerichtliche oder die behördliche Anordnung zu verstehen.

Der Absatz 3 regelt den verdeckten, technischen Eingriff in ein informationstechnisches System zum Zweck der Telekommunikationsüberwachung (sogenannte Quellen-Telekommunikationsüberwachung). Durch diese Befugnis kann verschlüsselte Telekommunikation mittels Internettelefonie überwacht werden. Eine solche Datenerhebung wird in der Tätigkeit der Ermittlungsbehörden eine immer größere Bedeutung erlangen, da die zukünftige Telekommunikation regelmäßig verschlüsselt ablaufen wird.

Das Bundesverfassungsgericht erkannte im Urteil vom 27. Februar 2008 (1 BvR 370/07 und 1 BvR 595/07, Absatz Nr. 190) an, dass das Fernmeldegeheimnis gemäß Artikel 10 des Grundgesetzes alleiniger grundrechtlicher Maßstab für die Beurteilung einer solchen Ermächtigung ist, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Kommunikationsvorgang beschränkt und dies durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt ist. Damit ist zwischen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung zu differenzieren. Beide Maßnahmen ähneln sich zwar in der Technik der Vorgehensweise. Sie unterscheiden sich allerdings im Inhalt der Daten, die durch den Eingriff in das informationstechnische System erhoben werden. Durch die Quellen-Telekommunikationsüberwachung dürfen ausschließlich Daten eines bereits begonnenen und noch nicht abgeschlossenen Telekommunikationsvorgangs und nicht sonstige, zum Beispiel auf der Festplatte abgelegte, Daten erhoben werden.

Im Unterschied zu Absatz 1 setzt die Quellen-Telekommunikationsüberwachung nach Absatz 3 keine gegenwärtige Gefahr, sondern eine konkrete Gefahr für hochwertige Rechtsgüter voraus. Eine gegenwärtige Gefahr verlangt, dass das schädigende Ereignis bereits begonnen hat oder unmittelbar oder in allernächster Zeit mit an Sicherheit grenzender Wahrscheinlichkeit bevorsteht. Da die technische Vorbereitung einer Quellen-Telekommunikationsüberwachung einige Zeit beansprucht, ist die Maßnahme zur Abwehr gegenwärtiger Gefahren in der Regel ungeeignet. Zur Abwehr konkreter Gefahren ist sie jedoch geeignet und erforderlich. Nach der Entscheidung des Bundesverfassungsgerichts vom 27. Februar 2008 kann der heimliche Zugriff auf ein informationstechnisches System bereits dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen (BVerfG, a. a. O., Absatz Nr. 242). Auch eine konkrete Gefahr genügt damit den Anforderungen der höchstrichterlichen Rechtsprechung.

Satz 1 Nr. 1 erklärt den Eingriff in ein informationstechnisches System zur Durchführung der Maßnahme nur dann für zulässig, wenn sichergestellt ist, dass ausschließlich laufende Telekommunikation erfasst wird. Satz 1 Nr. 2 stellt eine besondere Ausgestaltung des Verhältnismäßigkeitsgrundsatzes dar und nennt mit der Gewährleistung der Aufzeichnung von Telekommunikation in verschlüsselter Form einen der Hauptanwendungsfälle der Maßnahme. Satz 2 erklärt § 31 c Abs. 2 und 4 POG für anwendbar. Satz 3 stellt klar, dass § 31 c POG im Übrigen unberührt bleibt.

Absatz 4 Satz 1 bestimmt wie bisher den Richtervorbehalt. Nach Absatz 4 Satz 2 werden die erforderlichen Inhalte der richterlichen Anordnung, die bislang in § 31 Abs. 5 Satz 4 POG geregelt waren, näher konkretisiert.

Nummer 1 nimmt das Erfordernis auf, in der richterlichen Anordnung die Voraussetzungen und wesentlichen Abwägungsgesichtspunkte der Entscheidung anzugeben.

Nummer 2 berücksichtigt, dass Name und Anschrift der Person, gegen die sich die Maßnahme richtet, nicht stets vollständig bekannt sind. Die Klarstellung zeigt, dass beispielsweise auch gegen unbekannte Verantwortliche, von denen nur Rufnummern und Alias- oder Decknamen bekannt sind, Maßnahmen angeordnet werden können.

Nummer 3 erfordert neben Art, Umfang und Dauer der Datenerhebung nun auch die Benennung des Endzeitpunkts. Die Dauer der Maßnahme ist unter Berücksichtigung der Gefahrenlage und der Erforderlichkeit der Maßnahme zu bestimmen. Die gesetzlichen Fristen stellen dabei lediglich Höchstfristen dar.

Nummer 4 verlangt die Angabe der Rufnummer oder einer anderen Kennung des zu überwachenden Anschlusses oder des Endgeräts. Die Vorschrift orientiert sich an § 100 b Abs. 2 Satz 2 Nr. 2 StPO. Im Vergleich zur bisherigen Rechtslage besteht nunmehr die Möglichkeit, durch die Angabe der Kennung des Endgeräts (IMEI), wenn diese allein dem zu überwachenden Endgerät zuzuordnen ist, eine IMEI-gestützte Überwachung eines Telekommunikationsendgeräts durchzuführen. Die IMEI ist eine eindeutige 15-stellige Seriennummer, anhand derer jedes mobile Telekommunikationsendgerät identifiziert werden kann. IMEI-gestützte Überwachung kommt insbesondere dann in Betracht, wenn die verantwortliche Person über zahlreiche verschiedene Mobilfunkkarten verfügt, die sie abwechselnd zumeist in demselben Mobilfunkgerät einsetzt. Dadurch ändert sich fortwährend die zu überwachende Kennung des Mobilfunkanschlusses und die Zielperson kann die polizeilichen Überwachungsmaßnahmen gezielt unterlaufen. Bislang sind umfangreiche technische und personalintensive Ermittlungen erforderlich, um dennoch die Überwachung fortführen zu können. Ferner muss in diesem Fall des Wechsels der Mobilfunkkarte für jede Rufnummer eine erneute gerichtliche Anordnung beantragt werden. Die IMEI-gestützte Überwachung soll zukünftig die polizeiliche Überwachungsarbeit erleichtern und damit eine möglichst unterbrechungsfreie Überwachung gewährleisten.

Nummer 5 bezieht die Möglichkeit der Quellen-Telekommunikationsüberwachung nach Absatz 3 mit ein und verlangt die möglichst genaue Bestimmung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen wird, sowie des eingesetzten technischen Mittels. Im Hinblick auf das technische Mittel sind in der richterlichen Anordnung zumindest allgemein verständliche Angaben zu dessen Funktionsumfang anzugeben. Eine bloße Benennung des technischen Mittels ist hingegen nicht ausreichend.

Die Sätze 3 und 4 entsprechen dem bisherigen § 31 Abs. 5 Satz 2 und 3 POG.

Absatz 5 regelt die Zuständigkeit des anordnenden Oberverwaltungsgerichts Rheinland-Pfalz und die Anordnungskompetenz bei Gefahr im Verzug. Im Unterschied zur bisherigen Regelung in § 31 Abs. 5 Satz 5 POG tritt an die Stelle der Zuständigkeit des Amtsgerichts die Zuständigkeit des Oberverwaltungsgerichts Rheinland-Pfalz. Insoweit wird auf die Begründung zu Artikel 1 Nr. 15 Buchst. g Doppelbuchst. aa (§ 29 Abs. 6 Satz 1 POG) verwiesen.

Absatz 6 orientiert sich am bisherigen § 31 Abs. 6 POG. Allerdings verpflichtet Satz 1 die Telekommunikations-Diensteanbieter unter den erweiterten Voraussetzungen des Absatzes 1 zur Umsetzung einer Maßnahme nach dieser Vorschrift.

Der Satz 2 stellt nunmehr ausdrücklich klar, dass sich die Anordnungsbefugnis auch auf zukünftig anfallende Verkehrsdaten erstreckt. Die Telekommunikationsdiensteanbieter haben diese Daten im Einzelfall auf Anordnung aufzuzeichnen und der Polizei zu übermitteln.

Satz 3 verweist hinsichtlich der von den Telekommunikations-Diensteanbietern zu treffenden Vorkehrungen allgemein auf das Telekommunikationsgesetz und die darauf beruhenden Rechtsverordnungen. Eine inhaltliche Änderung zur bisherigen Regelung gemäß § 31 Abs. 6 Satz 2 POG ist damit nicht verbunden. Satz 4 übernimmt im Hinblick auf die Entschädigung der Telekommunikations-Diensteanbieter die bisherige Verweisung auf § 12 Abs. 5 POG.

Absatz 7 entspricht inhaltlich dem bisherigen § 31 Abs. 7 POG.

§ 31 a (Identifizierung und Lokalisierung von mobilen Telekommunikationsendgeräten)

Die Vorschrift regelt die polizeiliche Befugnis zum Einsatz technischer Mittel zur Ermittlung spezifischer Kennungen, insbesondere der Geräte- und Kartennummer von mobilen Telekommunikationsendgeräten, und des Standorts eines mobilen Telekommunikationsendgeräts. Die bisherige Befugnis hat seit ihrer Einführung durch das Landesgesetz vom 2. März 2004 (GVBl. S. 202) in der polizeilichen Praxis eine hohe Bedeutung erlangt. Standortfeststellungen zur Rettung von Suizidgefährdeten oder hilflosen Personen, beispielsweise gebrechlichen Personen oder Kindern, stellen heute unverzichtbare polizeiliche Maßnahmen der Lebensrettung dar.

Bislang wurden die Datenerhebungen auf die bisherige Ermächtigung zur Telekommunikationsüberwachung gemäß § 31 Abs. 1 in Verbindung mit Abs. 2 Satz 1 Nr. 3 und 4 POG gestützt. Da die Maßnahmen jedoch im Vergleich zur Überwachung der Telekommunikation gemäß § 31 POG minder schwere Eingriffe in Grundrechte der Betroffenen darstellen, soll dem künftig durch eine bereichsspezifische Regelung Rechnung getragen werden. Ziel der Neuregelung ist es, die Eingriffsschwelle für diese Maßnahmen herabzusenken und die Bestimmung sprachlich neu zu fassen.

Die neu geschaffene Ermächtigung soll nunmehr auch angewandt werden, um Gefahren durch die Begehung von Straftaten von erheblicher Bedeutung abwehren zu können. Der Begriff der Straftat von erheblicher Bedeutung ist in § 28 Abs. 3 POG legal definiert (vgl. hierzu auch die Gesetzesbegründung zum Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes und anderer Gesetze – Landtagsdrucksache 14/2287, S. 44 –). Durch Standortfeststellungen können Bewegungsbilder, insbesondere Reisewege von Zielpersonen ermittelt werden. Zur Gefahrenabwehr benötigt die Polizei auch diese wichtigen Informationen aus der – vor allem bei bandenmäßig oder organisiert handelnden Kriminellen sowie bei terroristischen Gewalttäterinnen und Gewalttätern – zum Teil langwierigen Vorbereitungsphase. Die angefallenen Standortdaten können Reisebewegungen und Trefferörtlichkeiten terroristischer Gewalttäterinnen und Gewalttäter offenbaren und dabei auch Hinweise auf die Ausspähung möglicher Anschlagsziele geben.

Die neue Befugnis steht auch im Einklang mit der Verfassung. Die Frage, ob spezifische Kennungen und Standortdaten, die durch den Einsatz technischer Mittel ermittelt werden, in den Schutzbereich des Fernmeldegeheimnisses gemäß Artikel 10 Abs. 1 des Grundgesetzes fallen, wird seit längerem kontrovers diskutiert. In fachgerichtlichen Entscheidungen (z. B. BGH, Urteil vom 14. März 2003, 2 StR 341/02) wurde das Fernmeldegeheimnis gemäß Artikel 10 Abs. 1 des Grundgesetzes als betroffen angesehen. Das Bundesverfassungsgericht hatte in der Begründung seines Nichtannahmebeschlusses vom 22. August 2006 (2 BvR 1345/03) aus Anlass der Überprüfung des § 100 i StPO festgestellt, dass die Ermittlung des Mobilfunkstandortes sowie der spezifischen Kennungen, wie einer Geräte- und Kartennummer, durch einen IMSI-Catcher nicht in den Schutzbereich des Fernmeldegeheimnisses gemäß Artikel 10 Abs. 1 des Grundgesetzes eingreift. Die Datenerhebung erfasse weder einen Kommunikationsvorgang noch dessen Inhalt, da sie technisch unabhängig von einem versuchten bzw. tatsächlich stattfindenden Gesprächskontakt erfolge. Durch Feststellung der Kennungen derjenigen mobilen Telekommunikationsendgeräte, die in der mittels IMSI-Catcher simulierten Funkzelle eingeloggt sind, werden zwar Rückschlüsse auf den Aufenthaltsort der betroffenen Mobilfunknutzerinnen und Mobilfunknutzer ermöglicht. Dadurch wird auch deren Recht auf informationelle Selbstbestimmung gemäß Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes berührt. Insofern sei die Regelung des § 100 i StPO, so das Bundesverfassungsgericht, jedoch verhältnismäßig (BVerfG, a. a. O., Absatz Nr. 57, 67 und 69). Die Grundsätze dieser Entscheidung sind auf die Ermächtigung zur Gefahrenabwehr übertragbar.

Absatz 1 orientiert sich hinsichtlich der zu erhebenden Daten an der bisherigen Regelung gemäß § 31 Abs. 2 Satz 1 Nr. 3 und 4 POG. Allerdings werden die Begriffe dem im modernen Telekommunikationsrecht üblichen Sprachgebrauch angepasst. Die bisherige Formulierung „Feststellung der Polizei nicht bekannter Telekommunikationsanschlüsse“ wird ersetzt durch den Begriff der „spezifischen Kennungen, insbesondere die Geräte- und Kartennummer von mobilen Telekommunikationsendgeräten“. Erfasst werden hiervon insbesondere die Kartennummer einer SIM-Karte (IMSI: International Mobile Subscriber Identity) und die Gerätenummer (IMEI). Bei der IMSI handelt es sich um eine weltweit eindeutige Kennung, die die Vertragspartnerin oder den Vertragspartner eines Netzbetreibers eindeutig identifiziert und die auf der SIM-Karte gespeichert ist, die der Mobilfunkteilnehmerin oder dem Mobilfunkteilnehmer bei Abschluss des Vertrages ausgehändigt wird. Hinsichtlich der IMEI wird auf die Begründung zu § 31 Abs. 4 Satz 2 Nr. 4 POG verwiesen.

Diese Kennungen werden in Satz 1 beispielhaft genannt, da sie wesentliche Anwendungsfälle der Norm darstellen. Die Kenntnis dieser Kennungen ist Voraussetzung für die Durchführung einer Telekommunikationsüberwachung oder genauen Standortbestimmung eines mobilen Telekommunikationsendgeräts.

Darüber hinaus enthält Satz 1 die Befugnis zur genauen Standortbestimmung eines mobilen Telekommunikationsendgeräts. Der Begriff des mobilen Telekommunikationsendgeräts wird verwendet, um zu verdeutlichen, dass die Standortfeststellung unabhängig von einem aktuellen Telekommunikationsvorgang zulässig ist.

Hinsichtlich der materiellen Voraussetzungen übernimmt Absatz 1 die Anforderungen, die an den Einsatz von besonderen Mitteln der verdeckten Datenerhebung gemäß § 28 Abs. 1 POG gestellt werden. Die Maßnahmen weisen eine vergleichbare Eingriffsintensität auf. So ermächtigt § 28 Abs. 1 in Verbindung mit Abs. 2 Nr. 5 POG zum Einsatz technischer Mittel zur Feststellung des jeweiligen Standortes einer Person oder eines Fahrzeugs. Durch die Observation über das satellitengestützte „Global Positioning System“ (GPS) mittels eines Peilsenders kann auf der Grundlage dieser Ermächtigung auch der Standort eines Fahrzeugs und einer Person bestimmt werden. Erfolgt die Ermittlung des Aufenthaltsortes einer Person über die Standortermittlung eines mobilen Telekommunikationsendgeräts, so ist § 31 a POG Lex specialis gegenüber § 28 Abs. 1 in Verbindung mit Abs. 2 Nr. 5 POG.

In Anspruch genommen werden kann neben den Handlungs- oder Zustandsverantwortlichen auch eine polizeirechtlich nicht verantwortliche Person unter den Voraussetzungen des § 7 POG. Daneben kann die Maßnahme gegen Personen gerichtet werden, bei denen durch Tatsachen begründete Anhaltspunkte die Annahme rechtfertigen, dass sie zukünftig Straftaten von erheblicher Bedeutung begehen werden und die Datenerhebung zur vorbeugenden Bekämpfung derselben erforderlich ist.

Weiterhin können Kontakt- und Begleitpersonen gemäß § 26 Abs. 3 Satz 2 POG in Anspruch genommen werden. Der Verfassungsgerichtshof Rheinland-Pfalz hat in seinem Urteil vom 29. Januar 2007 (VGH B 1/06, S. 37) diesen Begriff als verfassungsgemäß anerkannt. Der Begriff der Kontakt- und Begleitpersonen ist in § 26 Abs. 3 Satz 2 POG legal definiert. Als Kontakt- und Begleitpersonen kommen nur solche Personen in Betracht, die mit einer Straftäterin oder einem Straftäter in der Weise in Verbindung stehen, dass durch Tatsachen begründete Anhaltspunkte für ihren objektiven Tatbezug sprechen. Dies setzt voraus, dass die Kontakt- und Begleitperson in den weiteren Handlungskomplex der Straftatenbegehung einbezogen sein muss (vgl. hierzu auch die Gesetzesbegründung zum Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes und anderer Gesetze – Landtagsdrucksache 14/2287, S. 41 –). Flüchtige oder persönliche Kontakte reichen folglich zur Begründung des objektiven Tatbezugs nicht aus. Die beiden letzten Alternativen sollen insbesondere die Möglichkeit eröffnen, die Maßnahmen auch zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung zu nutzen.

Absatz 2 übernimmt die bisherige Regelung gemäß § 31 Abs. 3 POG und erweitert allerdings den Anwendungsbereich um die Fälle der Standortfeststellung eines mobilen Telekommunikationsendgeräts, da auch bei diesen Maßnahmen Daten Dritter unvermeidbar anfallen. Soweit danach aus technischen Gründen solche Daten erhoben werden, unterliegen diese nach Satz 2 einem Verwendungsverbot. Die Verpflichtung zur Löschung der erhobenen Geräte- und Kartennummern gemäß dem bisherigen § 31 Abs. 3 Satz 2 POG ist nunmehr in § 39 Abs. 2 Satz 1 Nr. 4 POG geregelt.

Nach Absatz 3 Satz 1 besteht ein Richtervorbehalt bei Datenerhebungen nach Absatz 1. Dieser gilt insbesondere auch für die Erstellung von Bewegungsbildern von Verantwortlichen, um Straftaten von erheblicher Bedeutung zu verhindern. Satz 2 enthält neben dem Verweis auf § 21 Abs. 1 Satz 3 einen Verweis auf § 31 Abs. 4 Satz 2 bis 4 POG, sodass diese Regelung im Hinblick auf die Inhalte der schriftlichen Anordnung und die Befristung und Verlängerung der Maßnahmen entsprechend gilt. Nach Satz 3 kann bei Gefahr im Verzug die Maßnahme durch die Behördenleitung angeordnet werden. Die richterliche Anordnung ist jedoch unverzüglich nachzuholen. Von dieser Verpflichtung besteht eine Ausnahme, sofern die Datenerhebung nach Absatz 1 Nr. 1 der Lebensrettung vermisster, suizidgefährdeter oder sonstiger hilfloser Personen dient. Damit wird die bisherige Rechtslage geändert, da bislang auch in diesen Fällen die richterliche Entscheidung nachträglich einzuholen ist. Die polizeiliche Praxis zeigt allerdings, dass die richterliche Anordnung bei Maßnahmen zur Lebensrettung regelmäßig erst nach Beendigung der Maßnahme erlassen wird. Die vorherige richterliche Kontrolle der Maßnahme ist wegen des Zeitablaufs regelmäßig nicht möglich. Aufgrund dieser Erfahrung und der geringen Eingriffsintensität der Maßnahme wird es als gerechtfertigt angesehen, auf die nachträgliche Einholung der richterlichen Anordnung bei Maßnahmen der Lebensrettung zu verzichten. Für die Betroffenen ergibt sich durch den Wegfall des Richtervorbehalts kein bedeutsames Rechtsschutzdefizit, da sie die Maßnahme nachträglich gerichtlich auf ihre Rechtmäßigkeit hin überprüfen lassen können.

Absatz 4 enthält Mitwirkungspflichten der Telekommunikations-Diensteanbieter. Satz 1 ändert die bisherige Rechtslage gemäß § 31 Abs. 6 POG dahingehend, dass die Telekommunikations-Diensteanbieter unter den niedrigeren Anforderungen des Absatzes 1 die erforderlichen spezifischen Kennungen, insbesondere die Geräte- und Kartennummer von mobilen Telekommunikationsendgeräten, oder den Standort des mobilen Telekommunikationsendgeräts der Polizei unverzüglich mitzuteilen haben. Entsprechend der Befugnis gemäß Absatz 1 ist diese Änderung gerechtfertigt, da diese Maßnahmen für die Betroffenen minder schwere Eingriffe darstellen. Bei einer solchen Standortermittlung erhält die Polizei nur die über die Funkzellenauswertung errechneten Positionsdaten. Diese lassen keine Rückschlüsse auf etwaige Kommunikationsbeziehungen bzw. -inhalte zu, sondern geben lediglich Auskunft über die Position des maßgeblichen mobilen Telekommunikationsendgeräts. Daher ist es gerechtfertigt, die Verpflichtung der Telekommunikations-Diensteanbieter auch unter den erleichterten Voraussetzungen des Absatzes 1 zuzulassen. Entsprechendes gilt für die spezifischen Kennungen.

Mit der Anordnung der Auskunft über spezifische Kennungen oder der Standortfeststellung ist ein Eingriff in den Schutzbereich der Berufsfreiheit und der Eigentumsfreiheit der Telekommunikations-Diensteanbieter gemäß Artikel 12 Abs. 1

und Artikel 14 Abs. 1 des Grundgesetzes verbunden. Diese Eingriffe sind jedoch auf der Grundlage des Absatzes 1 und dem Verweis auf die entsprechenden Bestimmungen des Telekommunikationsgesetzes und der darauf beruhenden Rechtsverordnungen zulässig. Solche Mitwirkungspflichten ergeben sich auch nach anderen gesetzlichen Regelungen wie beispielsweise nach § 100 g Abs. 2 Satz 1 in Verbindung mit § 100 b Abs. 3 StPO.

Satz 2 verweist auf Absatz 3 und § 31 Abs. 6 Satz 2 bis 4 POG. Durch den Verweis auf Absatz 3 wird klargestellt, dass für die Verpflichtung zu Auskünften der Telekommunikationsdiensteanbieter die Anordnungsvorbehalte entsprechend gelten. Durch den Verweis auf § 31 Abs. 6 Satz 2 bis 4 POG werden die Pflichten näher ausgestaltet und die Vergütungspflicht für die Leistungen wie bislang bestimmt.

Absatz 5 bestimmt die Zweckänderung der Daten. Diese ist nach Satz 1 zulässig, soweit dies zur Verfolgung von Straftaten von erheblicher Bedeutung gemäß § 28 Abs. 3 POG, zur Abwehr einer dringenden Gefahr oder zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist. Satz 2 regelt das Erfordernis, dass die Zweckänderung im Einzelfall festgestellt und dokumentiert werden muss. Damit soll ein Missbrauch der Zweckänderung ausgeschlossen werden.

§ 31 b (Auskunft über Nutzungsdaten)

Diese Bestimmung verpflichtet die Diensteanbieter zur Auskunft über Nutzungsdaten im Sinne des § 15 Abs. 1 TMG.

Die Telemedien, unter die alle elektronischen Informations- und Kommunikationsdienste fallen, werden in einem immer größeren Umfang von der Bevölkerung zur Kommunikation und Information genutzt. Auskünfte über Nutzungsdaten können somit für die Polizei auch zur Abwehr von Gefahren von großem Nutzen sein. Die Ermächtigung kann beispielsweise bei den zunehmenden Ankündigungen von Amoklagen oder volksverhetzender oder islamistischer Propaganda im Internet Anwendung finden.

Das Telemediengesetz ermöglicht den Sicherheitsbehörden den Zugriff auf Bestands- und Nutzungsdaten von Telemediendiensten auch zum Zweck der Gefahrenabwehr. § 15 Abs. 5 Satz 4 in Verbindung mit § 14 Abs. 2 TMG stellt die Öffnungsklausel für die zweckändernde Nutzung dieser nach dem Telemediengesetz erhobenen Daten dar. Die Bestimmungen des Telemediengesetzes begründen allerdings keine Auskunftspflichten von Diensteanbietern, sodass eine Regelung im jeweiligen Fachgesetz erforderlich ist.

Nach Absatz 1 Satz 1 kann die Polizei Auskunft über Nutzungsdaten im Sinne des § 15 Abs. 1 TMG 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, verlangen. Die Anforderungen entsprechen damit den Voraussetzungen der neu geschaffenen Ermächtigungen gemäß den §§ 31 c und 31 d. Insoweit wird auf die Begründung zu § 31 c POG verwiesen.

Nutzungsdaten im Sinne dieser Vorschrift sind personenbezogene Daten, mit denen die Inanspruchnahme von Telemedien ermöglicht oder mithilfe derer abgerechnet werden kann (vgl. § 15 Abs. 1 TMG). Es handelt sich dabei insbesondere um Merkmale zur Identifikation der Nutzerin oder des Nutzers, Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung und Angaben über die von der Nutzerin oder dem Nutzer in Anspruch genommenen Telemedien. Der Begriff der Telemedien ist dabei weit zu verstehen und umfasst alle elektronischen Informations- und Kommunikationsdienste, es sei denn, es handelt sich um Telekommunikation oder Rundfunk. Von dem Begriff werden beispielsweise Online-Angebote von Waren oder Dienstleistungen mit unmittelbarer Bestellmöglichkeit (insbesondere Internetauktionshäuser oder -tauschbörsen, elektronische Presse und Chatrooms), das Anbieten von Videos auf Abruf oder Suchmaschinen im Internet umfasst. Zu den Merkmalen zur Identifikation der Nutzerin oder des Nutzers von Telemedien gehören beispielsweise IP-Adressen, E-Mail-Adressen und Nutzerkennungen.

Auskunft über Bestandsdaten haben die Diensteanbieter bereits derzeit auf der Grundlage des § 14 Abs. 2 TMG in Verbindung mit § 9 POG zu erteilen. Bestandsdaten gemäß § 14 Abs. 1 TMG sind Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen Anbieter und Nutzerin oder Nutzer erforderlich sind. Bei der Abgrenzung zwischen Bestands- und Nutzungsdaten ist zu berücksichtigen, dass beispielsweise die IP-Adressen, E-Mail-Adressen und Nutzerkennungen abhängig vom Auskunftsersuchen entweder Bestands- oder Nutzungsdaten darstellen können.

Die rechtliche Einordnung der Nutzungsdaten ist bislang umstritten. Unzweifelhaft ist, dass die Auskunft über Nutzungsdaten in das Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes eingreift. Ein Eingriff in den Schutzbereich des Fernmeldegeheimnisses gemäß Artikel 10 Abs. 1 des Grundgesetzes wurde hingegen teilweise abgelehnt, da die Daten nicht im Rahmen des eigentlichen Übertragungsvorgangs erhoben werden (vgl. hierzu BT-Drucksache 16/3078, S. 18; a. A. Dix/Schaar, in: Roßnagel [Hrsg.], Recht der Multimediadienste, § 6 TDDSG RdNr. 200). Ungeachtet dessen stellen die Maßnahmen einen intensiven Grundrechtseingriff dar, da die erhobenen personenbezogenen Daten weitreichende Rückschlüsse auf die Persönlichkeit der verantwortlichen Person zulassen. Die Auskunft an die Polizei darf deshalb nur unter engen Voraussetzungen erfolgen. Damit wird der besonderen Grundrechtsintensität der Maßnahme Rechnung getragen.

Die Sätze 2 und 3 orientieren sich an den Bestimmungen gemäß § 31 Abs. 1 Satz 2 und 3 POG.

Nach Satz 4 kann die Auskunft auch für die Zukunft verlangt werden. Diese Regelung ist notwendig, da die Vorschrift nicht als Erhebungsbefugnis ausgestaltet ist.

Absatz 2 Satz 1 bestimmt, gegen wen sich die Anordnung zur Auskunft richten kann. Zur Auskunft über Nutzungsdaten werden danach die Diensteanbieter verpflichtet, die geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln.

Absatz 2 Satz 2 verweist auf § 31 Abs. 4 und 5 POG. Danach gelten die Bestimmungen zum Richtervorbehalt, zur Eilkompetenz und zur Zuständigkeit des Oberverwaltungsgerichts Rheinland-Pfalz entsprechend. Zur Zuständigkeit des

Oberverwaltungsgerichts Rheinland-Pfalz wird auf die Begründung zu Artikel 1 Nr. 15 Buchst. g Doppelbuchst. aa (§ 29 Abs. 6 Satz 1 POG) verwiesen.

Absatz 3 Satz 1 regelt, wie diese Daten an die Polizei zu übermitteln sind. Der Verweis in Satz 2 auf § 12 Abs. 5 POG legt fest, dass die Leistungen der Diensteanbieter von der Polizei zu vergüten sind.

Absatz 4 bestimmt, dass die Kennzeichnungspflicht für die übermittelten Daten sowie die Regelung zur Zweckänderung gemäß § 29 Abs. 5 POG entsprechend gelten.

§ 31 c (Datenerhebung durch den Einsatz technischer Mittel in informationstechnischen Systemen)

Die neu eingefügte Vorschrift bildet die polizeiliche Ermächtigung zum verdeckten Zugriff auf informationstechnische Systeme. In den letzten Jahren haben die modernen Kommunikations- und Informationstechnologien eine rasante Entwicklung genommen und werden von der Bevölkerung zunehmend in allen Lebensbereichen genutzt. Sie sind geprägt durch einen nahezu grenzenlosen Speicherumfang, Schnelligkeit der Informationsverarbeitung und eine Vielfalt von Nutzungsmöglichkeiten. Sie bieten auch potenziellen Straftäterinnen und Straftätern, insbesondere terroristischen Vereinigungen, eine Vielzahl von Möglichkeiten, um sie für ihre Zwecke zu missbrauchen. Die Arbeit der Sicherheitsbehörden wird folglich immer stärker von den neuen Technologien bestimmt.

Das Internet wird von islamistischen Extremistinnen und Extremisten zur Verbreitung ihrer Propaganda oder zur Androhung von Terroranschlägen genutzt. Detaillierte Bombenanleitungen werden für jeden zugänglich im Internet eingestellt. Einschlägige Foren und Tauschbörsen werden von Pädophilen zur Vorbereitung des sexuellen Missbrauchs von Kindern sowie zur Vorbereitung inkriminierter kinderpornografischer Darstellungen genutzt. Es besteht die Gefahr, dass die bisherigen polizeilichen Standardmaßnahmen, wie Sicherstellung und Auswertung von Computern, künftig ins Leere laufen. Insbesondere der Fortschritt auf dem Gebiet der Verschlüsselungstechniken bereitet zum Teil unüberwindbare Hindernisse bei der Datenauswertung. Den Sicherheitsbehörden wird so der Zugriff auf bedeutsame Informationen zur Gefahrenabwehr erschwert oder dieser vollständig ausgeschlossen, indem beispielsweise Daten verschlüsselt oder auf fremde Speicher ausgelagert werden können.

Für die erfolgreiche Gefahrenabwehr ist es daher erforderlich, dass die Methoden der Sicherheitsbehörden mit den technischen Möglichkeiten von Verantwortlichen Schritt halten. Damit die Sicherheitsbehörden auch zukünftig ihre Aufgaben der Gefahrenabwehr und Verhütung von Straftaten wahrnehmen können, benötigen sie Befugnisse, um die neuen Technologien im Bereich der Informationstechnik einsetzen zu können.

Das Bundesverfassungsgericht hat in seinem Urteil zur Online-Durchsuchung vom 27. Februar 2008 (1 BvR 370/07 und 1 BvR 595/07) die Zulässigkeit einer solchen Befugnis unter strengen Vorgaben zu Zwecken der Gefahrenabwehr oder Strafverfolgung anerkannt. Es weist in der Urteilsbegründung darauf hin, dass die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit Verfassungswerte sind, die mit anderen hochwertigen Rechtsgütern im gleichen Rang stehen. Dieser Pflicht zum Schutz seiner Bürgerinnen und Bürger kommt der Staat nach, indem er die polizeilichen Befugnisse den technischen Entwicklungen anpasst (BVerfG, a. a. O., Absatz Nr. 220).

Die neu geschaffene Befugnis steht im Einklang mit den verfassungsrechtlichen Anforderungen. Sie beachtet die Voraussetzungen zum Schutz des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Dieses Grundrecht leitete das Bundesverfassungsgericht in seiner Entscheidung vom 27. Februar 2008 aus dem allgemeinen Persönlichkeitsrecht gemäß Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes ab.

Das Bundeskriminalamt hat eine solche Befugnis zur Online-Durchsuchung durch das Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008 (BGBl. I S. 3083) erhalten. Die Befugnisse der Länder zur Gefahrenabwehr bleiben jedoch gemäß § 4 a Abs. 2 Satz 1 BKAG ausdrücklich unberührt, sodass auch die Länder entsprechende Ermächtigungen zum verdeckten Zugriff auf informationstechnische Systeme benötigen.

Absatz 1 benennt die materiellen Voraussetzungen der Maßnahme und orientiert sich dabei an der Befugnis zur Wohnraumüberwachung gemäß § 29 POG sowie an der Befugnis zur Telekommunikationsüberwachung gemäß § 31 POG. Damit wird den Vorgaben des Bundesverfassungsgerichts in dem oben genannten Urteil Rechnung getragen. Das vom Schutz des allgemeinen Persönlichkeitsrechts gemäß Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes umfasste Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme wird vor staatlichen Eingriffen geschützt, soweit der Schutz nicht durch andere Grundrechte gewährleistet ist, insbesondere das Fernmeldegeheimnis oder das Grundrecht auf Unverletzlichkeit der Wohnung sowie das Recht auf informationelle Selbstbestimmung (BVerfG, a. a. O., Absatz Nr. 167).

Das Bundesverfassungsgericht hat in der Entscheidung ausgeführt, dass in den Schutzbereich dieses Grundrechts eingegriffen werden darf, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. Überragend wichtig sind Leib, Leben, Freiheit der Person sowie solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt (BVerfG, a. a. O., Absatz Nr. 247).

Die Voraussetzungen in Satz 1 übernehmen diese verfassungsrechtlichen Vorgaben. Neben den hochrangigen Individualrechtsgütern wie Leib, Leben und Freiheit der Person, werden auch die Rechtsgüter der Allgemeinheit geschützt. Dieser Schutz ist allerdings auf existenzielle Bedrohungslagen begrenzt. Zu den zu schützenden Rechtsgütern zählt etwa die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen (BVerfG, a. a. O., Absatz Nr. 247). Nicht ausreichend für eine solche Maßnahme sind hingegen bloße Gefahren für Vermögenswerte.

Die Befugnis setzt das Bestehen einer konkreten Gefahr für ein überragend wichtiges Rechtsgut voraus. Die Polizei ist insbe-

sondere nicht zu Maßnahmen im Gefahrenvorfeld berechtigt. Andererseits fordert diese Ermächtigung nicht eine besondere zeitliche Nähe zum Gefahreneintritt, da die Maßnahme wegen ihrer technischen Vorbereitungsmaßnahmen regelmäßig nur in den Fällen eingesetzt werden kann, in denen keine zeitlich akute Gefahrensituation vorliegt.

Die Regelung zu den verantwortlichen Personen übernimmt die entsprechende Bestimmung gemäß § 31 Abs. 1 POG. Damit kann auch die Nachrichtenmittlerin oder der Nachrichtenmittler in Anspruch genommen werden.

Eingriffshandlung ist die ohne Wissen der verantwortlichen Person erfolgte Datenerhebung aus informationstechnischen Systemen. Der Begriff des informationstechnischen Systems entspricht § 2 Abs. 2 Nr. 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) vom 14. August 2009 (BGBl. I S. 2821) und ist bewusst weit gewählt, um alle nach der Rechtsprechung des Bundesverfassungsgerichts schutzbedürftigen informationstechnischen Systeme zu erfassen (vgl. BVerfG, a. a. O., Absatz Nr. 203). Darunter fallen beispielsweise mobile oder fest installierte Personalcomputer und solche Mobiltelefone und elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können.

Das Erheben von personenbezogenen Daten umfasst die bloße Sichtung, aber auch das Kopieren von Datenbeständen unter Belassung der Datenbestände auf dem Zielsystem. Die Daten können dabei sowohl im Arbeitsspeicher gespeichert als auch temporär oder dauerhaft auf den Speichermedien des Systems abgelegt sein (BVerfG, a. a. O., Absatz Nr. 205). Umfasst wird auch der Einsatz sogenannter Key-Logger, bei denen die Tastatureingaben erfasst werden, ohne dass notwendigerweise eine Zwischenspeicherung auf der Festplatte erfolgt.

Satz 2 normiert zusätzliche Anforderungen an die Maßnahme. Als Konkretisierung des Verhältnismäßigkeitsgrundsatzes wird bestimmt, dass die Maßnahme nur durchgeführt werden darf, wenn sie für die Aufgabenerfüllung nach Satz 1 auf andere Weise nicht möglich erscheint oder wesentlich erschwert wäre. Damit ist die Verhältnismäßigkeit der Maßnahme besonders zu belegen. Zu prüfen ist beispielsweise in diesem Zusammenhang, ob nicht bereits eine offene Sicherstellung zur Aufgabenerfüllung ausreichend ist. Ferner wird durch den Verweis auf die Voraussetzungen des § 39 a Abs. 3 POG klargestellt, dass die Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung zu beachten sind.

Nach Absatz 2 hat die Polizei bei der Durchführung der Maßnahme bestimmte technische Schutzvorkehrungen zu treffen, um den Eingriff in das informationstechnische System auf das unbedingt erforderliche Mindestmaß zu begrenzen und die Datensicherheit zu gewährleisten.

Satz 1 Nr. 1 bestimmt, dass beim Einsatz des technischen Mittels sicherzustellen ist, dass an dem informationstechnischen System nur solche Veränderungen vorgenommen werden, die für die Datenerhebung unbedingt erforderlich sind. Zu schützen sind dabei nicht nur die von der Nutzerin oder dem Nutzer des informationstechnischen Systems angelegten Anwenderdateien, sondern auch die für die Funktion des informationstechnischen Systems erforderlichen Systemdateien. Auch Beeinträchtigungen der Systemleistung sind auf das technisch Unvermeidbare zu begrenzen. Der Nachweis, dass diese Anforderung sichergestellt wird, erfolgt durch die elektronische Signatur des technischen Mittels, mit dem in das informationstechnische System eingegriffen wird. Die elektronische Signatur identifiziert das technische Mittel sowie dessen Funktionsumfang. Die Versionsbezeichnung und die Prüfsummen der elektronischen Signatur sind nach Absatz 4 Satz 1 Nr. 1 zu protokollieren.

Nach Satz 1 Nr. 2 sind bei Beendigung der Maßnahme alle an dem infiltrierten System vorgenommenen Veränderungen rückgängig zu machen, soweit dies technisch möglich ist. Insbesondere ist die auf dem informationstechnischen System installierte Überwachungssoftware vollständig zu löschen und sind Veränderungen an den bei der Installation der Überwachungssoftware vorgefundenen Systemdateien rückgängig zu machen. Die Rückgängigmachung der vorgenommenen Veränderungen hat im Interesse einer möglichst zuverlässigen und einfachen Abwicklung grundsätzlich automatisiert zu geschehen. Soweit eine automatisierte Rückgängigmachung technisch unmöglich ist, sind die vorgenommenen Veränderungen, sofern die Möglichkeit besteht, manuell rückgängig zu machen.

Satz 2 bestimmt in Anlehnung an § 14 Abs. 1 der Telekommunikations-Überwachungsverordnung (TKÜV) vom 3. November 2005 (BGBl. I. S. 3136), zuletzt geändert durch Artikel 4 des Gesetzes vom 25. Dezember 2008 (BGBl. I S. 3083), dass das eingesetzte technische Mittel nach dem Stand der Technik gegen unbefugte Nutzung zu schützen ist. Insbesondere hat die Polizei dafür Sorge zu tragen, dass die eingesetzte Software nicht durch Dritte (Hacker) zweckentfremdet werden kann. Speziell ist sicherzustellen, dass die Software nicht ohne erheblichen Aufwand dazu veranlasst werden kann, an einen anderen Server als den von der Polizei verwendeten zurückzumelden, und dass die Software weder von Unbefugten erkannt noch angesprochen werden kann. Ebenso wie Absatz 2 Satz 1 soll auch Satz 2 gewährleisten, dass die Eingriffe in die Integrität des informationstechnischen Systems und die Vertraulichkeit der in ihm gespeicherten Daten nicht über das hinausgehen, was nötig ist, um der Polizei die Datenerhebung zu ermöglichen. Die Verpflichtung, das eingesetzte Mittel „nach dem Stand der Technik“ gegen unbefugte Nutzung zu schützen, bedeutet, dass sich die Polizei fortschrittlicher technischer Verfahren bedienen muss, die auf gesicherten Erkenntnissen von Wissenschaft und Technik beruhen. Dieses Schutzniveau entspricht den Schutzanforderungen, die nach § 14 Abs. 1 TKÜV für Telekommunikations-Überwachungsmaßnahmen gelten.

Satz 3 schützt in Anlehnung an § 14 Abs. 2 Satz 1 TKÜV die Integrität und Authentizität der von dem technischen Mittel zum Zweck der Ausleitung an die Polizei bereitgestellten Daten (Kopien von Dateien, Protokolle von Tastatureingaben) vom Zeitpunkt der Bereitstellung für die Übertragung an die Polizei, während der Datenübertragung an die Polizei sowie während ihrer Speicherung bei der Polizei. Dies dient sowohl dem Schutz der betroffenen Personen davor, dass die auf dem Zielrechner vorgefundenen Daten nachträglich zufällig oder bewusst (zu ihrem Nachteil) verändert werden oder Unbefugten zur Kenntnis gelangen, als auch dem behördlichen Interesse an der Beweissicherheit der polizeilichen Erkenntnisse. Die Daten sind vor ihrer Übertragung an die Polizei zu ver-

schlüsseln und bei der Polizei beweissicher zu speichern, insbesondere mit einer elektronischen Signatur und einem elektronischen Zeitstempel zu versehen.

Absatz 3 normiert die Befugnis zum Einsatz von technischen Mitteln zur Identifikation und Lokalisation von informationstechnischen Systemen. Unter spezifischen Kennungen sind z. B. IP- oder Mac-Adressen zu verstehen, die es für die Polizei technisch erst möglich machen, auf die zur Gefahrenabwehr notwendigen gespeicherten Daten zuzugreifen. Diese Regelung ist angesichts der Entwicklung auf dem Gebiet der Informationstechnik erforderlich, da zunehmend informationstechnische Systeme eingesetzt werden, deren spezifische Kennungen der Polizei nicht bekannt sind. Die Spezifizierung der informationstechnischen Systeme ist allerdings im Regelfall Voraussetzung für die Durchführung der Maßnahme nach Absatz 1. Gleiches gilt für die Bestimmung des Standortes eines informationstechnischen Systems. Der Einsatz von Geräten, wie etwa des sogenannten WLAN-Catchers zur Bestimmung von spezifischen Kennungen bzw. des Standortes eines informationstechnischen Systems, wird an die strengen Voraussetzungen des Absatzes 1 geknüpft, da er in der Regel zur Vorbereitung einer dort genannten Maßnahme dient. Soweit aus technischen Gründen unvermeidbar Daten Dritter erhoben werden, sind diese nach der neu geschaffenen Vorschrift gemäß § 39 Abs. 2 Satz 1 Nr. 4 POG zu löschen.

Absatz 4 enthält Vorschriften über die Protokollierung der Maßnahmen. Diese Verfahrensvorschriften dienen der Gewährleistung eines effektiven Grundrechtsschutzes der betroffenen Person. Insbesondere ermöglicht die Protokollierung den Nachweis, dass die Daten tatsächlich von dem betroffenen informationstechnischen System stammen und weder absichtlich noch unabsichtlich verändert worden sind. Satz 1 bestimmt, worauf sich die Protokollierung im Einzelnen zu erstrecken hat. Nach Satz 1 Nr. 1 sind zunächst die Bezeichnung des eingesetzten technischen Mittels und der Zeitpunkt seines Einsatzes zu dokumentieren. Die Regelung verlangt allgemein verständliche Angaben zum Funktionsumfang des eingesetzten Mittels. Zu dokumentieren sind dessen Versionsbezeichnung und die Prüfsummen der elektronischen Signatur, mit der das technische Mittel zu versehen ist. Diese Angaben sollen z. B. der betroffenen Person oder einem Gericht die Beurteilung ermöglichen, ob die in der Anordnung der Maßnahme bestimmten Vorgaben hinsichtlich der Art der Maßnahme gemäß Absatz 5 Satz 2 Nr. 3 beachtet worden sind. Ferner ist in jedem Fall anzuzeigen,

- ob es sich um ein Mittel zur einmaligen Durchsicht oder um ein Mittel zur kontinuierlichen Überwachung des Zielrechners handelt,
- ob nur der Zielrechner selbst oder auch an den Zielrechner angeschlossene Speichermedien durchsucht werden,
- ob nur gespeicherte Daten kopiert oder auch Tastatureingaben protokolliert werden.

Nach Satz 1 Nr. 2 sind zum einen Angaben zur Identifizierung des infiltrierten informationstechnischen Systems und zum anderen alle an dem System vorgenommenen nicht lediglich flüchtigen Veränderungen zu protokollieren. Da es kein einzelnes Merkmal gibt, das ein informationstechnisches System eindeutig identifiziert, wird es zur konkreten Individualisierung erforderlich sein, eine Vielzahl von Informationen über die Hard- und Software zu dokumentieren, die das informationstechnische System so genau beschreiben, dass es keine ernsthaften Zweifel daran geben kann, dass Gegenstand der Maßnahme tatsächlich das in der Anordnung nach Absatz 5 Satz 1 Nr. 4 bezeichnete System war. Da jede aktive Software ständig eine Fülle vorübergehender Veränderungen des informationstechnischen Systems vornimmt, die für die Revisionssicherheit irrelevant sind und vielfach schon nach kurzer Zeit (z. B. beim vollständigen Herunterfahren des PC) automatisiert gelöscht werden, bestimmt Satz 1 Nr. 2, dass flüchtige Veränderungen nicht protokolliert werden müssen. Der Begriff „flüchtige Veränderungen“ ist eng auszulegen. „Flüchtige Veränderungen“ sind nur solche, die im Arbeitsspeicher (RAM) gespeichert werden.

Satz 1 Nr. 3 verlangt eine Protokollierung von Angaben, die die Feststellung der erhobenen Daten ermöglichen. Zu protokollieren sind also nicht die erhobenen Daten selbst, sondern lediglich Metadaten, die zuverlässige Rückschlüsse auf die erhobenen Daten erlauben. Von den Protokolldaten darf jedoch kein Rückschluss auf den Inhalt der erhobenen Daten möglich sein. Solche Metadaten sind beispielsweise die in den Dokumenteneigenschaften enthaltenen Angaben (Name der Datei, Versionsnummer, Zeitpunkt der letzten Änderung, Größe der Datei).

Nach Satz 1 Nr. 4 ist schließlich zu dokumentieren, welche Organisationseinheit der Polizei die Maßnahme durchführt.

Satz 2 normiert eine strenge Zweckbindung der Protokolldaten. Die Daten dürfen nur verwendet werden, um einer dazu befugten Behörde (Rechtsaufsichtsbehörde, Landesbeauftragte oder Landesbeauftragter für den Datenschutz), einem dazu befugten Gericht oder der betroffenen Person im Rahmen ihres Auskunftsanspruchs die Prüfung der rechtmäßigen Durchführung der Maßnahme zu ermöglichen. Absatz 4 Satz 2 führt kein neuartiges Prüfungsrecht der betroffenen Person ein, sondern setzt ein bestehendes Recht, wie es sich beispielsweise aus dem allgemeinen Auskunftsanspruch gemäß § 40 Abs. 1 POG ergibt, voraus.

Satz 3 regelt die Aufbewahrung und Löschung der Protokolldaten. Die Daten dürfen nur für die in Satz 2 genannten Zwecke aufbewahrt werden und sind unverzüglich zu löschen, wenn diese Zwecke nicht mehr erfüllt werden können. Durch diese Regelung soll sichergestellt werden, dass die Protokolldaten bei Überprüfung der Rechtmäßigkeit der Maßnahme vorhanden sind. Da eine allgemein festgelegte Aufbewahrungsfrist nicht stets den Anforderungen des Einzelfalls Rechnung tragen kann, wurde darauf verzichtet. Die Löschung der Protokolldaten beurteilt sich somit ausschließlich nach der Erforderlichkeit der Daten.

Absatz 5 bestimmt einen Richtervorbehalt für Maßnahmen nach dieser Vorschrift. Durch die Kontrolle einer unabhängigen und neutralen Instanz wird der Grundrechtsschutz zusätzlich abgesichert (BVerfG, a. a. O., Absatz Nr. 257 ff.). Die inhaltlichen Anforderungen orientieren sich an der entsprechenden Bestimmung zur Telekommunikationsüberwachung gemäß § 31 Abs. 4 POG. Wie bei der Quellen-Telekommunikationsüberwachung ist gemäß Satz 2 Nr. 4 möglichst genau das informationstechnische System, in das zur Datenerhebung eingegriffen wird, sowie das technische Mittel zu bestimmen. Satz 3 bestimmt das Oberverwaltungsgericht Rheinland-Pfalz als das für die Anordnung der Maßnahme zuständige Gericht.

Zu dessen Zuständigkeit wird auf die Begründung zu Artikel 1 Nr. 15 Buchst. g Doppelbuchst. aa (§ 29 Abs. 6 Satz 1 POG) verwiesen. Die richterliche Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Die zulässige Höchstdauer der Frist berücksichtigt, dass die Schaffung der technischen Voraussetzungen einen längeren Zeitraum in Anspruch nehmen kann. Da es sich um eine Bestimmung der Höchstdauer handelt, kann das anordnende Gericht je nach Lage des Einzelfalls die Maßnahme auch für eine kürzere Frist anordnen. Auf eine Eilfallregelung wird aufgrund des zeitlichen Vorlaufs für die technische Vorbereitung der Maßnahme verzichtet.

Absatz 6 verweist auf § 29 Abs. 5 und 8 POG. Es gelten somit die Kennzeichnungspflicht für die erhobenen Daten und die Regelung zur Zweckänderung gemäß § 29 Abs. 5 POG entsprechend. Eine Zweckänderung ist damit nur unter engen Voraussetzungen zulässig. Zwar steht derzeit einer Zweckänderung durch Verwendung zur Strafverfolgung die Vorschrift des § 161 Abs. 2 StPO entgegen. Danach dürfen die nach anderen Gesetzen als der Strafprozessordnung erlangten personenbezogenen Daten ohne Einwilligung der von der Maßnahme betroffenen Person zu Beweiszwecken im Strafverfahren nur zur Aufklärung solcher Straftaten verwendet werden, zu deren Aufklärung eine solche Maßnahme nach der Strafprozessordnung hätte angeordnet werden können. Da die Strafprozessordnung eine solche Ermächtigung zum verdeckten Zugriff auf informationstechnische Systeme nach der derzeitigen Rechtslage nicht vorsieht, läuft insoweit die Bestimmung zur Zweckänderung leer. Allerdings hat das Bundesverfassungsgericht in seinem Urteil vom 27. Februar 2008 (BVerfG, a. a. O., Absatz Nr. 207 ff.) eine solche Befugnis zu Zwecken der Strafverfolgung nicht ausgeschlossen, sodass mit einer entsprechenden Befugnis in naher Zukunft zu rechnen ist.

Ferner legt der Verweis auf § 29 Abs. 8 POG fest, dass für Maßnahmen nach dieser Vorschrift die Berichtspflicht der Landesregierung gegenüber dem Landtag gilt. Obwohl das Bundesverfassungsgericht in seiner Entscheidung zur Online-Durchsuchung vom 27. Februar 2008 eine solche parlamentarische Kontrolle nicht gefordert hat, wird diese aufgrund der Eingriffsintensität der Maßnahme als angemessen angesehen.

§ 31 d (Unterbrechung oder Verhinderung der Telekommunikation)

Die Ermächtigung befugt die Polizei, Telekommunikationsverbindungen zu unterbrechen oder zu verhindern, um dadurch Gefahren für hochrangige Rechtsgüter abwehren zu können.

Die Maßnahmen greifen in das Grundrecht der allgemeinen Handlungsfreiheit gemäß Artikel 2 Abs. 1 des Grundgesetzes ein, das Betätigungen jeder Art schützt. Ob das Fernmeldegeheimnis gemäß Artikel 10 des Grundgesetzes betroffen ist, ist zwar umstritten, aber selbst wenn man davon ausginge, dass auch die Unterbrechung einer Telekommunikationsverbindung dem Schutzbereich des Art. 10 des Grundgesetzes unterfällt, wäre der Eingriff verfassungsrechtlich gerechtfertigt, da er nur unter restriktiven Voraussetzungen zulässig ist.

Die Vorschrift befugt die Polizei zum Einsatz technischer Mittel, wie etwa des sogenannten IMSI-Catchers, um die Telekommunikation zu unterbrechen oder zu verhindern. Nicht erfasst sind hingegen Anordnungen gegenüber den Telekommunikations-Diensteanbietern zur Unterbrechung des Telekommunikationsverkehrs.

Absatz 1 Satz 1 fordert als Voraussetzung eine 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 Anforderungen entsprechen somit den Voraussetzungen eines Zugriffs auf ein informationstechnisches System gemäß § 31 c Abs. 1 POG (vgl. die Begründung zu § 31 c Abs. 1 POG). Die Befugnis kann beispielsweise bei einer Geiselnahme Anwendung finden, um die Kommunikation der Geiselnehmerin oder des Geiselnehmers mit Komplizinnen und Komplizen außerhalb des Tatorts über Mobiltelefone zu unterbinden oder zu verhindern.

Die Maßnahme kann in vielen Fällen auch Dritte, gänzlich unbeteiligte Personen, betreffen, wenn diese mit der betroffenen Person telefonieren oder auch nur versuchen, mit ihr telefonisch Kontakt aufzunehmen. Diese Eingriffe sind nach Absatz 1 Satz 2 als unvermeidbar hinzunehmen, da die Maßnahme der Abwehr einer Gefahr für hochrangige Rechtsgüter dient.

Absatz 2 regelt den Fall, dass die Polizei keine Kenntnis von der Rufnummer oder einer anderen Kennung des betreffenden Anschlusses oder des Endgeräts besitzt. Die Norm findet insbesondere bei Sprengstofffallen Anwendung, wenn lediglich bekannt ist, dass sich in einem bestimmten Gebiet eine Bombe befindet, die ferngesteuert über ein Mobilfunkgerät gezündet werden soll. Die Anschläge von Madrid im März 2004 haben gezeigt, dass vor allem terroristische Organisationen solche modernen Kommunikationstechniken zur Begehung von Anschlägen nutzen. Da die Maßnahmen zur Unterbrechung der Telekommunikationsverbindungen einer Vielzahl von Unbeteiligten führen können, sind sie nur zulässig, sofern sonst die Erreichung des Zwecks der Maßnahme nach Absatz 1 erheblich erschwert wäre.

Absatz 3 stellt die Anordnung und Durchführung der Maßnahmen unter den Vorbehalt der richterlichen Anordnung und verlangt die Befristung der Maßnahme. Satz 2 entspricht dabei der Bestimmung gemäß § 31 Abs. 4 Satz 2 Nr. 1 bis 4 POG. Satz 2 Nr. 5 berücksichtigt, dass im Fall des Absatzes 2 die Rufnummer oder eine andere Kennung des Anschlusses oder des Endgeräts nicht benannt werden kann. Anstelle dessen sind in der richterlichen Anordnung möglichst genau die Kommunikationsverbindungen räumlich und zeitlich zu bestimmen, die unterbrochen oder verhindert werden sollen. Satz 3 legt als zuständiges Gericht das Oberverwaltungsgericht Rheinland-Pfalz fest. Zur Begründung dieser Zuständigkeit wird auf Artikel 1 Nr. 15 Buchst. g Doppelbuchst. aa (§ 29 Abs. 6 Satz 1 POG) verwiesen. Satz 5 enthält eine Eilbefugnis bei Gefahr im Verzug. Satz 6 befristet die Maßnahme auf höchstens 24 Stunden, wobei jedoch die Maßnahme nach Satz 7 verlängert werden kann.

§ 31 e (Funkzellenabfrage)

Die Vorschrift regelt bereichsspezifisch die Funkzellenabfrage.

Darunter ist das Verlangen der Sicherheitsbehörden gegenüber Telekommunikations-Diensteanbietern nach Auskunft über Verkehrsdaten zu verstehen, die in einer bestimmten räumlich bezeichneten Funkzelle in einem bestimmten Zeitraum anfallen.

Absatz 1 bestimmt die materiellen Voraussetzungen der Funkzellenabfrage und nimmt insoweit Bezug auf § 31 Abs. 1 POG. Die Besonderheit der Regelung besteht darin, dass sie von dem Erfordernis, bei der Erhebung von Verkehrsdaten die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts anzugeben, absieht. Dagegen entbindet sie nicht von der Voraussetzung, dass sich die Anordnung zur Verkehrsdatenerhebung nur gegen die Verantwortlichen nach § 31 Abs. 1 POG richten darf. Ziel der Maßnahme ist die Auskunft über Verkehrsdaten der – wenn auch noch unbekannten – verantwortlichen Person. Die Polizei hat bei der Funkzellenabfrage die Möglichkeit, die Verkehrsdaten aller Personen zu erlangen, die in einer bestimmten Funkzelle zur angegebenen Zeit mittels eines Mobiltelefons kommuniziert haben. Durch Auswertung können dann die Daten über die Zielperson ermittelt werden. Da durch die Funkzellenabfrage regelmäßig in unvermeidbarer Weise auch Verkehrsdaten Dritter erhoben werden, die in der Funkzelle zur angegebenen Zeit mittels Mobiltelefon kommunizieren, kommt der Verhältnismäßigkeit der Maßnahme eine besondere Bedeutung zu. Aus Gründen der Verhältnismäßigkeit darf die Maßnahme nur durchgeführt werden, sofern anderenfalls die Erreichung des Zwecks der Maßnahme erheblich erschwert wäre. Zweck der Maßnahme ist die Abwehr der in § 31 Abs. 1 POG genannten Gefahren. Die Daten von unbeteiligten Dritten sind nach der allgemeinen Regelung gemäß § 39 Abs. 2 Satz 1 Nr. 4 POG zu löschen, wenn sie nicht mehr erforderlich sind.

Absatz 2 enthält Verweisungen auf Bestimmungen dieses Gesetzes. Durch den Verweis auf Bestimmungen zur Telekommunikationsüberwachung gemäß § 31 POG wird die Nähe dieser Maßnahme zur Telekommunikationsüberwachung deutlich. Nach Satz 1 gelten die Vorschriften zum Richtervorbehalt gemäß § 31 Abs. 4 POG entsprechend. Allerdings wird berücksichtigt, dass in der schriftlichen Anordnung der Funkzellenabfrage die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts nicht angegeben werden kann. Stattdessen ist in der schriftlichen Anordnung die Telekommunikation räumlich und zeitlich zu bestimmen, über die Verkehrsdaten erhoben werden soll. Satz 2 verweist auf die Zuständigkeit des Oberverwaltungsgerichts Rheinland-Pfalz und die Eilkompetenz gemäß § 31 Abs. 5 POG. Zur Begründung der Zuständigkeit des Oberverwaltungsgerichts Rheinland-Pfalz wird auf Artikel 1 Nr. 15 Buchst. g Doppelbuchst. aa (§ 29 Abs. 6 Satz 1 POG) verwiesen. Durch die Verweisung auf § 31 Abs. 6 Satz 2 bis 4 POG wird zudem die Verpflichtung der Diensteanbieter zur Auskunft näher konkretisiert. Ferner gilt die Bestimmung gemäß § 29 Abs. 5 POG zur Zweckänderung der erhobenen Daten entsprechend.

Zu Nummer 17 (§ 32)

Zu Buchstabe a

In Absatz 2 werden die Voraussetzungen an die Übermittlung von Erkenntnissen bei einer polizeilichen Beobachtung neu geregelt. Die bisherige Regelung wird erweitert, sodass bei einer Kontrollmeldung auch Erkenntnisse über etwaige Begleiterinnen oder Begleiter der ausgeschriebenen Person an die ausschreibende Behörde übermittelt werden dürfen. Die bisherige Begrenzung auf Kontakt- und Begleitpersonen gemäß § 26 Abs. 3 Satz 2 POG entfällt, da im Regelfall im Zeitpunkt der Übermittlung noch nicht festgestellt werden kann, ob die Begleiterin oder der Begleiter der ausgeschriebenen Person auch eine Kontakt- und Begleitperson nach der gesetzlichen Bestimmung ist. Die Ermächtigung erlaubt nun, Erkenntnisse über etwaige Begleiterinnen oder Begleiter zu übermitteln, um zu überprüfen, ob diese Personen Kontakt- und Begleitpersonen sind. Ist dies nicht der Fall, sind die erhobenen Erkenntnisse nach § 39 Abs. 2 Satz 1 Nr. 4 POG zu löschen.

Zu Buchstabe b

Zu Doppelbuchstabe aa

Nach Absatz 3 Satz 2 in seiner bisherigen Fassung ist die polizeiliche Beobachtung auf höchstens zwölf Monate zu befristen und kann wiederholt angeordnet werden. Die Befugnis zur wiederholten Anordnung der Maßnahme wird aufgehoben, da die Verlängerung der Maßnahme nunmehr in dem neu angefügten Satz 3 geregelt wird.

Zu Doppelbuchstabe bb

Der in Absatz 3 neu angefügte Satz 3 legt fest, dass eine Verlängerung der Maßnahme um jeweils nicht mehr als denselben Zeitraum, also um höchstens zwölf Monate, zulässig ist, sofern die Voraussetzungen der Anordnung vorliegen. Nach Satz 4 bedarf die Verlängerung der Maßnahme einer richterlichen Entscheidung. Durch die Einführung des Richtervorbehalts für polizeiliche Beobachtungen, die über einen Zeitraum von mehr als zwölf Monaten durchgeführt werden, wird der mit der zeitlichen Dauer einhergehenden Eingriffsintensität der Maßnahme Rechnung getragen.

Zu Buchstabe c

Die Bestimmung zur Beendigung der Maßnahme und Löschung der Ausschreibung wird aufgehoben, da ihr Regelungsinhalt bereits in der allgemeinen Vorschrift gemäß § 2 Abs. 3 POG enthalten ist. Diese Bestimmung gilt für sämtliche Maßnahmen nach diesem Gesetz, sodass die spezielle Regelung in § 32 Abs. 4 POG nicht erforderlich ist.

Zu Buchstabe d

Redaktionelle Änderungen.

Zu Nummer 18 (§ 33)

Zu Buchstabe a

Der neu eingefügte Satz 2 ergänzt die Bestimmung zur Festlegung der Prüfungstermine und Aufbewahrungsfristen von personenbezogenen Daten. Liegen danach aus unterschiedlichen Anlässen personenbezogene Daten zu Personen vor, die einer Straftat verdächtigt werden oder die in § 26 Abs. 3 POG genannt sind, bestimmen sich nunmehr die Prüfungstermine und Aufbewahrungsfristen einheitlich nach der Frist, die als letzte abläuft. Die betreffenden Daten werden zu Zwecken der Gefahrenabwehr und insbesondere zur vorbeugenden Be-

kämpfung von Straftaten gespeichert. Voraussetzung für die Erhebung und Speicherung solcher Daten sind Verhältnismäßigkeit, Erforderlichkeit und Geeignetheit der Maßnahmen. Die Prüfungstermine und Aufbewahrungsfristen werden dabei im Rahmen der gesetzlichen Vorgaben in einer Einzelfallentscheidung festgelegt. Die Entscheidung beruht auf einer Prognose, bei der neben der Persönlichkeit der betroffenen Person und der Art und Schwere der Straftat auch die Häufigkeit der begangenen Straftaten zu berücksichtigen ist. Durch die Gesetzesänderung soll ein selektives Löschen bedeutsamer Daten verhindert werden. Die weitere Speicherung der Daten ist auch angemessen, da die Betroffenen Anlass dazu gegeben haben. Vergleichbare Vorschriften gibt es auch in den Polizeigesetzen anderer Länder (vgl. beispielsweise Artikel 38 Abs. 2 Satz 6 des bayerischen Polizeiaufgabengesetzes; § 27 Abs. 4 Satz 4 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung – HSOG –).

Zu Buchstabe b

Die Bestimmung zur Anonymisierung von personenbezogenen Daten wird dahingehend ergänzt, dass Daten, die durch Maßnahmen nach § 31 c POG erhoben worden sind, stets zu anonymisieren sind, sofern sie zur Aus- und Fortbildung verwendet werden.

Zu Nummer 19 (§ 34 Abs. 7 Satz 2)

Nach Absatz 7 in seiner derzeitigen Fassung ist die sogenannte „Öffentlichkeitsfahndung“ nach einer Person nur zulässig, soweit die Abwehr einer Gefahr für Leib, Leben oder Freiheit dieser Person sonst nicht möglich ist oder wesentlich erschwert wird. Es muss also um die Abwehr von Gefahren gehen, die der Person, nach der gefahndet wird, selbst droht. Eine Öffentlichkeitsfahndung nach solchen Personen, die nicht selbst bedroht sind, von denen aber eine Gefahr für Leib, Leben oder Freiheit anderer Personen ausgeht, ist nach Absatz 7 ausgeschlossen.

Zwar besteht nach § 131 a Abs. 3 StPO die Möglichkeit zur Anordnung einer Öffentlichkeitsfahndung, wenn die oder der Beschuldigte einer Straftat von erheblicher Bedeutung dringend verdächtig ist und die Aufenthaltsermittlung auf andere Weise erheblich weniger Erfolg versprechend oder wesentlich erschwert wäre. In den Fällen, in denen es jedoch allein um Gefahrenabwehr geht, scheidet die Norm als Rechtsgrundlage aus.

Satz 2 lässt nunmehr die Öffentlichkeitsfahndung zum Zwecke der Ermittlung der Identität oder des Aufenthaltsortes auch in den Fällen zu, in denen von einer Person eine Gefahr für Leib, Leben oder Freiheit anderer Personen ausgeht. Während in den Fällen des Satz 1 sowohl die allgemeinen Ordnungsbehörden als auch die Polizei zur Vornahme einer Öffentlichkeitsfahndung ermächtigt sind, beschränkt sich die Befugnis in Satz 2 auf die Polizei. Nach der Aufgabenzuweisung in § 1 Abs. 1 Satz 3 POG liegt die Zuständigkeit für die vorbeugende Bekämpfung von Straftaten ausschließlich bei der Polizei. Da in den Fällen des Satz 2 die Begehung einer Straftat droht, ist es folgerichtig, die Ermächtigung allein der Polizei zu übertragen.

Die Öffentlichkeitsfahndung nach Satz 2 ist nur zulässig, wenn eine konkrete Gefahr für die genannten Schutzgüter vorliegt und die Abwehr der Gefahr sonst nicht möglich ist oder wesentlich erschwert wird. Unter einer konkreten Gefahr versteht man eine Sachlage, bei der im einzelnen Fall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden eintreten wird. Die gefahrenrelevante Sachlage muss also wirklich bestehen und darf nicht nur vermutet werden. Ferner muss aufgrund der festgestellten Sachlage nach bewährten Erfahrungssätzen davon ausgegangen werden können, dass bei ungehindertem Ablauf mit hinreichender Wahrscheinlichkeit ein polizeilich geschütztes Rechtsgut geschädigt wird. Ferner kommt dem Grundsatz der Verhältnismäßigkeit besondere Bedeutung zu, da die öffentliche Bekanntgabe der Personalien oder des Aussehens einer Person – etwa über die Presse – einen sehr intensiven Eingriff in das Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes darstellt.

Eine Öffentlichkeitsfahndung nach einer Person, von der eine Gefahr ausgeht, kommt danach zum Beispiel in Betracht, wenn die Polizei von der betroffenen Person selbst, über Dritte oder auf sonstige Weise Kenntnis davon erlangt, dass eine Person, deren Identität oder Aufenthaltsort nicht bekannt ist, in absehbarer Zeit schwere Straftaten zu begehen beabsichtigt. Sofern die Abwehr der Gefahr sonst nicht möglich ist oder wesentlich erschwert wird, dürfen die Personalien und eine Personenbeschreibung zum Zwecke der Ermittlung ihrer Identität oder ihres Aufenthaltsortes öffentlich bekannt gegeben werden.

Ein Anwendungsfall für die Öffentlichkeitsfahndung zum Zwecke der Ermittlung des Aufenthaltsortes könnte beispielsweise dann vorliegen, wenn die Polizei von der Ehefrau darüber informiert wird, dass ihr Mann, deren Aufenthaltsort ihr nicht bekannt ist, angekündigt habe, sich das Leben zu nehmen und dabei beabsichtige, andere „mit in den Tod zu nehmen“. Sofern unter Beachtung der Subsidiaritätsklausel der Aufenthaltsort des Mannes weder über die Ermittlung von Standortdaten noch durch andere polizeiliche Maßnahmen festgestellt werden kann, wäre die öffentliche Bekanntgabe seiner Daten zulässig.

Zur Ermittlung der Identität einer Person könnte eine Öffentlichkeitsfahndung in Betracht kommen, wenn jemand im Internet unter Angabe falscher Personalien ein Foto oder Video von sich veröffentlicht und gleichzeitig zum Ausdruck bringt, dass er eine Amoktat zu begehen beabsichtigt. Voraussetzung ist allerdings, dass seine Identität nicht auf andere Weise – etwa über die IP-Adresse – oder durch sonstige Ermittlungsmaßnahmen festgestellt werden kann.

Die Norm ermächtigt keinesfalls zur öffentlichen Bekanntgabe personenbezogener Daten, um die Bevölkerung vor Sexual- oder Gewaltverbrechern, die aus der Justizvollzugsanstalt entlassen worden sind, zu „warnen“. Zweck der Maßnahme muss immer die Ermittlung der – der Polizei nicht bekannten – Identität oder des Aufenthaltsortes einer Person sein, von der mit hinreichender Wahrscheinlichkeit angenommen werden kann, dass sie Leib, Leben oder Freiheit anderer Menschen schädigen wird.

Zu Nummer 20 (§ 37)

In der Bestimmung wird klargestellt, dass der polizeiliche

Datenabgleich mit dem Fahndungsbestand nur zu Zwecken der Gefahrenabwehr zulässig ist. Damit werden die Vorgaben des Bundesverfassungsgerichts im Urteil vom 11. März 2008 (1 BvR 2074/05 und 1 BvR 1254/07) zum Datenabgleich berücksichtigt. Das Bundesverfassungsgericht führte in dem Urteil aus, dass eine Ermächtigung zum Zugriff auf sogenannte Mischdateien, die sowohl strafprozessualen als auch präventiven Zwecken dienen, dem Gebot der Normenbestimmtheit und Normenklarheit nicht widersprechen, sofern die Zugriffszwecke bestimmt sind. Es muss erkennbar sein, ob der Zugriff selbst ausschließlich oder im Schwerpunkt präventiven oder repressiven Zwecken dient (BVerfG, a. a. O., Absatz Nr. 151). Der Fahndungsbestand stellt eine solche Mischdatei dar. Zwar ergibt sich aus dem Regelungszusammenhang, dass ein Datenabgleich mit dem Fahndungsbestand auf der Grundlage dieser Vorschrift nur zu Zwecken der Gefahrenabwehr vorgenommen werden darf. Im Interesse der Rechtsklarheit erfolgt jedoch nunmehr eine gesetzliche Klarstellung.

Zu Nummer 21 (§ 38)

Zu Buchstabe a

Die Ermächtigung zur Rasterfahndung wird neu gefasst und damit den Anforderungen des Bundesverfassungsgerichts im Beschluss vom 4. April 2006 (1 BvR 518/02) zur Rasterfahndung Rechnung getragen. Das Bundesverfassungsgericht hatte die im Land Nordrhein-Westfalen durchgeführte Rasterfahndung auf Grundlage des nordrhein-westfälischen Polizeigesetzes für verfassungswidrig erklärt. Danach ist die präventive polizeiliche Rasterfahndung mit dem Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes nur dann vereinbar, wenn zumindest eine konkrete Gefahr für hochrangige Rechtsgüter wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben ist. Aufgrund der Intensität der Eingriffe darf die Rasterfahndung nicht bereits im Vorfeld einer konkreten Gefahr ermöglicht werden. Anlass der Entscheidung war die Klage eines Betroffenen gegen die bundesweit nach den Anschlägen am 11. September 2001 in den USA durchgeführte Rasterfahndung. Ziel der Maßnahme war insbesondere die Erfassung sogenannter „Schläfer“. Die Landeskriminalämter erhoben Daten unter anderem bei Universitäten, Einwohnermeldeämtern und dem Ausländerzentralregister und rasterten diese nach bestimmten Kriterien.

Der Beschluss des Bundesverfassungsgerichts hat rechtliche Konsequenzen für das rheinland-pfälzische Polizei- und Ordnungsbehördengesetz.

Absatz 1 übernimmt die Vorgaben des Bundesverfassungsgerichts. Danach ist die Rasterfahndung nunmehr nur zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person zulässig. Dadurch scheidet eine Rasterfahndung im Vorfeld einer Gefahr aus. Bei der Auslegung des Gefahrenbegriffs sind die Grundsätze des Bundesverfassungsgerichts im genannten Beschluss vom 4. April 2006 zugrunde zu legen. Dementsprechend reichen allgemeine Bedrohungslagen, wie sie nach dem 11. September 2001 durchgehend bestanden haben, oder außenpolitische Spannungslagen zur Bejahung der konkreten Gefahr nicht aus (BVerfG, a. a. O., Absatz Nr. 134 und 147).

Zu Buchstabe b

Da die Maßnahme eine Vielzahl von Unbeteiligten betreffen kann, wird anstelle des Behördenleitervorbehalts ein Richtervorbehalt eingeführt. Nach Satz 3 ist wie bisher die oder der Landesbeauftragte für den Datenschutz unverzüglich von einer Maßnahme zu unterrichten.

Zu Buchstabe c

Redaktionelle Änderung.

Zu Nummer 22 (§ 39)

Zu Buchstabe a

Zu Doppelbuchstabe aa

Redaktionelle Folgeänderung.

Zu Doppelbuchstabe bb

Nach der neu eingefügten Alternative 4 sind durch eine verdeckte Datenerhebung erhobene personenbezogene Daten zu löschen, wenn sie für den zugrunde liegenden Zweck nicht mehr erforderlich sind. Die Regelung stellt eine allgemeine Verpflichtung zur Löschung von personenbezogenen Daten dar, wodurch dem Grundsatz der Verhältnismäßigkeit und den Belangen des Datenschutzes Rechnung getragen wird. Die bisherige bereichsspezifische Regelung in § 31 Abs. 3 Satz 2 POG entfällt, da ihr Regelungsgehalt nunmehr von dieser Vorschrift mit umfasst wird.

Zu Doppelbuchstabe cc

Der angefügte Satz 2 enthält allgemeine Verfahrensanforderungen bei der Löschung von durch verdeckte Datenerhebungen erhobenen personenbezogenen Daten. Um die Löschung solcher Daten zu dokumentieren, ist eine Niederschrift anzufertigen. Diese Bestimmung dient der Einhaltung der Löschungspflicht sowie der Nachvollziehbarkeit der Löschung.

Nach Satz 3 gelten zusätzliche Anforderungen bei der Löschung von personenbezogenen Daten, die durch Wohnraumüberwachungen gemäß § 29 POG, Telekommunikationsüberwachungen gemäß § 31 POG, Auskünfte über Nutzungsdaten gemäß § 31 b POG oder verdeckte Zugriffe auf informationstechnische Systeme gemäß § 31 c POG erhoben worden sind. Diese Daten sind unter Aufsicht der oder des behördlichen Datenschutzbeauftragten zu löschen. Spezielle Regelungen zur Löschung von Daten, wie beispielsweise in § 39 a Abs. 1 Satz 2 und 3 und § 39 b Abs. 1 Satz 2 und 3 POG, bleiben unberührt.

Zu Buchstabe b

Durch den eingefügten Absatz 4 wird klargestellt, dass die Bestimmungen zur Zweckänderung unberührt bleiben. Danach sind personenbezogene Daten dann nicht zu löschen, wenn die Voraussetzungen einer Zweckänderung vorliegen.

Zu Nummer 23 (§§ 39 a und 39 b)

§ 39 a (Schutz des Kernbereichs privater Lebensgestaltung)

Die Bestimmung regelt den Schutz des Kernbereichs privater Lebensgestaltung bei der Durchführung verdeckter Maßnah-

men. Das Bundesverfassungsgericht hat mehrfach einen Kernbereich privater Lebensgestaltung anerkannt, der dem staatlichen Zugriff schlechthin entzogen ist und in den der Staat unter keinen Umständen eindringen darf. Es hatte in seiner Entscheidung vom 3. März 2004 (1 BvR 2378/98 und 1 BvR 1084/99) erstmals einfachgesetzliche Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung für akustische Wohnraumüberwachungen nach der Strafprozessordnung gefordert. Dieses Urteil hat auch rechtliche Konsequenzen für entsprechende Maßnahmen zum Zweck der Gefahrenabwehr, da nach der Verfassungsrechtsprechung der Kernbereich privater Lebensgestaltung unabhängig von der Zielsetzung der Maßnahme zu schützen ist. Der Landesgesetzgeber ist diesen Anforderungen durch das Sechste Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes vom 25. Juli 2005 (GVBl. S. 320) zur Neuregelung der Wohnraumüberwachung nachgekommen. Der rheinland-pfälzische Verfassungsgerichtshof entschied durch Urteil vom 29. Januar 2007 (VGH B 1/06), dass die Ermächtigung zur Wohnraumüberwachung gemäß § 29 POG mit der Landesverfassung und dem Grundgesetz im Einklang steht. Es bestätigte, dass die Befugnis den absoluten Schutz des unantastbaren Kernbereichs privater Lebensgestaltung gewährleistet.

Das Bundesverfassungsgericht forderte in seiner Entscheidung vom 27. Juli 2005 (1 BvR 668/04) ferner, dass auch bei Maßnahmen der Telekommunikationsüberwachung Kommunikationsinhalte höchstpersönlichen Inhalts zu schützen sind. Jedoch legte es bei diesen Maßnahmen andere Maßstäbe zum Schutz des Kernbereichs als bei Eingriffen in das Grundrecht auf Unverletzlichkeit der Wohnung an. In seinem Urteil vom 27. Februar 2008 (1 BvR 370/07 und 1 BvR 595/07) zur Online-Durchsuchung entwickelte das Bundesverfassungsgericht ein zweistufiges Schutzkonzept zur Gewährleistung des verfassungsrechtlich gebotenen Schutzes des Kernbereichs privater Lebensgestaltung (BVerfG, a. a. O., Absatz Nr. 280 ff.).

Die neu eingefügte Vorschrift setzt die verfassungsrechtlichen Anforderungen zum Schutz des Kernbereichs privater Lebensgestaltung bei der Durchführung verdeckter Maßnahmen um. Bei der Ausgestaltung der zu treffenden Schutzmaßnahmen wird dort, wo es erforderlich ist, nach der jeweiligen Maßnahme im Einklang mit der Verfassungsrechtsprechung differenziert. Die Regelungsinhalte der bisherigen Schutzbestimmungen bei der Wohnraumüberwachung gemäß § 29 Abs. 3 bis 5 POG werden in diese Vorschrift aufgenommen.

Absatz 1 normiert allgemeine Grundsätze, die für sämtliche verdeckte Maßnahmen nach diesem Gesetz gelten. Satz 1 gibt das verfassungsrechtliche Verbot wieder, durch verdeckte Maßnahmen in den Kernbereich privater Lebensgestaltung einzugreifen. Dieses Verbot gilt uneingeschränkt und wird auch nicht durch Erwägungen der Verhältnismäßigkeit eingeschränkt. Das Sechste Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes hatte erstmals ein solches Verbot in die Ermächtigung zur Wohnraumüberwachung aufgenommen. Nunmehr wird dieses Verbot als allgemeiner Grundsatz für sämtliche verdeckte Maßnahmen festgeschrieben.

Ob ein Sachverhalt dem Kernbereich zuzuordnen ist, hängt nach der Rechtsprechung des Bundesverfassungsgerichts (Beschluss vom 14. September 1989, 2 BvR 1062/87) unter anderem davon ab, ob er nach seinem Inhalt höchstpersönlichen Charakter hat und in welcher Art und Intensität er aus sich heraus die Sphäre anderer oder die Belange der Gemeinschaft berührt. Zudem ist von Bedeutung, ob die betroffene Person den Sachverhalt geheim halten will oder nicht (vgl. hierzu auch die Gesetzesbegründung zum Änderungsgesetz vom 25. Juli 2005 – Landtagsdrucksache 14/3936, S. 9 –).

Nach Satz 2 sind Daten, die trotz des Verbots erlangt wurden, unverzüglich zu löschen. Abgesehen von der speziellen Bestimmung in Absatz 4 dieser Regelung verpflichtet das Gebot zur unverzüglichen Löschung grundsätzlich diejenige Person, die dazu am ehesten in der Lage ist. Dies werden die mit der Auswertung betrauten Polizeibeamtinnen und Polizeibeamten sein.

Das Verwertungsverbot nach Satz 3 entspricht den vom Bundesverfassungsgericht aufgestellten Vorgaben, die von dem Gedanken ausgehen, dass durch eine derartige Verwertung der unzulässige Eingriff in den Kernbereich noch vertieft würde.

Satz 4 soll die Erlangung von Rechtsschutz gegen den Eingriff sichern, indem die Tatsache der Erfassung der Daten zu dokumentieren und damit aktenkundig zu machen ist. Die Dokumentation der Erfassung der Daten darf keine Rückschlüsse auf den Inhalt der erhobenen Daten zulassen. Die Dokumentation kann für Zwecke der Datenschutzkontrolle oder im Rahmen der gerichtlichen Überprüfung der Maßnahme verwendet werden.

Die Verpflichtung, die Löschung der erhobenen Daten zu dokumentieren, ergibt sich aus dem neu eingefügten § 39 Abs. 2 Satz 2 und 3 POG.

Absatz 2 übernimmt die bisherige Regelung gemäß § 29 Abs. 3 POG. Eine inhaltliche Änderung ist nicht beabsichtigt. Das Verbot, in den Kernbereich privater Lebensgestaltung einzugreifen, ergibt sich bereits aus dem allgemeinen Verbot nach Absatz 1 Satz 1.

Absatz 3 regelt den Schutz des Kernbereichs privater Lebensgestaltung bei Telekommunikationsüberwachungen nach § 31 POG, Auskünften über Nutzungsdaten nach § 31 b POG und verdeckten Zugriffen auf informationstechnische Systeme nach § 31 c POG.

In Fortführung seiner bisherigen Rechtsprechung hatte das Bundesverfassungsgericht in seinem Urteil vom 27. Juli 2005 (1 BvR 668/04) auch einfachgesetzliche Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung bei Telekommunikationsüberwachungen gefordert. Es erkannte aber an, dass hier andere Maßstäbe als bei Eingriffen in die Unverletzlichkeit der Wohnung gemäß Artikel 13 des Grundgesetzes anzulegen sind. Damit wurde berücksichtigt, dass die Bürgerinnen und Bürger zur höchstpersönlichen Kommunikation nicht in gleicher Weise auf Telekommunikation wie auf eine Wohnung angewiesen sind. Das Bundesverfassungsgericht führte im Urteil zur Online-Durchsuchung vom 27. Februar 2008 (1 BvR 370/07 und 1 BvR 595/07) diese Grundsätze fort und entwickelte ein zweistufiges Schutzkonzept. Danach haben die gesetzlichen Regelungen auf der ersten Stufe darauf hinzuwirken, dass die Erhebung kernbereichsrelevanter Daten, soweit informations- und ermittlungstechnisch möglich, unterbleibt. Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen (BVerfG, a. a. O., Absatz Nr. 281). Auf der zweiten Stufe hat

der Gesetzgeber durch geeignete Verfahrensvorschriften sicherzustellen, dass dann, wenn Daten mit Bezug zum Kernbereich privater Lebensgestaltung erhoben worden sind, die Intensität der Kernbereichsverletzung und ihre Auswirkungen für die Persönlichkeit und Entfaltung der betroffenen Person so gering wie möglich bleiben (BVerfG, a. a. O., Absatz Nr. 283 ff.).

Die Ausführungen des Bundesverfassungsgerichts in den zuletzt zitierten Entscheidungen beziehen sich auf die Telekommunikationsüberwachung und den verdeckten Zugriff auf informationstechnische Systeme. Sie haben aber im gleichen Maße für Auskünfte über Nutzungsdaten Bedeutung, da diese Maßnahmen vergleichbare Gefährdungssituationen für den Kernbereich privater Lebensgestaltung darstellen können. Deshalb werden diese Maßnahmen in den Anwendungsbereich des Absatzes 3 einbezogen.

Absatz 3 orientiert sich an dem zweistufigen Schutzkonzept und enthält die Schutzanforderungen der ersten Stufe. Nach Satz 1 sind Maßnahmen nach den §§ 31, 31 b und 31 c POG unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch die Überwachung allein Erkenntnisse aus diesem Bereich erlangt würden. Bereits die Anordnung einer solchen Maßnahme, aber auch deren Durchführung ist unzulässig. Die Unzulässigkeit ist allerdings nicht bereits dann gegeben, wenn ein Eingriff in den Kernbereich nicht ausgeschlossen werden kann. Von einer alleinigen Erfassung von kernbereichsrelevanten Inhalten ist insbesondere auch dann nicht auszugehen, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Betroffenen Inhalte aus dem Kernbereich privater Lebensgestaltung mit gefahrenrelevanten Inhalten verknüpfen, um die Maßnahme zu verhindern. Die Unzulässigkeit kann sich jedoch beispielsweise ergeben, wenn über einen bestimmten Anschluss nur Privatgespräche zwischen Verwandten, Ehepaaren oder Lebenspartnerinnen und Lebenspartnern geführt werden. Die Prognose nach Satz 1 verlangt, anders als bei der Wohnraumüberwachung, keine besonderen vorausgehenden Ermittlungen.

Durch diese Regelung wird dem Umstand Rechnung getragen, dass bei Anordnung der entsprechenden Maßnahmen regelmäßig nicht sicher vorhersehbar ist, welchen Inhalt die abgehörten Gespräche oder die erhobenen Daten haben werden. Nur in seltenen Fällen kann jedes Risiko ausgeschlossen werden, dass die Maßnahmen in den Schutzbereich privater Lebensgestaltung eingreifen. So kann beispielsweise eine Prognose, mit wem ein Telefongespräch zustande kommt und in welchem Verhältnis die beiden Gesprächspartnerinnen oder Gesprächspartner zueinander stehen, in der Regel angesichts der Vielgestaltigkeit von Telekommunikationsvorgängen nicht getroffen werden. Das Gleiche gilt für den verdeckten Zugriff auf informationstechnische Systeme und für Auskünfte über Nutzungsdaten. Aus diesen Gründen wird ein nicht so strenger Maßstab wie bei Anordnung der Wohnraumüberwachung gemäß Absatz 2 angelegt.

Satz 2 fordert weiterhin für die Datenerhebung durch den Zugriff auf informationstechnische Systeme, dass, soweit dies informations- und ermittlungstechnisch möglich ist, mittels geeigneter Vorkehrungen sicherzustellen ist, dass bereits die Erhebung von kernbereichsrelevanten Daten unterbleibt. Diese Voraussetzung steht unter dem Vorbehalt des informations- und ermittlungstechnisch Möglichen, indem die Sicherstellung in der Erhebungsphase voraussetzt, dass geeignete Vorkehrungen vorhanden und einsetzbar sind. Auch das Bundesverfassungsgericht stellte in seiner Entscheidung vom 27. Februar 2008 fest, dass es bei einem heimlichen Zugriff auf ein informationstechnisches System praktisch unvermeidbar sei, Informationen zur Kenntnis zu nehmen, bevor der Kernbereichsbezug bewertet werden kann (BVerfG, a. a. O., Absatz Nr. 279). Zudem heißt es in der Entscheidung, dass „technische Such- oder Ausschlussmechanismen zur Bestimmung der Kernbereichsrelevanz persönlicher Daten…“ nach einhelliger Auffassung der vom Senat angehörten sachkundigen Auskunftspersonen nicht so zuverlässig arbeiten, dass mit ihrer Hilfe ein wirkungsvoller Kernbereichsschutz erreicht werden könnte (BVerfG, a. a. O., Absatz Nr. 278).

Absatz 4 stellt die zweite Stufe des vom Bundesverfassungsgericht entwickelten zweistufigen Schutzkonzepts (BVerfG, a. a. O., Absatz Nr. 280 ff.) dar. Die Norm enthält Verfahrensbestimmungen, die bei Wohnraum- und Telekommunikationsüberwachungen, der Erhebung von Nutzungsdaten und des verdeckten Zugriffs auf informationstechnische Systeme zu beachten sind.

Satz 1 bestimmt, dass die Auswertung der erhobenen Daten nur unter Sachleitung des zuständigen Oberverwaltungsgerichts Rheinland-Pfalz erfolgen darf. Eine vergleichbare Regelung enthält § 20 k Abs. 7 Satz 3 BKAG im Hinblick auf den verdeckten Zugriff auf informationstechnische Systeme. Durch die Vorschrift wird im Interesse des Grundrechtsschutzes gewährleistet, dass die Auswertung der erhobenen Daten durch eine unabhängige und neutrale Instanz kontrolliert wird. Das Oberverwaltungsgericht Rheinland-Pfalz leitet die Auswertung der erhobenen Daten, prüft und trifft die erforderlichen Maßnahmen.

Satz 2 legt zusätzliche Anforderungen bei der Auswertung von Daten, die durch eine Wohnraumüberwachung oder einen verdeckten Zugriff auf informationstechnische Systeme erhoben worden sind, fest. Danach müssen zwei Bedienstete der zuständigen Polizeibehörde, von denen einer die Befähigung zum Richteramt hat, und die oder der behördliche Datenschutzbeauftragte die Daten auf die Kernbereichsrelevanz überprüfen. Auch diese Bestimmung orientiert sich an § 20 k Abs. 7 Satz 3 BKAG.

Absatz 5 entspricht inhaltlich weitgehend dem bisherigen § 29 Abs. 4 POG, der bereits bisher für die Wohnraumüberwachung das sogenannte Richterband regelte. Die Anforderungen dieser Bestimmung gelten nunmehr ebenso für die Telekommunikationsüberwachung und den verdeckten Zugriff auf informationstechnische Systeme. Ferner wird die Bestimmung sprachlich neu gefasst. In Satz 1 wird der allgemeine Begriff „unmittelbare Kenntnisnahme einer Maßnahme nach den §§ 29, 31 und 31 c“ anstelle der bisherigen Aufzählung „Abhören, die Beobachtung sowie die Auswertung der erhobenen Daten“ verwendet, da die Regelung nun auf verschiedene Befugnisse Anwendung findet. Danach ist die unmittelbare Kenntnisnahme wie das Live-Mithören und Live-Beobachten durch die Polizei zu unterbrechen, wenn sich bei der Überwachung tatsächliche Anhaltspunkte ergeben, dass kernbereichsrelevante Daten erfasst werden. Im Unterschied zu Absatz 1 Satz 1 steht in diesen Fällen noch nicht fest, ob ein Eingriff in den Kernbereich privater Lebensgestaltung vorliegt. Bei diesen Zweifelsfällen soll jedoch ausgeschlossen werden, dass die Polizei weiterhin unmittelbar Kenntnis von den erhobenen Daten erhält.

Satz 2 bestimmt, dass in Fällen des Satzes 1 die automatische Aufzeichnung fortgesetzt werden darf. Die Aufzeichnung ist dem Oberverwaltungsgericht Rheinland-Pfalz vorzulegen, das über die weitere Verwertbarkeit oder Löschung der Daten entscheidet.

Satz 3 legt fest, unter welchen Voraussetzungen die unmittelbare Kenntnisnahme der Maßnahme fortgesetzt werden darf und verweist insoweit auf die Bestimmungen, die bei Anordnung der Maßnahme gelten.

§ 39 b (Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger)

Die Bestimmung regelt den Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträgerinnen und Berufsgeheimnisträger bei verdeckten Maßnahmen nach diesem Gesetz.

Nach Absatz 1 besteht bei Durchführung verdeckter Maßnahmen ein absolutes Erhebungs- und Verwertungsverbot für Erkenntnisse, die dem Zeugnisverweigerungsrecht der Berufsgeheimnisträgerinnen und Berufsgeheimnisträger gemäß § 53 Abs. 1 und § 53 a Abs. 1 StPO unterfallen. Vorbehaltlich der Verstrickungsregelung in Absatz 2 darf in diese Vertrauensverhältnisse auch nicht zur Abwehr von Gefahren für hochrangige Rechtsgüter eingegriffen werden. Nach Satz 1 dürfen diese Berufsgeheimnisträgerinnen und Berufsgeheimnisträger entsprechend dem Recht zur Verweigerung der Auskunft gemäß dem künftigen § 9 a Abs. 4 Satz 3 POG durch verdeckte Maßnahmen gleich welcher Art nicht in ihrem Vertrauensverhältnis beeinträchtigt werden; auf die Begründung zu Artikel 1 Nr. 2 Buchst. a Doppelbuchst. aa wird verwiesen. Bereits bestehende Regelungen gemäß § 28 Abs. 4, § 29 Abs. 6 und § 31 Abs. 4 POG werden aufgehoben.

Satz 2 verpflichtet zur unverzüglichen Löschung von Daten, die entgegen des Verbots in Satz 1 erlangt wurden. Nach Satz 3 dürfen Erkenntnisse darüber nicht verwertet werden. Damit wird einer etwaigen Aufrechterhaltung einer Verletzung vorgebeugt und die Vertraulichkeit der Kommunikation mit den genannten Personen im Rahmen des ihnen zustehenden Zeugnisverweigerungsrechts gewährleistet. Zugleich sichert es die Einhaltung des Erhebungsverbots nach Satz 1.

Nach Satz 4 ist die Tatsache von Datenerhebungen, die unter das Erhebungsverbot nach Satz 1 fallen, in geeigneter Form zu dokumentieren. Dies dient vor allem der späteren Nachvollziehbarkeit im Rahmen etwaiger Rechtsschutzbegehren. Die Dokumentation darf keinen Rückschluss auf den Inhalt der Daten geben. Die Verpflichtung zur Dokumentation der Löschung ergibt sich aus dem neu eingefügten § 39 Abs. 2 Satz 2 und 3 POG.

Absatz 2 beinhaltet eine sogenannte Verstrickungsregelung. Dies bedeutet, dass der von Absatz 1 gewährleistete besondere Schutz des Verhältnisses zu einer Berufsgeheimnisträgerin oder einem Berufsgeheimnisträger endet, wenn diese oder dieser selbst für die Gefahr verantwortlich ist, welche mit der in Rede stehenden Maßnahme abgewehrt werden soll. Der Schutz des Vertrauensverhältnisses ist in diesen Fällen nicht mehr gerechtfertigt, da das Vertrauensverhältnis missbraucht wird.

Zu Nummer 24 (§ 40 Abs. 5)

Zu Buchstabe a

Durch die Gesetzesänderung wird der Kreis der sonstigen betroffenen Personen, die von einer verdeckten Maßnahme zu unterrichten sind, erweitert. Zu unterrichten sind nunmehr auch sonstige Personen, die von einer Maßnahme nach § 31 c POG betroffen sind.

Zu Buchstabe b

Die Zuständigkeit der Amtsgerichte für die Zustimmung über die Zurückstellung der Unterrichtung der von verdeckten Datenerhebungen betroffenen Personen wird neu geregelt. Entsprechend der Zuständigkeitsregelungen in anderen Fällen soll auch hier das Amtsgericht zuständig sein, in dessen Bezirk die Polizeidienststelle ihren Sitz hat.

Zu Buchstabe c

Der künftige § 40 Abs. 5 Satz 9 POG trifft eine praktischen Bedürfnissen Rechnung tragende Regelung für den Fall, dass mehrere verdeckte Maßnahmen in einem zeitlichen und sachlichen Zusammenhang durchgeführt werden. Dadurch soll verhindert werden, dass die Verantwortlichen oder sonstige Personen zu frühzeitig von verdeckten Maßnahmen Kenntnis erlangen und somit die polizeiliche Tätigkeit beeinträchtigen oder vereiteln können. Nach dem ersten Halbsatz soll deshalb in solchen Fällen die Unterrichtung mit Abschluss der letzten verdeckten Maßnahme erfolgen. Sofern die Unterrichtung nach den gesetzlichen Gründen unterbleibt, gelten nach dem zweiten Halbsatz die gleichen Grundsätze für die Einholung der richterlichen Zustimmung wie für jede weitere Zurückstellung der Unterrichtung. Entscheidend für den Beginn der anzurechnenden Frist für die Unterrichtung und die Einholung der richterlichen Zustimmung für eine Zurückstellung ist somit der Abschluss der letzten verdeckten Maßnahme. Ein sachlicher Zusammenhang ist immer dann gegeben, wenn einzelne Maßnahmen eingesetzt werden, um ein gemeinsames Ziel zur Gefahrenabwehr wie beispielsweise die Verhütung eines terroristischen Anschlags oder rechtsextremistischer Straftaten zu erreichen.

Zu Nummer 25 (§ 41 Abs. 2 Satz Nr. 11)

Es handelt sich um eine durch die Einfügung des § 41 a POG bedingte Folgeänderung.

Zu Nummer 26 (§ 41 a)

Durch die neu eingefügte Vorschrift werden technisch-organisatorische Datenschutzregelungen in das Polizei- und Ordnungsbehördengesetz integriert, die sicherstellen sollen, dass die vom Bundesverfassungsgericht in seinem Urteil vom 2. März 2010 (1 BvR 256/08) zur Vorratsdatenspeicherung geforderten hohen Anforderungen zur Datensicherheit bei der Verarbeitung von Verkehrsdaten durch die Telekommunikations-Diensteanbieter auch für die Polizei gelten, die ebenfalls Verkehrsdaten im Rahmen der Telekommunikationsüberwachung und bei der Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten zu verarbeiten hat. Derzeit gelten für polizeiliche Verfahren die allgemeinen Regelungen zum technisch-organisatorischen Datenschutz in § 9 des Landesdatenschutzgesetzes (LDSG) vom 5. Juli 1994

(GVBl. S. 293), zuletzt geändert durch Artikel 1 des Gesetzes vom 17. Juni 2008 (GVBl. S. 99), BS 204-1. Diese Vorschrift steht allerdings wie die entsprechenden Bestimmungen im Bundesdatenschutzgesetz (BDSG) in der Fassung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) und den Datenschutzgesetzen der Länder in der Diskussion. Eine Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder hat in diesem Zusammenhang Empfehlungen zur Novellierung der Technikregelungen der Datenschutzgesetze erarbeitet, die darauf abzielen, die unterschiedlichen Regelungen im Bund und in den Ländern zu harmonisieren. Es ist davon auszugehen, dass zunächst im Bundesdatenschutzgesetz eine Novellierung der Technikregelungen erfolgen und den Ländern als Muster zur Überarbeitung ihrer Bestimmungen dienen wird. Der Zeitpunkt für eine Novellierung des § 9 LDSG ist jedoch ungewiss, sodass es angezeigt erscheint, für den Polizeibereich eine Datenschutzregelung zu schaffen, die im Hinblick auf die Sensibilität der bei der Polizei zu verarbeitenden Daten hohe Sicherheitsstandards dem Grunde nach verbindlich vorgibt.

So hat das Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung ausgeführt, dass angesichts des Umfangs und der potenziellen Aussagekraft der mit einer vorsorglichen Speicherung von Telekommunikationsverkehrsdaten geschaffenen Datenbestände die Datensicherheit von großer Bedeutung sei (BVerfG, a. a. O., Absatz Nr. 222). Nach dem gegenwärtigen Stand der Diskussion müsse grundsätzlich eine getrennte Speicherung der Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffsregime sowie eine revisionssichere Protokollierung sichergestellt sein (BVerfG, a. a. O., Absatz Nr. 224).

Ferner ist zu berücksichtigen, dass die Überlegungen der Sicherheitsbehörden dahin gehen, die Telekommunikationsüberwachung gegebenenfalls zu zentralisieren, sodass mittelfristig von Datenbeständen bei der Polizei auszugehen ist, die vom Umfang her mit den bei einer Speicherung von Verbindungsdaten durch die Anbieter von Telekommunikationsleistungen anfallenden Datenbeständen vergleichbar ist.

In Absatz 1 Satz 1 wird zunächst auf die allgemeinen Anforderungen zur Datensicherheit in § 9 LDSG verwiesen. Es handelt sich hierbei um eine dynamische Verweisung, damit eine entsprechende Anpassung der Norm an die – wenn auch zu einem noch ungewissen Zeitpunkt – abzusehende Novellierung des § 9 LDSG gewährleistet ist. Absatz 1 Satz 2 stellt klar, dass technische und organisatorische Maßnahmen des Datenschutzes insbesondere die Vertraulichkeit und Integrität der personenbezogenen Daten sicherzustellen haben. Erforderlich sind Vorkehrungen, die unbefugte Zugriffe auf Datenverarbeitungsverfahren und personenbezogene Daten ausschließen. Ferner ist sicherzustellen, dass versehentliche oder bewusste Veränderungen der gespeicherten personenbezogenen Daten unterbleiben. Die Unversehrtheit, Zurechenbarkeit und Vollständigkeit der Daten sind unabdingbare Voraussetzungen für die Herstellung der Rechtsverbindlichkeit.

Absatz 2 regelt, dass die nach Absatz 1 zu treffenden technischen und organisatorischen Maßnahmen in einem umfassenden IT-Sicherheits- und Datenschutzkonzept festgelegt werden. Die Festlegung hat nach den Standards des Bundesamtes für Sicherheit in der Informationstechnik zu erfolgen (Grundschutzkataloge). In diesen Standards wird die Vorgehensweise für die Erstellung von IT-Sicherheits- und Datenschutzkonzepten beschrieben und beinhaltet auch die Feststellung des Schutzbedarfs der Daten sowie die gegebenenfalls erforderliche Risikoanalyse.

Die Schutzbedarfsfeststellung ist die Basis für die Definition ausreichender und angemessener technischer und organisatorischer Maßnahmen. Hierbei wird nach einem definierten Schema bewertet, wie hoch die Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit sind.

Bei einem erhöhten Schutzbedarf oder entsprechender Komplexität soll die Risikoanalyse (BSI-Standard 100-3) Gefahren identifizieren, die durch die IT-Grundschutzmaßnahmen möglicherweise nicht abgedeckt werden.

Der Baustein „Datenschutz“ der Grundschutzkataloge enthält die für eine datenschutzrechtliche Beurteilung notwendigen Informationen zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Bestandteil des IT-Sicherheits- und Datenschutzkonzeptes sind alle getroffenen bzw. geplanten technischen und organisatorischen Maßnahmen nach Absatz 1 Satz 1. Um ein hohes IT-Sicherheits- und Datenschutzniveau kontinuierlich sicherzustellen, sind das IT-Sicherheits- und Datenschutzkonzept und die in ihm beschriebenen technischen und organisatorischen Maßnahmen in angemessenen Abständen oder bei Verfahrensänderung von der verantwortlichen Stelle auf ihre Eignung hin zu überprüfen. Angemessen ist ein Zeitraum von etwa drei bis fünf Jahren.

Absatz 3 Satz 1 regelt das sogenannte IT-Sicherheits- und Datenschutzaudit. Ziel des Datenschutzaudits ist die Überprüfung der datenschutzrechtlichen Eignung von Produkten und Verfahren durch eine unabhängige Stelle. So sieht § 9 a Satz 1 BDSG vor, dass Anbieter von Datenverarbeitungssystemen und -programmen und Daten verarbeitende Stellen ihre Datenschutzkonzepte sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachterinnen und Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen können. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachterinnen und Gutachter werden nach § 9 a Satz 2 BDSG durch besonderes Gesetz geregelt. Dieses Gesetz sowie die erforderlichen Ausführungsbestimmungen zu § 9 a BDSG stehen noch aus, sodass bislang anerkannte Kriterien für das Datenschutzaudit nach § 9 a BDSG, mit denen die datenschutzrechtliche Qualität von Produkten und Datenverarbeitungsverfahren gemessen werden kann, fehlen. Dies schließt jedoch nicht aus, landesintern für den Datenschutz im Polizeibereich ein Auditierungsverfahren einzuführen, wie es bereits für die IT-Sicherheit zwischen den Polizeien des Bundes und der Länder seit dem Jahr 2003 existiert. Das Landesdatenschutzgesetz in Schleswig-Holstein eröffnet in § 43 Abs. 2 öffentlichen Stellen die Möglichkeit, ihr Datenschutzkonzept im Rahmen eines Datenschutz-Behördenaudits durch das Unabhängige Landeszentrum für Datenschutz überprüfen und beurteilen zu lassen.

Nach Absatz 3 Satz 1 sollen die Polizeibehörden und -einrichtungen zur Verbesserung des Datenschutzes und der Datensicherheit die von ihnen eingesetzten Verfahren zur automatisierten Verarbeitung personenbezogener Daten sowie die dabei genutzten technischen Einrichtungen durch unabhängiges

und fachkundiges Personal in Form von IT-Sicherheits- und Datenschutzaudits prüfen und bewerten lassen.

Da die Prüfungsergebnisse sowie deren Unterlagen grundsätzlich schutzbedürftige Informationen enthalten, dürfen sie nur bei dienstlichem Interesse Dritten in geeigneter Form zugänglich gemacht oder veröffentlicht werden, um eine Kompromittierung von sicherheitsrelevanten Informationen (z. B. Sicherheitslücken oder Informationen über die technische Infrastruktur), die Gegenstand der Audit-Unterlagen sind, zu verhindern.

Aus der Formulierung „sollen“ wird ersichtlich, dass die Durchführung eines Auditierungsverfahrens anzustreben ist. Das Ziel ist die Feststellung des adäquaten Datenschutzniveaus sowie die Erhöhung der Akzeptanz und des Vertrauens der Bürgerinnen und Bürger in die Datenschutzkonformität bei der polizeilichen Verarbeitung personenbezogener Daten.

Durch das Erfordernis des unabhängigen und fachkundigen Personals wird verdeutlicht, dass die Prüfung außerhalb der eigentlich verantwortlichen Stelle im Sinne des Landesdatenschutzgesetzes erfolgen muss, damit die erforderliche Objektivität des Auditierungsverfahrens gewährleistet ist.

Die Abweichung gegenüber den im Bundesdatenschutzgesetz genannten „zugelassenen Gutachtern“ trägt der bewährten Praxis der Polizeien, IT-Verfahren gegenseitig zu auditieren, Rechnung. Für die Prüfung der Datenschutzkonformität der technischen und organisatorischen Maßnahmen bei Audits, die nicht mit einer offiziellen Zertifizierung abschließen müssen, genügt die Fachkunde, die in der Regel durch geeignete Weiterbildungsmaßnahmen erworben wird.

Nach § 3 Abs. 3 LDSG ist verantwortliche Stelle jede Person oder sonstige Stelle, die personenbezogene Daten für sich selbst verarbeitet oder dies durch andere im Auftrag vornehmen lässt. Als unabhängiges und fachkundiges Personal kommen somit alle Personen in Betracht, die nicht derjenigen Polizeibehörde oder -einrichtung angehören, deren Datenschutzkonzept geprüft und bewertet werden soll. Auditorin oder Auditor können danach Personen aus anderen Polizeibehörden oder -einrichtungen in Rheinland-Pfalz oder anderen Bundesländern sein. Gleichzeitig wird die Möglichkeit eröffnet, zu gegebener Zeit das Datenschutzaudit unter Rückgriff auf zugelassene Gutachterstellen, die bislang noch nicht benannt wurden, durchzuführen.

Absatz 3 Satz 3 legt fest, dass Verfahren und technische Einrichtungen, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem Verfahren nach Satz 1 geprüft wurde, von den Polizeibehörden und -einrichtungen vorrangig eingesetzt werden sollen. Sind diese nämlich grundsätzlich verpflichtet, zuverlässige und gegebenenfalls zertifizierte Verfahren und technische Einrichtungen einzusetzen, so ist eine umfängliche Qualitätssicherung in allen Polizeibereichen gewährleistet.

Nach Absatz 4 Satz 1 unterliegen Verfahren der Polizeibehörden und -einrichtungen zur automatisierten Verarbeitung personenbezogener Daten der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Satz 2 legt fest, dass die oder der behördliche Datenschutzbeauftragte für die Vorabkontrolle zuständig ist. Mit Blick auf das in § 41 a Abs. 2 angesprochene IT-Sicherheits- und Datenschutzkonzept sollte hierbei auch die oder der IT-Sicherheitsbeauftragte frühzeitig einbezogen werden. Eine Vorabkontrolle automatisierter Datenverarbeitungsverfahren stellt sicher, dass bereits zu Beginn der Datenverarbeitung der Datenschutzkonformität hinreichend Rechnung getragen wird. Zusätzliche Qualitätssicherung wird dadurch erreicht, dass sich die oder der behördliche Datenschutzbeauftragte nach Satz 3 in Zweifelsfällen an die oder den Landesbeauftragten für den Datenschutz zu wenden hat. Nach Satz 4 ist das Ergebnis der Vorabkontrolle zu dokumentieren, damit die Transparenz des Verfahrens gewährleistet ist.

Zu Nummer 27 (§ 58 Abs. 5 Satz 1)

Der Begriff „Bundesgrenzschutz“ wird durch den Begriff „Bundespolizei“ ersetzt. Dieser neue Begriff wurde durch das Gesetz zur Umbenennung des Bundesgrenzschutzes in Bundespolizei vom 21. Juni 2005 (BGBl. I S. 1818) eingeführt.

Zu Nummer 28 (§ 79 Abs. 3)

Die Zuständigkeit des Landeskriminalamtes wird erweitert, sodass die Behörde auch Aufgaben zur Abwehr von Gefahren wahrnehmen kann. Das Landeskriminalamt wird befugt, zur Abwehr von Gefahren in Fällen von überregionaler oder besonderer Bedeutung die Zuständigkeit einer anderen als der örtlich zuständigen Polizeibehörde zu übertragen oder selbst zu übernehmen. Bislang war die Befugnis des Landeskriminalamtes auf Fälle der Verfolgung von Straftaten begrenzt. Aktuelle Ermittlungsverfahren im Bereich des internationalen Terrorismus haben jedoch gezeigt, dass es erforderlich sein kann, dass das Landeskriminalamt ebenso bei der Gefahrenabwehr und der vorbeugenden Bekämpfung von Straftaten als zentrale Behörde des Landes eine fachliche Zuständigkeit besitzt.

Zu Nummer 29 (§ 86 Abs. 3)

Absatz 3 regelt neu die Voraussetzungen, unter denen Polizeibeamtinnen und Polizeibeamte des Bundes und ausländische Polizeibedienstete im Zuständigkeitsbereich von Rheinland-Pfalz tätig werden dürfen. Satz 1 übernimmt inhaltlich unverändert die bisherige Bestimmung hinsichtlich der Polizeibeamtinnen und Polizeibeamten des Bundes. Aufgrund der fortschreitenden internationalen Zusammenarbeit der Polizei erweitert Satz 2 die Befugnis zum Einsatz von ausländischen Polizeibediensteten. Wie bisher können ausländische Einsätze auf der Grundlage von völkerrechtlichen Vereinbarungen erfolgen. Die bisherige Alternative, wenn sonst Gegenseitigkeit gewährleistet ist, wird ersetzt durch die Bestimmung, dass Amtshandlungen ausländischer Polizeibediensteter zulässig sind, wenn das fachlich zuständige Ministerium allgemein oder im Einzelfall zustimmt. Vergleichbare Vorschriften gibt es auch in den Polizeigesetzen anderer Länder (vgl. z. B. § 102 Abs. 3 Satz 2 HSOG; § 103 Abs. 3 Satz 2 Nds. SOG).

Diese Alternative trägt den Artikeln 17 ff. des Beschlusses 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. EU Nr. L 210 S. 1), Rechnung. Durch die Neufassung wird ein Einsatz von ausländischen Polizeibediensteten zu operativen Zwecken auch ohne völkerrechtlichen Vertrag oder sonstige Gewährleistung der Gegenseitigkeit ermöglicht.

Zu Nummer 30 (§ 95 Abs. 3)

Die Änderung berücksichtigt, dass durch Artikel 12 a des Ersten Gesetzes zur Modernisierung der Justiz vom 24. August 2004 (BGBl. I S. 2198) der Begriff des Hilfsbeamten der Staatsanwaltschaft durch den Begriff der Ermittlungspersonen der Staatsanwaltschaft in § 152 des Gerichtsverfassungsgesetzes in der Fassung vom 9. Mai 1975 (BGBl. I. S. 1077), zuletzt geändert durch Artikel 5 des Gesetzes vom 30. Juli 2009 (BGBl. I. S. 2474), ersetzt wurde. Diese neue Begrifflichkeit wird in das Polizei- und Ordnungsbehördengesetz übernommen.

Zu Nummer 31 (§ 100)

Zu Buchstabe a

Zu Doppelbuchstabe aa

Das Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes und anderer Gesetze vom 2. März 2004 (GVBl. S. 202) führte erstmalig die Verpflichtung der Landesregierung zu einer fünfjährigen Evaluation bestimmter polizeilicher Maßnahmen ein. § 100 POG in der bisherigen Fassung umfasste die Sicht- und Anhaltekontrollen im öffentlichen Verkehrsraum, die Wohnraumüberwachung, die Telekommunikationsüberwachung und die sogenannte Rasterfahndung. Um den vollen Erfassungszeitraum zu gewährleisten, wurde die Erhebung der erforderlichen Daten im Herbst 2009 beendet. Mit der Vorlage dieses Evalutionsberichts endet die Verpflichtung der Landesregierung nach dieser Bestimmung.

Satz 1 führt eine neue Verpflichtung zur Evaluation bestimmter polizeilicher Maßnahmen ein. Diese Norm bezieht wie bislang die Wohnraumüberwachung gemäß § 29 POG, die Telekommunikationsüberwachung gemäß § 31 POG und die sogenannte Rasterfahndung gemäß § 38 POG mit ein, da diese Maßnahmen mit intensiven Grundrechtseingriffen verbunden sein können. Darüber hinaus sollen die neu geschaffenen Ermächtigungen zur Auskunft über Nutzungsdaten gemäß § 31 b POG, zur Online-Überwachung gemäß § 31 c POG und zur Funkzellenabfrage gemäß § 31 e POG evaluiert werden. Dagegen entfällt die bisherige Verpflichtung, die Sicht- und Anhaltekontrollen im öffentlichen Verkehrsraum zu evaluieren.

Der Berichtszeitraum erstreckt sich auf fünf Jahre und beginnt am ersten Tag des zweiten auf die Verkündung des Änderungsgesetzes folgenden Kalendermonats. In dem Zeitraum zwischen dessen Verkündung und dem Inkrafttreten der Evaluationspflicht hat die Landesregierung die erforderlichen Vorbereitungen zur Durchführung der Evaluation zu treffen.

Im Hinblick auf die inhaltlichen Anforderungen an die Evaluation wird verwiesen auf die Gesetzesbegründung zum Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes und anderer Gesetze (Landtagsdrucksache 14/2287, S. 55 f.).

Zu Doppelbuchstabe bb

In Satz 2 erfolgt die Anpassung an den geänderten § 29 POG.

Zu Buchstabe b

Der neu eingefügte Absatz 2 legt fest, dass die Anfertigung des Berichts der Landesregierung unter Mitwirkung einer Stelle erfolgt, die eine wissenschaftlich fundierte Überprüfung der Maßnahmen gewährleistet. Eine solche Stelle könnte etwa die Deutsche Hochschule für Verwaltungswissenschaften in Speyer sein. In einer Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. März 2010 wurde darauf hingewiesen, dass jede Evaluation auf der Grundlage valider und strukturierter Daten zu erfolgen habe. Durch die Mitwirkung einer Stelle, die eine wissenschaftlich fundierte Überprüfung der Maßnahme gewährleistet, wird dieser Forderung Rechnung getragen.

Die Mitwirkung umfasst die Erstellung eines Fragenkatalogs zur Erfassung einer aussagekräftigen Datengrundlage bis hin zur Bewertung der erhobenen Daten. Um dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung zu stellen, muss der Bericht insbesondere die im künftigen § 100 Abs. 3 Satz 1 POG genannten Kriterien zur Wirksamkeit der Maßnahmen darlegen und bewerten.

Zu Buchstabe c

Redaktionelle Änderung.

Zu Artikel 2

Mit der Regelung wird dem in Artikel 19 Abs. 1 Satz 2 des Grundgesetzes enthaltenen Zitiergebot Rechnung getragen. Das Zitiergebot erfüllt eine Warn- und Besinnungsfunktion, die nach dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 (1 BvR 668/04 Absatz Nr. 87) nicht nur die einmalige Grundrechtseinschränkung betrifft, sondern bei jeder Veränderung der Eingriffsvoraussetzungen bedeutsam wird, die zu neuen Grundrechtseinschränkungen führt.

Zu Artikel 3

Artikel 3 regelt das Inkrafttreten des Gesetzes.