LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 7/3694**
7. Wahlperiode **05.06.2019**

GESETZENTWURF

der Landesregierung

Entwurf eines Gesetzes über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern und zur Änderung anderer Gesetze

A Problem und Ziel

Bei der Schaffung gefahrenabwehrrechtlicher Regelungen befindet sich der Gesetzgeber in einem Spannungsfeld zwischen der Wahrung der öffentlichen Sicherheit und der Freiheitsrechte der Bürgerinnen und Bürger. Bei der hierbei erforderlichen Abwägung sind die aktuelle Gefahrenlage, insbesondere durch den internationalen Terrorismus, und die auf europäischer Ebene erfolgte besondere Betonung des Rechts auf informationelle Selbstbestimmung zu beachten. In diesen umfassenden Abwägungsprozess sind einerseits neue kriminelle Begehungsweisen, insbesondere unter Nutzung neuer technischer Möglichkeiten, und andererseits die vom Bundesverfassungsgericht ausgeformten verfassungsrechtlichen Vorgaben einzubeziehen. Je tiefer behördliches Handeln in die Freiheitsrechte der Bürgerinnen und Bürger eingreifen kann, desto enger sind die Eingriffsvoraussetzungen und die Schutzmaßnahmen, etwa durch Regelungen zum Richtervorbehalt sowie zum Schutz des Kernbereichs privater Lebensgestaltung, auszugestalten.

In diesem Lichte ist der Gesetzentwurf zur Neufassung des Sicherheits- und Ordnungsgesetzes zu verfassen. Freiheitsrechte werden nur dort eingeschränkt, wo es für die Gefahrenabwehr zwingend erforderlich und aufgrund der Schwere der Straftatbestände verfassungsrechtlich zulässig ist. Der Polizeialltag zeigt, dass schwerwiegende Eingriffsbefugnisse nur im Ausnahmefall zur Anwendung gelangen. Eine flächendeckende oder anlasslose Einschränkung von Freiheitsrechten ist ausgeschlossen.

Unabhängig von diesen besonderen gesetzlichen Schutzmechanismen gewährleistet Artikel 19 Absatz 4 des Grundgesetzes, dass das Handeln der Sicherheitsbehörden als Teil der öffentlichen Verwaltung von jeder Person gerichtlich überprüft werden kann und daneben im Bereich des Datenschutzes auch der Kontrolle durch den Landesbeauftragten für den Datenschutz unterliegt.

Im Einzelnen:

Seit 25. Mai 2018 gilt die „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ (Datenschutz-Grundverordnung; im Folgenden als Verordnung (EU) 2016/679 bezeichnet) als unmittelbar anzuwendendes Recht. Mit ihr wird unter Beachtung der Erwägungsgründe 10 und 13 das Ziel verfolgt, ein unionsweites gleichwertiges Schutzniveau für die Rechte und die Freiheiten von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten zu schaffen. Die Verordnung (EU) 2016/679 regelt das allgemeine und bereichsspezifische Datenschutzrecht jedoch nicht abschließend. So enthält sie sowohl an die Mitgliedstaaten adressierte Regelungsaufträge als auch Öffnungsklauseln und die Möglichkeit zur Schaffung spezifischer Bestimmungen und zur Beschränkung ihrer Vorschriften.

Die direkte Geltung der Verordnung (EU) 2016/679 erfordert, dass der Bund und auch die Länder ihre allgemeinen und fachspezifischen Datenschutzvorschriften anpassen, um insbesondere widersprüchliche und unzureichende Regelungslagen oder Doppelungen zu vermeiden. Vor diesem Hintergrund wurde im Land Mecklenburg-Vorpommern bereits das allgemeine Datenschutzrecht, das Landesdatenschutzgesetz, angepasst (vergleiche GVOBl. M-V 2018, Seite 193). Unter Berücksichtigung dieses neu gefassten Landesgesetzes und der unmittelbar geltenden Vorschriften der Verordnung (EU) 2016/679 bedarf es auch einer - bereichsspezifischen - Anpassung der datenschutzrechtlichen Bestimmungen in folgenden Gesetzen:

- „Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern“ (Sicherheits- und Ordnungsgesetz - SOG M-V),
- „Gesetz über den Brandschutz und die Technischen Hilfeleistungen durch die Feuerwehren für Mecklenburg-Vorpommern“ (Brandschutz- und Hilfeleistungsgesetz M-V),
- „Gesetz über den Katastrophenschutz in Mecklenburg-Vorpommern“ (Landeskatastrophenschutzgesetz).

Zudem ist am 5. Mai 2016 die „Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates“ (zukünftig bezeichnet als Richtlinie (EU) 2016/680) in Kraft getreten. Sie war nach deren Artikel 63 bis zum 6. Mai 2018 in den Mitgliedstaaten verpflichtend umzusetzen. Mit Blick auf den Anwendungsbereich und Regelungsinhalt der Richtlinie besteht insbesondere ein zwingender Umsetzungsbedarf in den Polizei- beziehungsweise Sicherheits- und Ordnungsgesetzen der Länder.

In der Koalitionsvereinbarung 2016 - 2021 zwischen SPD und CDU für die 7. Wahlperiode des Landtages Mecklenburg-Vorpommern wurde zum einen unter Nummer 434 festgelegt, das Landesrecht an die Verordnung (EU) 2016/679 anzupassen. Zum anderen wurde unter Nummer 379 eine Novellierung des SOG M-V vereinbart, soweit dies aufgrund geänderter EU-Vorschriften rechtlich geboten ist.

Darüber hinaus hat das Bundesverfassungsgericht in seiner Entscheidung vom 20. April 2016 - Aktenzeichen 1 BvR 966/09 - zur verfassungsgemäßen Ausgestaltung bestimmter Regelungen im Bundeskriminalamtgesetz (BKAG) seine Rechtsprechung zu den verfassungsgerichtlichen Anforderungen an die Ausgestaltung eingriffsintensiver Befugnisse weiterentwickelt und präzisiert. Die Ausführungen in der Entscheidung sind auch für das Gefahrenabwehrrecht der Länder von grundsätzlicher und allgemeingültiger Bedeutung und müssen daher im SOG M-V nachvollzogen werden.

Des Weiteren wurde mit Blick auf den Beschluss der Innenministerkonferenz vom Juni 2017, nach dem durch gemeinsame gesetzliche Standards im Gefahrenabwehrrecht der Länder eine effektive Erhöhung der öffentlichen Sicherheit erreicht werden soll, die Notwendigkeit einer weiteren Anpassung des SOG M-V geprüft. In Anbetracht der aktuellen Sicherheitslage, des Standes der technischen Entwicklung und der im Bund beziehungsweise in anderen Ländern vorhandenen oder geplanten Normen sollen weitere Befugnisse neu oder zur Klarstellung im SOG M-V verankert werden, damit die Ordnungsbehörden und die Polizei weiterhin in einem hohen Maß die öffentliche Sicherheit und Ordnung in unserem Land gewährleisten können.

B Lösung

Zur Umsetzung des sogenannten EU-Datenschutzpakets (Verordnung (EU) 2016/679 und Richtlinie (EU) 2016/680) sowie zur Schaffung eines effektiven und zeitgemäßen Gefahrenabwehrrechts bedarf es folgender Gesetzesänderungen:

1. Neufassung des SOG M-V

Mit Artikel 1 des vorliegenden Gesetzentwurfes erfolgt eine Neufassung des SOG M-V. Diese enthält im Wesentlichen folgende Änderungen und Ergänzungen:

a) Anpassungen aufgrund von EU-Datenschutzvorschriften

Die notwendigen Anpassungen aufgrund der Verordnung (EU) 2016/679 und die zwingend gebotene Umsetzung der Richtlinie (EU) 2016/680 im Gefahrenabwehrrecht führen zu umfangreichen Änderungen im SOG M-V. Mit der Neufassung wird im Gesetz eine Anpassung an den Sprachgebrauch der genannten EU-Vorschriften vorgenommen (§ 3) und ausdrücklich bestimmt, dass auch die Verhütung von Ordnungswidrigkeiten von der Gefahrenabwehr umfasst ist (§ 4). Darüber hinaus erfolgt eine umfangreiche datenschutzrechtliche Anpassung und Ergänzung der Regelungen unter Abschnitt 3 „Verarbeitung personenbezogener Daten“ (§§ 25 bis 49).

Es werden in diesem Abschnitt zusätzliche Unterabschnitte eingeführt, die insbesondere zur Umsetzung der Richtlinie (EU) 2016/680 detaillierte Vorschriften
- zur Einwilligung (§ 26)
- zur Datenübermittlung (§§ 39 ff),
- zu den Pflichten der im Sinne des Datenschutzrechts verantwortlichen Stelle sowie des Auftragsverarbeiters (§§ 45 bis 46k),
- zu den Rechten der betroffenen Person (§§ 47 bis 48a) und
- zum Bereich der datenschutzaufsichtlichen Kontrolle (§§ 48b bis 48h)

enthalten. Zudem wird die Regelung der Schadensersatzansprüche und der Entschädigung aus der Verarbeitung personenbezogener Daten (§ 76) überarbeitet.

Es wird - soweit wie rechtlich zulässig und möglich - eine direkte Regelung der im Bereich des Gefahrenabwehrrechtes zu beachtenden datenschutzrechtlichen Bestimmungen im SOG M-V selbst vorgenommen. Dies bedeutet zwar einerseits einen größeren gesetzgeberischen Aufwand, anderseits erspart es den Gesetzesanwendern aber weitestgehend ein ständiges „Hineinspringen“ in verschiedene datenschutzrechtliche Regelungswerke und gewährleistet so die bessere praktische Handhabung. Auch stellt dieses Vorgehen eine möglichst einheitliche Verfahrensweise bei Polizei und Ordnungsbehörden im Land Mecklenburg-Vorpommern mit Blick auf die notwendige Zusammenarbeit im Bereich der Gefahrenabwehr sicher.

Soweit Regelungen aus der Verordnung (EU) 2016/679 in das Gesetz übernommen werden, erfolgt dies in Ansehung des Erwägungsgrundes 8 der Verordnung (EU) 2016/679. Danach sind Wiederholungen von Regelungen der Verordnung im nationalen Recht insoweit möglich, als im Falle von Präzisierungen oder Einschränkungen von Regelungen der Verordnung (EU) 2016/679 durch das nationale Recht diese erforderlich sind, um die Kohärenz zu wahren und die Vorschriften des nationalen Rechts für die Personen, für die sie gelten, verständlicher zu machen. Im Übrigen wird mit § 25 SOG M-V eine Vorschrift geschaffen, die den Gesetzesanwender darauf hinweist, dass soweit das SOG M-V nichts Besonderes regelt, das Landesdatenschutzgesetz ergänzend zur Anwendung gelangt (hierzu eingehender siehe Begründung zu Artikel 1, dort § 25).

b) Anpassungen an die Vorgaben des Bundesverfassungsgerichtes aus dem Urteil vom 20. April 2016

Zur Umsetzung der Vorgaben des Bundesverfassungsgerichtes in seinem Urteil vom 20. April 2016 - 1 BvR 966/09 und andere - wird im SOG M-V im Wesentlichen ebenfalls der Abschnitt 3 zur Verarbeitung personenbezogener Daten (§§ 25 bis 49) angepasst.

Insbesondere wird dort eine explizite und umfassende Regelungslage zum Kernbereichsschutz (§ 26a) und zum Schutz von zeugnisverweigerungsberechtigten Personen (§ 26b) geschaffen. Die Eingriffsvoraussetzungen verdeckter Maßnahmen werden insgesamt überarbeitet und teilweise ergänzt. Die hierzu bestehenden Anordnungsvorbehalte haben Änderungen erfahren. Vorgegeben wird hinsichtlich gesetzlich normierter Anordnungen nunmehr, welche Inhalte behördliche Anträge an das Gericht aufweisen müssen und welche Inhalte gerichtliche oder behördliche Anordnungen mindestens zu enthalten haben. Zu den bestehenden verdeckten Maßnahmen nach § 33 und zur Rasterfahndung nach § 44 werden weitere Richtervorbehalte eingefügt.

Zugleich werden mit Blick auf den Grundsatz der hypothetischen Datenneuerhebung in Bezug auf die Datenerhebungsbefugnisse nach dem SOG M-V verstärkte Anforderungen an die Zweckbindung und die weitere Verarbeitung von personenbezogenen Daten, die durch eingriffsintensive Maßnahmen gewonnen wurden, geregelt. Insbesondere sind in diesem Zuge auch die Bestimmungen zur Datenübermittlung (§§ 39 bis 39h) neu ausgestaltet worden. Es werden weitere Vorschriften zur Information und Benachrichtigung der Personen, die von den Maßnahmen betroffen sind oder waren (§§ 46 bis 46c), zur Dokumentation und Protokollierung behördlichen Handelns (§§ 46d bis 46f) sowie zur Kennzeichnung von personenbezogenen Daten (§ 46g) geschaffen.

Ferner erfolgt die Anpassung der Vorschriften zu den Berichts- und Unterrichtungspflichten gegenüber dem Landtag, seinem SOG-Gremium sowie der Öffentlichkeit bei eingriffsintensiven und verdeckten Maßnahmen.

Mit § 115 wird hierzu und auch zur Kennzeichnung von personenbezogenen Daten sowie zur Protokollierung eine Ausnahme- beziehungsweise Übergangsregelung geschaffen, um der Praxis nach Inkrafttreten des Gesetzes die notwendige Umsetzungszeit einzuräumen.

c) Ergänzung des SOG M-V um neue Befugnisnormen und klarstellende Regelungen

Es werden folgende Befugnisse neu beziehungsweise aus Gründen der Rechtssicherheit ausdrücklich im SOG M-V verankert:

- Eilkompetenz für Zollbedienstete in den Vollzugsbereichen der Zollverwaltung (§ 9),
- ausdrückliche Regelung zum Einsatz technischer Mittel zur Fertigung von Übersichtsaufnahmen/-aufzeichnungen im öffentlichen Raum zur Herstellung von Rechtssicherheit (§ 32 Absatz 1),
- polizeiliche Befugnis zur offenen Bildbeobachtung und Anfertigung von Bild- und Tonaufzeichnungen in den für die Durchführung der Gewahrsamnahme genutzten polizeilichen Räumen (§ 32 Absatz 9) sowie klarstellende Regelung zur Anfertigung von Bild- und Tonaufzeichnungen zur Suche nach Personen, deren Leben oder Gesundheit gefährdet ist (§ 32 Absatz 10),
- polizeiliche Befugnis mit Richtervorbehalt zum verdeckten Zugriff auf fremde informationstechnische Systeme über Kommunikationsnetze mittels einer Überwachungssoftware (sogenannte Online-Durchsuchung; § 33c),
- polizeiliche Befugnis mit Richtervorbehalt zur Ausleitung von Telekommunikationsinhalten vor der Verschlüsselung mittels spezieller Software, die auf dem Endgerät der betroffenen Person verdeckt installiert wird (sogenannte Quellen-TKÜ; § 33d Absatz 3),
- polizeiliche Befugnis mit Richtervorbehalt zur Beauskunftung von Nutzungsdaten nach dem Telemediengesetz (§ 33e) sowie eine polizeiliche Befugnis zur Beauskunftung von Bestandsdaten nach dem Telemediengesetz (§ 33h) zur Schaffung von Rechtssicherheit und Rechtsklarheit,
- klarstellende Auflistung der Anlässe für den offenen und verdeckten Einsatz von unbemannten Luftfahrtsystemen (sogenannter Drohneneinsatz; § 34),
- polizeiliche Befugnis zur Ausschreibung zur gezielten Kontrolle (§ 35),
- polizeiliche Befugnis zur Datenübermittlung zum Zwecke einer Zuverlässigkeitsüberprüfung (§ 40),

- Erweiterung des Katalogs der Straftaten von erheblicher Bedeutung in § 49 wie folgt:
  - in § 49 Nummer 2 Erweiterung um die Vergehenstatbestände der §§ 89c Absatz 1 bis 4 (Terrorismusfinanzierung), 129a (Bildung terroristischer Vereinigungen), 129b (kriminelle und terroristische Vereinigungen im Ausland), 184b Absatz 1 und 2 sowie 184c Absatz 2 (Verbreitung, Erwerb und Besitz kinderpornographischer und jugendpornographischer Schriften), 303b Absatz 4 (besonders schwerer Fall der Computersabotage) des Strafgesetzbuches und
  - in § 49 Nummer 3 Erweiterung um banden-, gewerbs-, serienmäßige oder sonst organisierte Vergehen nach § 261 des Strafgesetzbuches (Geldwäsche) sowie nach § 96 Absatz 2 des Aufenthaltsgesetzes (Einschleusen von Ausländern).
- Erweiterung bestimmter bereits bestehender Eingriffsbefugnisse zur Verhütung von drohenden terroristischen Straftaten im Sinne des § 67c,
- ausdrückliche polizeiliche Befugnis zur Erteilung von Meldeauflagen (§ 52b),
- Aufnahme von Forderungen und anderen Vermögensrechten in die Sicherstellungsbefugnis (§ 61) und
- klarstellende Regelung zum finalen Rettungsschuss (§ 109 Absatz 1).

Zudem werden die Regelungen aus § 52 Absatz 3 (Betretungs- und Aufenthaltsgebote bis maximal zehn Wochen) herausgelöst und in eine gesonderte Norm (§ 52a) - unter Anpassung der Höchstfrist auf drei Monate und unter Ergänzung weiterer notwendiger Regelungen zur Anordnung - überführt.

d) Weitere Änderungen im SOG M-V

Ferner werden mit der in Artikel 1 vorgesehenen Neufassung des SOG M-V weitere notwendige rechtliche Anpassungen und redaktionelle Korrekturen vollzogen. Es erfolgt die Aufnahme der großen kreisangehörigen Städte in das Gesetz. Die sprachliche Gleichstellung sowie die Aktualisierung von Behördenbezeichnungen und Verweisungen werden vorgenommen.

2. Änderung des Brandschutz- und Hilfeleistungsgesetzes M-V

Mit Artikel 2 erfolgt im Brandschutz- und Hilfeleistungsgesetz M-V eine Anpassung der datenschutzrechtlichen Bestimmungen aufgrund der unmittelbaren Geltung der Verordnung (EU) 2016/679 und der ergänzenden Bestimmungen im Landesdatenschutzgesetz. Zudem wird die Bezeichnung des Innenressorts aktualisiert.

3. Änderung des Landeskatastrophenschutzgesetzes

Mit Artikel 3 wird im Landeskatastrophenschutzgesetz ebenfalls eine Anpassung der datenschutzrechtlichen Bestimmungen aufgrund der unmittelbaren Geltung der Verordnung (EU) 2016/679 und der ergänzenden Bestimmungen im Landesdatenschutzgesetz vorgenommen. Es erfolgt eine Aktualisierung der Bezeichnung des Innenressorts.

C Alternativen

1. In Bezug auf die in Artikel 1 bis 3 vorgesehenen gesetzlichen Änderungen aufgrund der EU-Datenschutzvorschriften:

Keine. Die mit Artikel 1 bis 3 vorgesehene Anpassung der datenschutzrechtlichen Vorschriften im Landesrecht an die Verordnung (EU) 2016/679 ist geboten, um einen rechtssicheren Vollzug des unmittelbar geltenden europäischen Rechts zu gewährleisten. Mit Artikel 1 wird darüber hinaus der bestehenden Pflicht der Mitgliedstaaten zum Erlass der für die Umsetzung der Richtlinie (EU) 2016/680 notwendigen Vorschriften nachgekommen.

2. In Bezug auf die im Artikel 1 vorgesehenen Änderungen zur Umsetzung bundesverfassungsgerichtlicher Vorgaben im SOG M-V:

Keine. Aufgrund der Rechtsprechung des Bundesverfassungsgerichtes in seinem Urteil vom 20. April 2016 zu bestimmten Befugnissen im Bundeskriminalamtgesetz sind auch die mit diesen Befugnissen vergleichbaren Eingriffsbefugnisse im SOG M-V anzupassen.

3. In Bezug auf die im Artikel 1 vorgesehene Aufnahme neuer Befugnisnormen in das SOG M-V:

Keine. Ohne die vorgesehenen Änderungen im SOG M-V stünden der Polizei und den Ordnungsbehörden die aktuell notwendigen Befugnisse zur Gewährleistung einer effektiven Gefahrenabwehr im Land nicht zur Verfügung. Dem erklärten Ziel, gerade durch gemeinsame gesetzliche Standards im Gefahrenabwehrrecht der Länder eine effektive Erhöhung der öffentlichen Sicherheit in der Bundesrepublik Deutschland zu erreichen, würde nicht gefolgt werden. Auch das in Bezug auf die Aufnahme der klarstellenden Regelungen verfolgte Ziel der Herstellung von Rechtssicherheit würde nicht erreicht werden.

D Notwendigkeit (§ 3 Absatz 1 Satz 1 GGO II)

Die Neufassung beziehungsweise Änderung der in Artikel 1 bis 3 genannten Landesgesetze ist aufgrund der notwendigen Harmonisierung mit den oben angeführten EU-Vorschriften und unter Berücksichtigung des neugefassten Landesdatenschutzgesetzes notwendig. Mit Artikel 1 werden zudem Vorgaben des Bundesverfassungsgerichtes in seiner Entscheidung zum Bundeskriminalamtgesetz vom 20. April 2016 umgesetzt (siehe Ausführungen unter Buchstabe A).

Nach dem Grundsatz vom Vorbehalt des Gesetzes setzen neue oder geänderte Eingriffs- und auch Datenverarbeitungsbefugnisse wegen der damit verbundenen Grundrechtseingriffe das Vorliegen entsprechender gesetzlicher Ermächtigungen voraus. Diesem Grundsatz wird durch die in Artikel 1 bis 3 vorgesehenen Gesetzesänderungen Rechnung getragen.

E Finanzielle Auswirkungen auf die Haushalte des Landes und der Kommunen

1 Haushaltsausgaben ohne Vollzugsaufwand

Hinsichtlich der Kennzeichnung personenbezogener Daten und der Protokollierung sind umfangreiche IT-seitige Anpassungen der Fachverfahren vorzunehmen. Die diesbezüglich mit Artikel 1 neu eingefügten Regelungen beruhen auf den Vorgaben des Bundesverfassungsgerichtes aus dem Urteil zum Bundeskriminalamtgesetz vom 20. April 2016 und dienen deren Umsetzung. Die für die IT-seitige Anpassung aufzuwendenden Mittel können derzeit noch nicht konkret beziffert werden.

Wird die Befugnis zum Einsatz von Videoüberwachungstechnik in den für die Durchführung der Gewahrsamnahme genutzten polizeilichen Räumen (Artikel 1 § 32 Absatz 9) geschaffen, ist die vollständige Nachrüstung von Videoüberwachungstechnik in allen vorhandenen Gewahrsamszellen und den diesbezüglichen Vorfluren in der Landespolizei einschließlich des Aufbaus eines separaten Übertragungsnetzes vorzunehmen. Diese beabsichtigten Maßnahmen würden schrittweise umgesetzt werden. Die hierfür entstehenden Ausgaben sind derzeit noch nicht abschließend bezifferbar.

Der Aufwand zur Beauskunftung von Bestands- und Nutzungsdaten nach den §§ 14 und 15 des Telemediengesetzes (siehe hierzu Regelungslage in Artikel 1 §§ 33e und 33h) wird den Anbietern von Telemediendiensten entsprechend dem § 23 des Justizvergütungs- und -entschädigungsgesetzes (JVEG) entschädigt. Die Ausgaben hierfür werden davon abhängen, wie viele praktische Anwendungsfälle im Land Mecklenburg-Vorpommern zu verzeichnen sein werden. Zum aktuellen Zeitpunkt können die Mittelbedarfe nicht verlässlich beziffert werden.

Zur Beschaffung von Drohnen (siehe Regelungslage in Artikel 1 § 34) sind für das Haushaltsjahr 2019 bereits Haushaltsmittel in Höhe von 50.000 Euro veranschlagt.

Zur Schaffung der neuen Befugnisse zur Online-Durchsuchung (Artikel 1 § 33c) und Quellen-TKÜ (Artikel 1 § 33d Absatz 3) ist zu den finanziellen Auswirkungen erläuternd Folgendes anzumerken:

Wird von diesen Befugnissen Gebrauch gemacht, wird sowohl Technik als auch Software benötigt. Nach derzeitigem Stand ist jedoch davon auszugehen, dass die Länder die Softwarelösungen, die ihnen für die strafprozessualen Maßnahmen der Quellen-TKÜ und der Online-Durchsuchung vom Bund zur Verfügung gestellt werden, auch für gefahrenabwehrrechtliche Maßnahmen zur Quellen-TKÜ und zur Online-Durchsuchung nutzen können. Insoweit werden derzeit keine zusätzlichen Kosten für das Land hinsichtlich der für die Durchführung dieser Maßnahmen benötigten Software erwartet. Dies gilt auch für die notwendige IT-Technik und für die erforderlichen speziell ausgebildeten IT-Kräfte, da diese bereits für die Durchführung einer strafprozessualen Quellen-TKÜ beziehungsweise Online-Durchsuchung in der Landespolizei vorgehalten werden müssen beziehungsweise im Einsatz sind und insofern ebenfalls eine Mitnutzung beziehungsweise deren Einsatz für den gefahrenabwehrrechtlichen Bereich erfolgen kann.

Im Übrigen enthalten die Neuregelungen haushaltsneutrale Befugnisse.

Finanzielle Bedarfe werden grundsätzlich im Rahmen bereits veranschlagter Mittel sowie der mittelfristigen Finanzplanung abgedeckt. Über gegebenenfalls bestehende finanzielle Mehrbedarfe und deren Veranschlagung wird, soweit diese schon heute bezifferbar sind, im Rahmen der Aufstellung des Doppelhaushaltes 2020/2021 entschieden.

2 Vollzugsaufwand

Zu Artikel 1

Durch die Umsetzung der vorbenannten EU-Vorschriften und der verfassungsrechtlichen Vorgaben sowie durch die neu geschaffenen Befugnisse im SOG M-V werden derzeit noch nicht konkret bezifferbare personelle Ressourcen gebunden. Generell gilt, dass der Bedarf personeller Ressourcen durch Organisationsmaßnahmen im Rahmen der vereinbarten Stellenpläne und Personalentwicklungsplanungen kompensiert wird, sodass keine Stellenmehrbedarfe entstehen. Finanzielle Bedarfe werden grundsätzlich im Rahmen bereits veranschlagter Mittel sowie der mittelfristigen Finanzplanung abgedeckt.

Im Einzelnen:

a) Vollzugsaufwand bei den Polizeibehörden

Zusätzlicher Aufwand entsteht aus der gebotenen Umsetzung der vorbenannten EU-Vorschriften und verfassungsrechtlichen Vorgaben; insbesondere

- aufgrund von Kennzeichnungs-, Dokumentations-, Protokollierungs-, Prüf-, Informations- und Benachrichtigungspflichten,
- bei der notwendigen Anpassung polizeilicher Fachverfahren zur Umsetzung bestehender Kennzeichnungs- und Protokollierungspflichten,
- durch die zusätzlichen Aufgaben der behördlichen Datenschutzbeauftragten bei den Polizeibehörden,
- mit den erhöhten Anforderungen bei der Anordnung von eingriffsintensiven beziehungsweise verdeckten Maßnahmen,
- durch die Ausweitung der in § 48h vorgesehenen Berichts- und Unterrichtungspflichten in allen Polizeibehörden (einschließlich dem Ministerium für Inneres und Europa).

Inwieweit und wie oft die im SOG M-V neu geschaffenen Befugnisse (siehe oben Punkt B „Lösung“ unter Nummer 1 Buchstabe c), die an das Vorliegen der jeweiligen gesetzlichen Voraussetzungen gebunden und damit erst zur Abwehr entsprechend vorliegender Gefahren anzuwenden sind, durch die Landespolizei in Anspruch genommen werden müssen und somit einen personellen Aufwand auslösen, ist nicht abzusehen.

Hinzuweisen ist auch darauf, dass mit § 52b nun eine ausdrückliche und ausschließliche polizeiliche Befugnisnorm zum Erlass von Meldeauflagen geschaffen wird. Die Zuständigkeit zum Erlass von Meldeauflagen lag bisher grundsätzlich bei den Ordnungsbehörden. Auch insoweit entsteht mithin ein zusätzlicher, aber überschaubarer personeller Aufwand bei der Polizei.

Die aufgrund der geänderten Vorschriften erforderliche Anpassung der polizeilichen Vorschriftenlage löst ebenfalls einen weiteren personellen Aufwand aus.

b) Vollzugsaufwand bei der Justiz

Insbesondere werden durch die Einführung weiterer Richtervorbehalte (vergleiche etwa Anordnungsregelungen in §§ 33a, 33c, 33d Absatz 3, 33e und § 44 oder auch vorgesehene richterliche Entscheidungen wie in § 26a Absatz 4 oder §§ 54 oder 61), die jedoch alle verfassungsrechtlich geboten sind, zusätzliche personelle Kapazitäten bei der Justiz gebunden. Mehrheitlich werden die Amtsgerichte am Sitz der Polizeibehörde (siehe gerichtliche Zuständigkeit in § 25b) und damit die Amtsgerichte Schwerin, Rostock und Neubrandenburg belastet sein. Der zusätzliche personelle Aufwand ist nicht bezifferbar, da die Anzahl der notwendigen unter Richtervorbehalt stehenden Maßnahmen nicht absehbar ist.

c) Vollzugsaufwand bei den Ordnungsbehörden

Es ist nicht davon auszugehen, dass dieses Gesetz eine wesentliche zusätzliche Bindung personeller Kapazitäten bei den Ordnungsbehörden auslöst. Im Zusammenhang mit der Umsetzung der EU-Datenschutzvorschriften ist darauf hinzuweisen, dass zusätzlicher personeller Aufwand etwa durch bestehende Informations- oder auch Dokumentationspflichten durch die oben benannten EU-Vorschriften selbst veranlasst wird. Auch ist eventuell eine Anpassung der Fachverfahren hinsichtlich der Kennzeichnung und Protokollierung von personenbezogenen Daten notwendig. Der dadurch gegebenenfalls entstehende personelle Mehraufwand ist jedoch auf die Umsetzung der Vorgaben des Bundesverfassungsgerichtes zurückzuführen.

Soweit eine Datenübermittlung an Drittstaaten und an andere als die in § 39c genannten zwischen- und überstaatlichen Stellen auf der Grundlage des SOG M-V oder der Verordnung (EU) 2016/679 erfolgt, werden Ordnungsbehörden diese dem Ministerium für Inneres und Europa melden müssen, da das Ministerium in Umsetzung der bundesverfassungsrechtlichen Vorgaben nach § 48h über diese Datenübermittlungen zu berichten und zu unterrichten hat.

Die Ordnungsbehörden werden durch das Gesetz gegenüber der bisherigen Rechtslage um den Erlass von Meldeauflagen vollständig entlastet. So wird mit § 52b nun eine ausdrückliche und ausschließlich polizeiliche Befugnisnorm zum Erlass von Meldeauflagen geschaffen.

Die Ordnungsbehörden trifft eine zusätzliche unverzügliche Unterrichtungspflicht gegenüber der örtlich zuständigen Polizeidienststelle, soweit die Ordnungsbehörde ein Aufenthalts- und Betretungsverbot anordnet (§ 52a).

Im Ministerium für Inneres und Europa ist durch die in § 20 Absatz 3 vorgesehene Genehmigungspflicht für Gefahrenabwehrverordnungen der großen kreisangehörigen Städte ein zusätzlicher personeller Aufwand zu erwarten.

d) Vollzugsaufwand bei der oder dem Landesbeauftragten für den Datenschutz

Mit den in das SOG M-V zur Umsetzung der Richtlinie (EU) 216/680 neu aufgenommenen §§ 47 bis 48d wird bei der oder bei dem Landesbeauftragten für den Datenschutz als Aufsichtsbehörde ein zusätzlicher Vollzugsaufwand entstehen.

Dieser Aufwand ist jedoch durch die notwendige Umsetzung des EU-Datenschutzpaketes und der bundesverfassungsgerichtlichen Vorgaben veranlasst.

e) Weiterer Vollzugsaufwand

Im Übrigen ist darauf hinzuweisen, dass die geänderten Regelungen und auch die Neuregelungen im SOG M-V im Rahmen der Aus- und Fortbildung an der Fachhochschule für öffentliche Verwaltung und Rechtspflege in Güstrow zu berücksichtigen sind.

Zu den Artikeln 2 und 3

Die gesetzlichen Änderungen im Brandschutz- und Hilfeleistungsgesetz M-V (Artikel 2) und im Landeskatastrophenschutzgesetz (Artikel 3) erfolgen in Anbetracht der Umsetzung der Verordnung (EU) 2016/679. Auch diesbezüglich ist mit einem zusätzlichen Vollzugsaufwand aufgrund der Änderung der datenschutzrechtlichen Vorschriften zu rechnen, der jedoch nicht aufgrund dieses Gesetzes ausgelöst wird.

F Sonstige Kosten (zum Beispiel Kosten für die Wirtschaft, Kosten für soziale Sicherungssysteme)

Auch mit der Neufassung der Vorschriften zur Telekommunikationsüberwachung beziehungsweise Auskunftserteilung über bestimmte Telekommunikationsdaten (Artikel 1 §§ 33d, 33f bis 33h) bleibt es bei der bestehenden Verpflichtung zur Entschädigung der zur Auskunft verpflichteten Diensteanbieter im Sinne des Telekommunikationsgesetzes nach § 23 JVEG.

Soweit Diensteanbieter im Sinne des Telemediengesetzes nun - statt des bisher praktizierten Rückgriffs auf die allgemeinen Datenerhebungsvorschriften im SOG M-V - auf gesetzlicher Grundlage zur Erteilung von Auskünften nach den §§ 14 und 15 des Telemediengesetzes verpflichtet werden (vergleiche Artikel 1 §§ 33e und 33h), werden sie ebenfalls entsprechend dem § 23 JVEG entschädigt. Da nicht klar ist, wie oft diese neuen Normen zur Gefahrenabwehr in Anspruch genommen werden müssen, ist die Höhe der zu zahlenden Entschädigung nicht konkret bezifferbar.

G Bürokratiekosten

Durch das Gesetz werden keine Informationspflichten für Unternehmen eingeführt.

**DIE MINISTERPRÄSIDENTIN
DES LANDES
MECKLENBURG-VORPOMMERN**

Schwerin, den 5. Juni 2019

An die
Präsidentin des Landtages
Mecklenburg-Vorpommern
Frau Birgit Hesse
Lennéstraße 1

19053 Schwerin

Betr.: Entwurf eines Gesetzes über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern und zur Änderung anderer Gesetze

Sehr geehrte Frau Präsidentin,

als Anlage übersende ich Ihnen den von der Landesregierung am 4. Juni 2019 beschlossenen Entwurf des vorbezeichneten Gesetzes mit Begründung.

Ich bitte Sie, die Beschlussfassung des Landtages herbeizuführen.

Federführend ist das Ministerium für Inneres und Europa.

Mit freundlichen Grüßen

Manuela Schwesig

ENTWURF

eines Gesetzes über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern und zur Änderung anderer Gesetze

Der Landtag hat das folgende Gesetz beschlossen:

Inhaltsübersicht:

Artikel 1
Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern (Sicherheits- und Ordnungsgesetz - SOG M-V)

Inhaltsübersicht:

Unterabschnitt 3
Speicherung, Übermittlung und sonstige Verarbeitung personenbezogener Daten (§§ 36 - 44)

Unterabschnitt 4
Pflichten der verantwortlichen Stelle und des Auftragsverarbeiters (§§ 45 - 46k)

Unterabschnitt 5
Rechte der betroffenen Person (§§ 47 - 48a)

Unterabschnitt 6
Datenschutzaufsichtliche und parlamentarische Kontrolle (§§ 48b - 48h)

Abschnitt 1
Aufgaben und Zuständigkeit (§§ 1 - 11)

§ 1
Aufgaben

(1) Das Land, die Landkreise, die kreisfreien und die großen kreisangehörigen Städte, die Ämter und die amtsfreien Gemeinden haben die Aufgabe, von der Allgemeinheit oder dem Einzelnen Gefahren abzuwehren, durch die die öffentliche Sicherheit oder Ordnung bedroht wird (Gefahrenabwehr).

(2) Unbeschadet der Zuständigkeit der Polizei zur vorbeugenden Bekämpfung von Straftaten (§ 7 Absatz 1 Nummer 4) sollen staatliche und nichtstaatliche Träger öffentlicher Aufgaben im Rahmen ihres jeweiligen gesetzlichen Zuständigkeitsbereichs zusammenwirken und zur Vermeidung strafbarer Verhaltensweisen (Kriminalprävention) beitragen.

(3) Der Schutz privater Rechte gehört zur Gefahrenabwehr, wenn gerichtlicher Schutz nicht rechtzeitig zu erlangen ist und ohne die Hilfe die Gefahr besteht, dass die Verwirklichung des Rechts vereitelt oder wesentlich erschwert wird.

(4) Die Gefahrenabwehr wird von den Landkreisen, kreisfreien und großen kreisangehörigen Städten, Ämtern und amtsfreien Gemeinden als Landesaufgabe im übertragenen Wirkungskreis wahrgenommen.

§ 2
Ordnungsbehörden und Polizei

(1) Die Gefahrenabwehr obliegt den Ordnungsbehörden und der Polizei.

(2) Die Ordnungsbehörden und die Polizei haben ferner diejenigen Aufgaben zu erfüllen, die ihnen durch besondere Rechtsvorschriften übertragen sind. Soweit für die Durchführung dieser Aufgaben die besonderen Rechtsvorschriften nichts Abweichendes bestimmen, gelten die §§ 2 bis 78 nach Maßgabe der §§ 4 und 7.

§ 3
Begriffsbestimmungen

(1) Ordnungsbehörden sind:

1. die Ministerien im Rahmen ihres Geschäftsbereichs (Landesordnungsbehörden),
2. die Landräte für die Landkreise (Kreisordnungsbehörden),
3. die Oberbürgermeister beziehungsweise Bürgermeister für die kreisfreien und die großen kreisangehörigen Städte, die Amtsvorsteher für die Ämter, die Bürgermeister für die amtsfreien Gemeinden (örtliche Ordnungsbehörden),
4. die Landesbehörden, denen Aufgaben der Gefahrenabwehr durch besondere Rechtsvorschriften übertragen sind (Sonderordnungsbehörden).

Die Oberbürgermeister der kreisfreien Städte sind für das Gebiet ihrer Stadt zugleich Kreisordnungsbehörden.

(2) Polizei im Sinne dieses Gesetzes sind die Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten sowie die Polizeibehörden des Landes.

(3) Im Sinne dieses Gesetzes ist
1. eine im einzelnen Falle bevorstehende Gefahr:
   eine Sachlage, bei der bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens ein die öffentliche Sicherheit oder Ordnung schädigendes Ereignis im konkreten Einzelfall in absehbarer Zeit mit hinreichender Wahrscheinlichkeit eintreten wird;
2. gegenwärtige Gefahr:
   eine Sachlage, bei der das die öffentliche Sicherheit oder Ordnung schädigende Ereignis bereits eingetreten ist (Störung) oder unmittelbar oder in allernächster Zeit mit an Sicherheit grenzender Wahrscheinlichkeit bevorsteht;
3. erhebliche Gefahr:
   eine Gefahr für ein bedeutsames Rechtsgut, wie Leib, Leben oder Freiheit einer Person, wesentliche Sach- oder Vermögenswerte oder den Bestand des Staates.

(4) „Dritter“ ist
1. eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person (Person, gegen die sich die Maßnahme gezielt richtet), der verantwortlichen Stelle (Absatz 5 Nummer 9), dem Auftragsverarbeiter (Absatz 5 Nummer 10) und den Personen, die unter der unmittelbaren Verantwortung der verantwortlichen Stelle oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten oder
2. eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person.

(5) Im Sinne dieses Gesetzes
1. sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
2. sind „Grunddaten“ Daten, die zur Identifizierung einer Person dienen, wie insbesondere Name, Geschlecht, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Anschrift.
3. sind „besondere Kategorien personenbezogener Daten“:
   a) Daten, aus denen die ethnische Herkunft, die politische Meinung oder die religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit hervorgehen,
   b) genetische Daten,
   c) biometrische Daten; Lichtbilder jedoch nur, soweit sie mit speziellen technischen Verfahren verarbeitet werden sollen, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen,
   d) Gesundheitsdaten,
   e) Daten zum Sexualleben,
   f) Daten der sexuellen Orientierung.

4. ist „Verarbeitung“ jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
5. ist „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.
6. ist „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.
7. ist „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.
8. ist ein „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.
9. ist „verantwortliche Stelle“ die Polizeibehörde oder Ordnungsbehörde, die die personenbezogenen Daten zur Erfüllung der ihr obliegenden Aufgaben nach diesem Gesetz verarbeitet.
10. ist „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag der verantwortlichen Stelle verarbeitet.
11. ist „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten nach Absatz 4 Nummer 1 handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.
12. ist „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.
13. ist „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

14. sind „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.
15. sind „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.
16. sind „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.
17. ist „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

§ 4
Sachliche Zuständigkeit der Ordnungsbehörden, Ermächtigung zum Erlass von Rechtsverordnungen

(1) Für die Gefahrenabwehr sind die Ordnungsbehörden zuständig, soweit durch Rechtsvorschrift nichts anderes bestimmt ist. Zur Gefahrenabwehr gehört auch die Verhütung von Ordnungswidrigkeiten.

(2) Sachlich zuständig ist die örtliche Ordnungsbehörde, soweit durch Rechtsvorschrift nichts anderes bestimmt ist. Das fachlich zuständige Ministerium kann im Einvernehmen mit dem Ministerium für Inneres und Europa durch Rechtsverordnung die Zuständigkeit auf die Landes-, Kreis- oder Sonderordnungsbehörden übertragen.

(3) Bei Gefahr im Verzug ist für unaufschiebbare Maßnahmen jedoch jede örtlich zuständige Ordnungsbehörde auch sachlich zuständig. Dies gilt nicht für Sonderordnungsbehörden. Die nach Absatz 2 zuständige Behörde ist unverzüglich zu unterrichten.

(4) Neben den örtlichen Ordnungsbehörden sind auch die Landes- und Kreisordnungsbehörden, neben den Kreisordnungsbehörden auch die Landesordnungsbehörden für den Erlass von Verordnungen über die öffentliche Sicherheit oder Ordnung zuständig, wenn sie eine einheitliche Regelung für ihren Bezirk oder für Teile ihres Bezirks für erforderlich halten. Sie können insoweit ihrer Verordnung entgegenstehende oder inhaltsgleiche Vorschriften der nachgeordneten Ordnungsbehörde aufheben.

§ 5
Örtliche Zuständigkeit der Ordnungsbehörden, Ermächtigung zum Erlass von Rechtsverordnungen

(1) Örtlich zuständig ist im Bereich ihrer sachlichen Zuständigkeit die Ordnungsbehörde, in deren Bezirk die zu schützenden Interessen verletzt oder gefährdet werden.

(2) Ist es zweckmäßig, eine Angelegenheit, die benachbarte Bezirke berührt, einheitlich zu regeln, so kann die gemeinsame Fachaufsichtsbehörde eine der beteiligten Ordnungsbehörden für allein zuständig erklären.

(3) Ist die nach Absatz 1 zuständige Ordnungsbehörde nicht ohne eine Verzögerung, durch die der Erfolg des Eingreifens beeinträchtigt würde, zu erreichen, so ist für unaufschiebbare Maßnahmen eine örtlich zuständige Ordnungsbehörde der angrenzenden Bezirke zuständig. Die nach Absatz 1 zuständige Behörde ist unverzüglich zu unterrichten.

(4) Das fachlich zuständige Ministerium kann im Einvernehmen mit dem Ministerium für Inneres und Europa durch Rechtsverordnung die örtliche Zuständigkeit der Ordnungsbehörden abweichend von den Absätzen 1 und 3 regeln.

§ 6
(aufgehoben)

§ 7
Sachliche Zuständigkeit der Polizei

(1) Die Polizei hat
1. Gefahren für die öffentliche Sicherheit oder Ordnung festzustellen und aus gegebenem Anlass zu ermitteln;
2. die zuständige Ordnungsbehörde über alle Vorgänge unverzüglich zu unterrichten, die deren Eingreifen erfordern oder für deren Entschließung von Bedeutung sein können;
3. im Einzelfall zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung selbständig diejenigen Maßnahmen zu treffen, die sie nach pflichtgemäßem Ermessen für unaufschiebbar hält;
4. im Rahmen der Gefahrenabwehr auch Straftaten zu verhüten und für die Verfolgung künftiger Straftaten vorzusorgen (vorbeugende Bekämpfung von Straftaten) sowie andere Vorbereitungen zu treffen, um künftige Gefahren abwehren zu können.

(2) Die Polizei leistet anderen Behörden Vollzugshilfe (§§ 82a bis 82c).

§ 8
Örtliche Zuständigkeit der Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten

Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte sind befugt, Amtshandlungen im gesamten Landesgebiet und in den Hoheitsgewässern vorzunehmen. Soweit sie im Bezirk einer Behörde der Polizei tätig werden, der sie nicht zugeteilt sind, gelten ihre dienstlichen Handlungen als Maßnahme dieser Behörde.

§ 9
Amtshandlungen von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten eines anderen Landes oder des Bundes oder anderer Staaten sowie von Zollbediensteten in den Vollzugsbereichen der Zollverwaltung

(1) Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte eines anderen Landes oder des Bundes können in Mecklenburg-Vorpommern Amtshandlungen vornehmen

1. auf Anforderung oder mit Zustimmung der zuständigen mecklenburg-vorpommerschen Behörde;
2. in den Fällen des Artikels 35 Absatz 2 und 3 und des Artikels 91 Absatz 1 des Grundgesetzes;
3. zur Abwehr einer gegenwärtigen erheblichen Gefahr, zur Verfolgung von Straftaten auf frischer Tat sowie zur Verfolgung und Wiederergreifung Entwichener, wenn die zuständige mecklenburg-vorpommersche Behörde die erforderlichen Maßnahmen nicht rechtzeitig treffen kann;
4. zur Erfüllung polizeilicher Aufgaben bei Gefangenentransporten;
5. zur Verfolgung von Straftaten und Ordnungswidrigkeiten und zur Gefahrenabwehr in den durch Verwaltungsabkommen, Staatsvertrag oder Gesetz geregelten Fällen.

In den Fällen des Satzes 1 Nummer 3 bis 5 ist die zuständige Polizeidienststelle unverzüglich zu unterrichten.

(2) Werden Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte nach Absatz 1 tätig, haben sie die gleichen Befugnisse wie Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte des Landes Mecklenburg-Vorpommern. Ihre Maßnahmen gelten als Maßnahmen derjenigen Polizeibehörde, in deren örtlichem und sachlichem Zuständigkeitsbereich sie tätig geworden sind; sie unterliegen insoweit deren Weisungen.

(3) Besondere Rechtsvorschriften über die Zuständigkeit von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten des Bundes bleiben unberührt.

(4) Absatz 1 und 2 gelten für Zollbedienstete in den Vollzugsbereichen der Zollverwaltung, denen der Gebrauch von Schusswaffen bei Anwendung des unmittelbaren Zwangs bei Ausübung öffentlicher Gewalt gestattet ist, entsprechend.

(5) Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte anderer Staaten können in Mecklenburg-Vorpommern Amtshandlungen vornehmen, soweit dies durch völkerrechtliche Vereinbarungen oder nach Maßgabe von Rechtsakten der Europäischen Union vorgesehen ist. Sie können nur mit solchen Amtshandlungen betraut werden, die auch von den Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten des Landes Mecklenburg-Vorpommern vorgenommen werden dürfen.

§ 10
Amtshandlungen von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten außerhalb Mecklenburg-Vorpommerns

(1) Die Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten des Landes Mecklenburg-Vorpommern dürfen außerhalb des Landes im Zuständigkeitsbereich eines anderen Landes oder des Bundes nur unter den Voraussetzungen, die § 9 Absatz 1 entsprechen, und im Falle des Artikels 91 Absatz 2 des Grundgesetzes sowie nur dann tätig werden, wenn das dort geltende Recht es vorsieht. Außerhalb der Bundesrepublik Deutschland dürfen Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte des Landes Mecklenburg-Vorpommern tätig werden, soweit dies durch völkerrechtliche Vereinbarungen oder nach Maßgabe von Rechtsakten der Europäischen Union vorgesehen ist.

(2) Einer Anforderung von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten durch ein anderes Land oder durch den Bund ist zu entsprechen, wenn die Anforderung alle für die Entscheidung wesentlichen Merkmale des Einsatzauftrages enthält und soweit nicht die Verwendung der Polizei im eigenen Lande dringlicher ist als die Unterstützung der Polizei des anderen Landes oder des Bundes.

§ 11
Zusammenarbeit von Ordnungsbehörden und Polizei

Die Ordnungsbehörden und die Polizei arbeiten im Rahmen ihrer sachlichen Zuständigkeit zusammen und unterrichten sich gegenseitig über Vorkommnisse und Maßnahmen von Bedeutung. Näheres, insbesondere über die Zusammenarbeit im Rahmen der Vollzugshilfe, regelt das Ministerium für Inneres und Europa im Einvernehmen mit dem fachlich zuständigen Ministerium durch Verwaltungsvorschrift.

Abschnitt 2
Maßnahmen zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung (§§ 12 - 24)

§ 12
Grundsatz

(1) Die Ordnungsbehörden und Polizei führen die Aufgabe der Gefahrenabwehr nach den hierfür erlassenen besonderen Gesetzen und Rechtsverordnungen durch.

(2) Nur soweit solche besonderen Gesetze und Rechtsverordnungen fehlen oder eine abschließende Regelung nicht enthalten, gelten für die Durchführung der Gefahrenabwehr die §§ 13 bis 78.

§ 13
Allgemeine Befugnisse

Die Ordnungsbehörden und die Polizei haben im Rahmen der geltenden Gesetze die nach pflichtgemäßem Ermessen notwendigen Maßnahmen zu treffen, um von der Allgemeinheit oder dem Einzelnen Gefahren abzuwehren, durch die die öffentliche Sicherheit oder Ordnung bedroht wird.

§ 14
Ermessen

(1) Die Ordnungsbehörden und die Polizei entscheiden über die von ihnen zu treffenden notwendigen Maßnahmen zur Gefahrenabwehr nach sachlichen Gesichtspunkten unter Abwägung der öffentlichen Belange und der Interessen des Einzelnen, soweit Rechtsvorschriften nicht bestimmen, dass oder in welcher Weise sie tätig zu werden haben (pflichtgemäßes Ermessen).

(2) Den Betroffenen ist auf Antrag zu gestatten, ein anderes ebenso wirksames Mittel anzuwenden, sofern die Allgemeinheit dadurch nicht stärker beeinträchtigt wird. Der Antrag kann nur innerhalb der Frist gestellt werden, die den Betroffenen zur Abwehr der Gefahr gesetzt wurde.

§ 15
Grundsatz der Verhältnismäßigkeit

(1) Von mehreren möglichen und geeigneten Maßnahmen haben die Ordnungsbehörden und die Polizei diejenigen Maßnahmen zu treffen, die den Einzelnen und die Allgemeinheit voraussichtlich am wenigsten beeinträchtigen. Kommen dabei mehrere Mittel in Betracht, so genügt es, wenn eines davon bestimmt wird.

(2) Eine Maßnahme darf nicht zu einem Nachteil führen, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht.

(3) Eine Maßnahme ist nur solange zulässig, bis ihr Zweck erreicht ist oder sich zeigt, dass er nicht erreicht werden kann.

§ 16
Verfügungen

(1) Verfügungen (Ordnungs- und Polizeiverfügungen) als Maßnahmen zur Gefahrenabwehr, die in die Rechte des Einzelnen eingreifen, sind, sofern nicht die nachfolgenden Vorschriften, ein besonderes Gesetz oder eine Verordnung über die öffentliche Sicherheit oder Ordnung die Befugnisse der Polizei und der Ordnungsbehörden besonders regeln, nur zulässig, soweit sie

1. zur Beseitigung einer Störung der öffentlichen Sicherheit oder Ordnung oder
2. zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für die öffentliche Sicherheit oder Ordnung

erforderlich sind.

(2) Ordnungs- und Polizeiverfügungen sind Verwaltungsakte im Sinne des § 35 des Landesverwaltungsverfahrensgesetzes.

§ 17
Verordnungen über die öffentliche Sicherheit oder Ordnung

(1) Die Landes-, Kreis- und örtlichen Ordnungsbehörden können zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung Verordnungen erlassen (Verordnungen über die öffentliche Sicherheit oder Ordnung).

(2) Die Verordnungen über die öffentliche Sicherheit oder Ordnung des Landes werden von den Landesbehörden, die der Landkreise werden vom Landrat erlassen (Kreisverordnungen). Verordnungen über die öffentliche Sicherheit oder Ordnung kreisfreier Städte stehen Kreisverordnungen gleich.

(3) Die Verordnungen über die öffentliche Sicherheit oder Ordnung der kreisfreien und der großen kreisangehörigen Städte, der amtsfreien Gemeinden und der Ämter (Stadt-, Gemeinde- und Amtsverordnungen) werden vom Oberbürgermeister, Bürgermeister oder Amtsvorsteher für das Gemeinde- oder Amtsgebiet oder für Teile von ihnen erlassen.

(4) Landesordnungsbehörden dürfen Verordnungen über die öffentliche Sicherheit oder Ordnung nur erlassen, wenn eine einheitliche Regelung für das ganze Land oder für Landesteile, die mehr als einen Landkreis oder eine kreisfreie Stadt umfassen, geboten ist. Die Kreisordnungsbehörden dürfen Verordnungen über die öffentliche Sicherheit oder Ordnung nur erlassen, wenn eine einheitliche Regelung für den Landkreis oder für Gebiete, die mehr als eine Gemeinde umfassen, geboten ist.

§ 18
Inhalt der Verordnungen über die öffentliche Sicherheit oder Ordnung

(1) Verordnungen über die öffentliche Sicherheit oder Ordnung müssen ihrem Inhalt nach bestimmt sein.

(2) Verweisungen auf Bekanntmachungen, Festsetzungen oder sonstige Anordnungen außerhalb von Gesetzen und Rechtsverordnungen sind unzulässig, soweit diese Anordnungen Gebote oder Verbote von unbeschränkter Dauer enthalten.

§ 19
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig einer aufgrund des § 17 erlassenen Verordnung zuwiderhandelt, soweit sie für einen bestimmten Tatbestand auf diese Bußgeldvorschrift verweist.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 5 000 Euro geahndet werden.

(3) Verwaltungsbehörden im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten sind die Landräte, die Oberbürgermeister beziehungsweise Bürgermeister für die kreisfreien und großen kreisangehörigen Städte, die Bürgermeister der amtsfreien Gemeinden und die Amtsvorsteher der Ämter jeweils für die Verfolgung und Ahndung von Zuwiderhandlungen gegen eine von ihnen aufgrund von § 17 erlassene Verordnung. Für die Verfolgung und Ahndung von Zuwiderhandlungen gegen Verordnungen einer Landesordnungsbehörde über die öffentliche Sicherheit oder Ordnung sind die Landräte und die Oberbürgermeister der kreisfreien Städte zuständig, soweit keine andere Behörde bestimmt ist.

(4) Gegenstände, auf die sich die Ordnungswidrigkeit bezieht oder die zu ihrer Vorbereitung oder Begehung verwendet worden sind, können eingezogen werden, soweit die Verordnung für einen bestimmten Tatbestand auf diese Vorschrift verweist.

§ 20
Verhältnis zu anderen Rechtsvorschriften; Genehmigungspflicht

(1) Verordnungen über die öffentliche Sicherheit oder Ordnung dürfen keine Bestimmungen enthalten, die mit Gesetzen und Rechtsverordnungen in Widerspruch stehen. Stadt-, Gemeinde-, Kreis- und Amtsverordnungen dürfen keine Bestimmungen enthalten, die mit Verordnungen über die öffentliche Sicherheit oder Ordnung einer Landesordnungsbehörde in Widerspruch stehen. Dies gilt entsprechend für Stadt-, Gemeinde- und Amtsverordnungen im Verhältnis zu Kreisverordnungen.

(2) Eine Verordnung über die öffentliche Sicherheit oder Ordnung einer Landesordnungsbehörde darf durch Stadt-, Gemeinde-, Kreis- oder Amtsverordnung nur ergänzt werden, soweit die Verordnung einer Landesordnungsbehörde dies ausdrücklich zulässt. Dies gilt entsprechend für Stadt-, Gemeinde- und Amtsverordnungen im Verhältnis zu Kreisverordnungen.

(3) Verordnungen über die öffentliche Sicherheit oder Ordnung der Landkreise und der kreisfreien sowie der großen kreisangehörigen Städte bedürfen der Genehmigung des Ministeriums für Inneres und Europa, die der Ämter und der amtsfreien Gemeinden bedürfen der Genehmigung des Landrates. Die Ausfertigung der nach Satz 1 genehmigungsbedürftigen Verordnungen erfolgt nach Erteilung der Genehmigung.

§ 21
Form der Verordnungen über die öffentliche Sicherheit oder Ordnung

(1) Die Verordnungen über die öffentliche Sicherheit oder Ordnung müssen
1. als Kreis-, Stadt-, Gemeinde- oder Amtsverordnung in der Überschrift entsprechend gekennzeichnet sein,
2. die Rechtsvorschriften angeben, welche die Ermächtigung zum Erlass der Verordnung enthalten,
3. auf die erteilte Genehmigung, Zustimmung oder das Einvernehmen mit anderen Stellen hinweisen, soweit dies gesetzlich vorgeschrieben ist,
4. das Datum angeben, unter dem sie ausgefertigt sind, und
5. die Behörde bezeichnen, die die Verordnung erlassen hat.

(2) Verordnungen über die öffentliche Sicherheit oder Ordnung sollen
1. in der Überschrift ihren wesentlichen Inhalt kennzeichnen und
2. den örtlichen Geltungsbereich und die Geltungsdauer angeben. Ist der Geltungsbereich nicht angegeben, so gelten die Verordnungen für den gesamten Bezirk der Behörde.

§ 22
Geltungsdauer

(1) Verordnungen über die öffentliche Sicherheit oder Ordnung sollen eine Beschränkung ihrer Geltungsdauer enthalten. Die Geltung darf nicht über 20 Jahre hinaus erstreckt werden. Verordnungen, die keine Beschränkung der Geltungsdauer enthalten, treten 20 Jahre nach ihrem Inkrafttreten außer Kraft.

(2) Absatz 1 findet keine Anwendung auf Verordnungen über die öffentliche Sicherheit oder Ordnung, durch die Verordnungen über die öffentliche Sicherheit oder Ordnung abgeändert oder aufgehoben werden.

§ 23
Amtliche Bekanntmachung

(1) Verordnungen über die öffentliche Sicherheit oder Ordnung einer Landesordnungsbehörde sind im Gesetz- und Verordnungsblatt für Mecklenburg-Vorpommern zu verkünden.

(2) Stadt-, Gemeinde-, Kreis- und Amtsverordnungen sind örtlich in der für Satzungen bestimmten Weise zu verkünden.

(3) Bei Gefahr im Verzug kann die Verkündung durch Bekanntmachung in Tageszeitungen, im Hörfunk, im Fernsehen, im Internet, durch Lautsprecher oder in anderer ortsüblicher Art ersetzt werden (Ersatzverkündung). Die Verordnung über die öffentliche Sicherheit oder Ordnung ist sodann unverzüglich nach Absatz 1 oder 2 bekanntzumachen. Hierbei sind der Zeitpunkt und die Art der Ersatzverkündung anzugeben.

§ 24
Inkrafttreten der Verordnungen über die öffentliche Sicherheit oder Ordnung

Verordnungen über die öffentliche Sicherheit oder Ordnung treten, soweit in ihnen nichts anderes bestimmt ist, am Tage nach ihrer Verkündung in Kraft.

Abschnitt 3
Verarbeitung personenbezogener Daten (§§ 25 - 49)

Unterabschnitt 1
Grundsätze der Verarbeitung (§§ 25 - 26b)

§ 25
Bestimmungen zur Anwendbarkeit der Vorschriften dieses Gesetzes im Anwendungsbereich der Verordnung (EU) 2016/679 und des Landesdatenschutzgesetzes

(1) Die Vorschriften zur Datenverarbeitung nach diesem Gesetz gelten in Anwendung der Artikel 6 Absatz 2 und 3 jeweils in Verbindung mit Absatz 1 Buchstabe e sowie Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, L 314 vom 22.11.2016, S. 72, L 127 vom 23.5.2018, S. 2) auch für die Erfüllung von ordnungsbehördlichen und polizeilichen Aufgaben, die in den Anwendungsbereich der Verordnung (EU) 2016/679 fallen. Dies gilt nicht, soweit diese Vorschriften bereits auf den Anwendungsbereich der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89, L 127 vom 23.5.2018, S. 9) beschränkt sind und soweit die Definitionen in § 3 Absatz 4 und 5 denen des Artikels 4 der Verordnung (EU) 2016/679 entsprechen.

(2) Zur Schaffung einer kohärenten Regelungslage im Bereich des Gefahrenabwehrrechtes werden zu folgenden Regelungen der Verordnung (EU) 2016/679 spezifische Bestimmungen im Sinne des Artikels 6 Absatz 2 und 3 jeweils in Verbindung mit Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 erlassen und zwar

1. mit § 3 Absatz 4 Nummer 1 zu Artikel 4 Nummer 7.
2. mit § 3 Absatz 5 Nummer 3 Buchstabe c zu Artikel 9 Absatz 1.
3. mit § 25a Absatz 1 zu Artikel 6 Absatz 1 Buchstabe e.
4. mit § 25a Absatz 2 zu Artikel 5 Absatz 1 Buchstabe a, b und e.
5. mit § 25a Absatz 3 Satz 1, Absatz 4 Satz 1 und Absatz 7 sowie mit § 46j zu Artikel 5 Absatz 1 Buchstabe a.
6. mit § 25a Absatz 5 zu den Artikeln 13 und 14.
7. mit § 26 zu Artikel 7.
8. mit den §§ 27 Absatz 1 bis 3, 37a und 42 Absatz 1, 2 und 4 zu Artikel 6 Absatz 1 Buchstabe e.
9. mit § 27 Absatz 4 zu Artikel 6 Absatz 1 Buchstabe e und zu Artikel 9 Absatz 2 Buchstabe g.
10. mit § 36 zu Artikel 6 Absatz 1 Buchstabe e und Absatz 4.
11. mit § 37 zu Artikel 10.
12. mit den §§ 39 bis 39c zu Artikel 5 Absatz 1 Buchstabe a, b und d.
13. mit § 42 Absatz 3 zu Artikel 26 Absatz 2 Satz 2.
14. mit den §§ 42 Absatz 6 und 45c Absatz 3 und 4 zu Artikel 30.
15. mit den §§ 45 und 45a zu Artikel 5 Absatz 1 Buchstabe d.
16. mit § 45b zu Artikel 35.
17. mit den §§ 46d bis 46f zu Artikel 5 Absatz 1 Buchstabe a und b und zu Artikel 31.

18. mit § 46g zu Artikel 5 Absatz 1 Buchstabe a und b.
19. mit § 46h zu Artikel 25.
20. mit § 46i zu Artikel 5 Absatz 1 Buchstabe f und zu Artikel 32.
21. mit § 46k zu Artikel 28.
22. mit § 47 zu Artikel 77 Absatz 1.
23. mit § 48a zu Artikel 16 bis 19.
24. mit § 48b Absatz 6 Satz 2 zu Artikel 57 Absatz 1 Buchstabe a.
25. mit § 48c zu Artikel 31 und zu Artikel 36.
26. mit § 48d zu Artikel 33.
27. mit den §§ 48e, 48f, 48g Absatz 2 bis 4 zu den Artikeln 37 bis 39.
28. mit § 48h zu Artikel 5 Absatz 1 Buchstabe a.

(3) Ferner
1. wird mit § 25a Absatz 3 Satz 2 und Absatz 4 Satz 2 der Artikel 5 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 beschränkt nach Artikel 23 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679,
2. wird mit § 25a Absatz 6 der Artikel 22 der Verordnung (EU) 2016/679 beschränkt nach Artikel 23 Absatz 1 Buchstabe i der Verordnung (EU) 2016/679,
3. werden mit den §§ 46a und 46b zu Artikel 14 Absatz 5 Buchstabe b der Verordnung (EU) 2016/679 spezifische Bestimmungen im Sinne des Artikels 6 Absatz 2 und 3 jeweils in Verbindung mit Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 erlassen und zudem wird Artikel 14 beschränkt im Sinne des Artikels 23 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679,
4. werden mit § 46c zu Artikel 34 der Verordnung (EU) 2016/679 spezifische Bestimmungen im Sinne des Artikels 6 Absatz 2 und 3 jeweils in Verbindung mit Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 erlassen und § 46c enthält zudem Beschränkungen im Sinne des Artikels 23 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679 und
5. werden mit § 48 zu Artikel 15 der Verordnung (EU) 2016/679 spezifische Bestimmungen im Sinne des Artikels 6 Absatz 2 und 3 jeweils in Verbindung mit Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 erlassen und § 48 enthält zudem Beschränkungen im Sinne des Artikels 23 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679.

(4) Mit den übrigen Vorschriften zur Datenverarbeitung im Sinne des Absatzes 1 werden zu Artikel 6 Absatz 1 der Verordnung (EU) 2016/679 spezifische Bestimmungen im Sinne des Artikels 6 Absatz 2 und 3 jeweils in Verbindung mit Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 erlassen.

(5) Soweit in diesem Gesetz nichts Besonderes geregelt ist, findet das Landesdatenschutzgesetz ergänzend Anwendung.

§ 25a
Allgemeine Grundsätze

(1) Die Ordnungsbehörden und die Polizei dürfen personenbezogene Daten zum Zwecke der Gefahrenabwehr verarbeiten, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist und
1. die Art und der Umfang des Umgangs mit den personenbezogenen Daten durch Gesetz ausdrücklich zugelassen ist oder
2. die betroffene Person gemäß § 26 eingewilligt hat.

(2) Die verantwortliche Stelle hat bei der Verarbeitung personenbezogener Daten so weit wie möglich zwischen den verschiedenen Kategorien betroffener Personen zu unterscheiden. Es sind insbesondere die in § 27 Absatz 1 und 3 jeweils aufgeführten Kategorien zu bilden.

(3) Personenbezogene Daten sind bei der betroffenen Person zu erheben. Bei Behörden und anderen öffentlichen Stellen oder bei Personen und Stellen außerhalb der öffentlichen Verwaltung dürfen sie nur erhoben werden, wenn die Erhebung bei der betroffenen Person nicht oder nicht rechtzeitig möglich ist oder sonst die Erfüllung der jeweiligen polizeilichen oder ordnungsbehördlichen Aufgabe erheblich erschwert oder gefährdet werden würde.

(4) Personenbezogene Daten sind offen zu erheben. Eine Erhebung, die nicht als polizeiliche oder ordnungsbehördliche Maßnahme erkennbar sein soll, ist nur zulässig, wenn sonst die Erfüllung polizeilicher oder ordnungsbehördlicher Aufgaben erheblich gefährdet werden würde oder wenn anzunehmen ist, dass dies im Interesse der betroffenen Person ist.

(5) Werden personenbezogene Daten bei der betroffenen Person oder bei Dritten (§ 3 Absatz 4 Nummer 1) aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, so sind diese hierauf, sonst auf die Freiwilligkeit ihrer Auskunft, auf bestehende Auskunftsverweigerungsrechte und auf Verlangen auf die Rechtsgrundlage für die Erhebung hinzuweisen.

(6) Eine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung, einschließlich Profiling, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt, ist nur zulässig, wenn sie in diesem Gesetz vorgesehen ist. Entscheidungen nach Satz 1 dürfen nicht auf besonderen Kategorien personenbezogener Daten beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechtsgüter sowie der berechtigten Interessen der betroffenen Personen getroffen wurden. Profiling, das zur Folge hat, dass betroffene Personen auf der Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist verboten. Kinder dürfen von keinen Maßnahmen nach Satz 1 betroffen sein.

(7) Die verantwortliche Stelle hat bei der Verarbeitung so weit wie möglich danach zu unterscheiden, ob personenbezogene Daten auf Tatsachen oder auf persönlichen Einschätzungen beruhen. Zu diesem Zweck hat sie, soweit dies im Rahmen der jeweiligen Verarbeitung möglich und angemessen ist, Beurteilungen, die auf persönlichen Einschätzungen beruhen, als solche kenntlich zu machen. Es muss außerdem feststellbar sein, welche Stelle die Unterlagen führt, die der auf einer persönlichen Einschätzung beruhenden Beurteilung zugrunde liegen.

§ 25b
Gerichtliche Zuständigkeit, Verfahren

Wird in diesem Gesetz eine richterliche Entscheidung bestimmt, ist das Amtsgericht zuständig, in dessen Bezirk die die Maßnahme durchführende Ordnungsbehörde oder Polizeibehörde ihren Sitz hat. Für das Verfahren findet das Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechende Anwendung. Satz 1 und 2 gelten nicht, soweit dieses Gesetz die gerichtliche Zuständigkeit oder das Verfahren abweichend regelt. Gegen die Entscheidung des Gerichtes ist auch die Beschwerde der beantragenden Behörde zulässig. Die Rechtsbeschwerde findet nicht statt. Die Entscheidung des Gerichtes bedarf zu ihrer Wirksamkeit auch dann nicht der Anhörung der betroffenen Person und der Bekanntgabe an die betroffene Person, soweit der Zweck der Maßnahme durch diese gefährdet würde. § 77 bleibt unberührt.

§ 26
Einwilligung

(1) Die Verarbeitung personenbezogener Daten kann auch auf Grundlage einer Einwilligung der betroffenen Person erfolgen. Unter Berücksichtigung der Umstände des Einzelfalles kann diese schriftlich, entsprechend § 3a des Landesverwaltungsverfahrensgesetzes auf elektronischem Wege oder mündlich erfolgen. Die verantwortliche Stelle muss die Einwilligung der betroffenen Person nachweisen können.

(2) Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich eingeholt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild des Schriftstücks hervorzuheben und sprachlich derart abzufassen, dass eine eindeutige Zuordnung zu dem die Einwilligung betreffenden Teil durch die betroffene Person möglich ist.

(3) Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

(4) Die betroffene Person ist vor Abgabe der Einwilligung in geeigneter Weise über die Bedeutung und Tragweite der Einwilligung, insbesondere über die Art und den Umfang der Verarbeitung sowie über Empfänger beabsichtigter Übermittlungen von Daten, aufzuklären. Die Anschrift der datenverarbeitenden Stelle ist ihm mitzuteilen.

(5) Die betroffene Person ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass sie die Einwilligung verweigern und mit Wirkung für die Zukunft jederzeit widerrufen kann. An die Form des Widerrufs dürfen keine höheren Anforderungen als an die der Erteilung der Einwilligung gestellt werden.

(6) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden.

§ 26a
Schutz des Kernbereiches privater Lebensgestaltung

(1) Rechtfertigen Tatsachen die Annahme, dass durch eine Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist diese unzulässig.

(2) Werden durch eine Maßnahme auch Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt, dürfen diese nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen und die Tatsache ihrer Erlangung und Löschung ist gemäß § 46d zu dokumentieren; für die Protokollierung gilt § 46e. Die Dokumentation und entsprechende Protokollierung dürfen ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden; sie sind frühestens nach Abschluss der Datenschutzkontrolle § 48b Absatz 6 und spätestens nach vierundzwanzig Monaten zu löschen.

(3) Dürfen Daten nach diesem Gesetz erhoben werden und rechtfertigen während der Erhebung Tatsachen die Annahme, dass Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erfasst werden, ist die Maßnahme abzubrechen; dies gilt nicht, sofern mit dem Abbruch der Maßnahme eine Gefährdung der eingesetzten Polizeibeamtinnen und Polizeibeamten oder Vertrauenspersonen oder ihrer weiteren Verwendung verbunden wäre. Soweit Daten aufgezeichnet werden, ist der Aufzeichnungsvorgang, soweit dies technisch möglich ist, unverzüglich zu unterbrechen. Nach einer Unterbrechung darf die Datenerhebung und -aufzeichnung nur fortgesetzt werden, wenn aufgrund geänderter Umstände davon ausgegangen werden kann, dass die Gründe, die zur Unterbrechung geführt haben, nicht mehr vorliegen. Die Tatsache der Unterbrechung und der Fortsetzung ist zu dokumentieren oder zu protokollieren; Absatz 2 Satz 3 gilt entsprechend.

(4) Soweit in diesem Gesetz nichts Besonderes geregelt ist, ist vor einer Verwendung von Daten in oder aus Wohn- oder Geschäftsräumen oder in oder von befriedetem Besitztum die Rechtmäßigkeit dieser Datenerhebung zuvor richterlich festzustellen. Bei Gefahr im Verzug entscheidet über die Verwendung die Behördenleitung oder eine von ihr besonders beauftragte Beamtin oder ein von ihr besonders beauftragter Beamter; eine richterliche Entscheidung ist unverzüglich nachzuholen. Sind in den Fällen des Satzes 2 Daten an andere Stellen übermittelt worden und wurde die Rechtmäßigkeit dieser Datenerhebung nicht richterlich bestätigt, ist § 45 Absatz 5 zu beachten.

(5) Soweit in diesem Gesetz nichts Besonderes geregelt ist, sind vor einer Verwendung von Daten in Fällen einer Unterbrechung nach Absatz 3, die nicht bereits von Absatz 4 erfasst werden, die erhobenen Daten der oder dem behördlichen Datenschutzbeauftragten zur Auswertung und Entscheidung über die Rechtmäßigkeit dieser Datenerhebung vorzulegen. Absatz 4 Satz 2 gilt entsprechend. Sind in den Fällen des Satzes 2 Daten an andere Stellen übermittelt worden und wurde die Rechtmäßigkeit dieser Datenerhebung nicht von der oder dem behördlichen Datenschutzbeauftragten festgestellt, ist § 45 Absatz 5 zu beachten.

§ 26b
Schutz von zeugnisverweigerungsberechtigten Personen

(1) Maßnahmen zur Datenerhebung, die sich gegen eine in § 53 Absatz 1 der Strafprozessordnung genannten Berufsgeheimnisträger richten und voraussichtlich Erkenntnisse erbringen würden, über die diese Person das Zeugnis verweigern dürfte, sind unzulässig. § 28 Absatz 2 bleibt unberührt. Dennoch erlangte Erkenntnisse dürfen nicht verwertet werden. Für die Dokumentation, Protokollierung und Löschung ist § 26a Absatz 2 Satz 2 und 3 anzuwenden. Die Sätze 2 bis 4 gelten entsprechend, wenn durch eine Maßnahme, die sich nicht gegen einen in § 53 Absatz 1 der Strafprozessordnung genannten Berufsgeheimnisträger richtet, von einer dort genannten Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte.

(2) Maßnahmen zur Datenerhebung, durch die ein Berufsgeheimnisträger betroffen wäre und dadurch voraussichtlich Erkenntnisse erlangt würden, über die diese Person das Zeugnis verweigern dürfte, sind abweichend von Absatz 1 zulässig, soweit dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit erforderlich ist. Dies gilt nicht für Berufsgeheimnisträger nach § 53 Absatz 1 Satz 1 Nummer 1, 2 und 4 der Strafprozessordnung sowie für einen Rechtsanwalt, eine nach § 206 der Bundesrechtsanwaltsordnung in eine Rechtsanwaltskammer aufgenommene Person oder einen Kammerrechtsbeistand. Nach Satz 1 erhobene Daten dürfen nur für den dort bezeichneten Zweck verwendet werden.

(3) Die Absätze 1 und 2 gelten entsprechend, soweit die in § 53a der Strafprozessordnung Genannten das Zeugnis verweigern dürften.

(4) Die Absätze 1 bis 3 gelten nicht, sofern Tatsachen die Annahme rechtfertigen, dass die zeugnisverweigerungsberechtigte Person für die Gefahr verantwortlich ist.

Unterabschnitt 2
Maßnahmen der Datenerhebung (§§ 27 - 35)

§ 27
Allgemeine Befugnisse zur Datenerhebung

(1) Zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr können personenbezogene Daten erhoben werden über

1. die in den §§ 69 und 70 genannten Personen und, unter den Voraussetzungen des § 71, über die dort genannten Personen,
2. geschädigte, hilflose oder vermisste Personen sowie deren Angehörige, gesetzliche Vertreter oder Vertrauenspersonen,
3. gefährdete Personen,
4. Zeuginnen und Zeugen, Hinweisgeberinnen und Hinweisgeber oder sonstige Auskunftspersonen,
5. unbekannte Personen und
6. Tote.

(2) Zur Vorbereitung für die Hilfeleistung und das Handeln in Gefahrenfällen können von
1. Personen, deren besondere Kenntnisse oder Fähigkeiten zur Gefahrenabwehr benötigt werden,
2. Verantwortlichen für Anlagen oder Einrichtungen, von denen eine erhebliche Gefahr ausgehen kann,
3. Verantwortlichen für gefährdete Anlagen oder Einrichtungen und
4. Verantwortlichen für Veranstaltungen in der Öffentlichkeit, die nicht dem Versammlungsgesetz unterliegen,

Namen, Vornamen, akademische Grade, Anschriften, Telefonnummern und andere personenbezogene Daten über die Erreichbarkeit sowie nähere Angaben über die Zugehörigkeit zu einer der genannten Personengruppen aus allgemein zugänglichen Quellen, bei Behörden oder aufgrund freiwilliger Angaben der betroffenen Person erhoben werden. Eine verdeckte Datenerhebung ist nicht zulässig. Kommt es im Zusammenhang mit einem Gefahrenfall zur Begehung einer Straftat oder Ordnungswidrigkeit, so dürfen die nach Satz 1 Nummer 2 bis 4 erhobenen personenbezogenen Daten zur Verfolgung einer solchen Straftat oder Ordnungswidrigkeit verarbeitet werden. Werden die nach Satz 1 Nummer 4 erhobenen personenbezogenen Daten nicht nach Satz 3 verwendet, sind sie spätestens einen Monat nach Beendigung des Anlasses ihrer Erhebung zu löschen.

(3) Bestehen tatsächliche Anhaltspunkte für die künftige Begehung von Straftaten von erheblicher Bedeutung (§ 49) oder von terroristischen Straftaten (§ 67c), kann die Polizei personenbezogene Daten erheben über
1. Personen, bei denen tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass sie künftig solche Straftaten begehen oder sich an solchen beteiligen werden,
2. Personen, die mit einer Person nach Nummer 1 in nicht nur flüchtigem oder in zufälligem Kontakt stehen und
   a) von der Vorbereitung einer Straftat nach Satz 1 Kenntnis haben,
   b) aus der Verwertung der Tat Vorteile ziehen könnten oder
   c) die Person nach Nummer 1 sich ihrer zur Begehung der Straftat bedienen könnte

   und die Verhütung dieser Straftaten auf andere Weise aussichtslos oder wesentlich erschwert wäre,
3. Personen, bei denen tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass sie Opfer solcher Straftaten werden, oder
4. Zeuginnen und Zeugen, Hinweisgeberinnen und Hinweisgeber oder sonstige Auskunftspersonen, die dazu beitragen können, den Sachverhalt solcher Straftaten aufzuklären.

(4) In den Fällen des Absatzes 1 Nummer 1 bis 3, 5 und 6 sowie des Absatzes 3 Nummer 1 und 2 kann die Polizei auch ohne Einwilligung nach § 26 besondere Kategorien personenbezogener Daten im Sinne des § 3 Absatz 5 Nummer 3 erheben, sofern die Kenntnis dieser Daten zur Abwehr der Gefahr für die öffentliche Sicherheit im jeweiligen Einzelfall zwingend erforderlich ist. Für die Ordnungsbehörden gilt Satz 1 ausschließlich in den Fällen des Absatzes 1 Nummer 1 bis 3, 5 und 6.

(5) Die Polizei sowie Behörden, die Aufgaben der Hilfs- und Rettungsdienste wahrnehmen, können fernmündlich an sie gerichtete Notrufe und über Notrufeinrichtungen eingehende sonstige Mitteilungen aufzeichnen; ausgehende Gespräche können aufgezeichnet werden, sofern sie mit der Bearbeitung des Notrufs in Zusammenhang stehen. Im Übrigen ist eine Aufzeichnung von Anrufen zulässig, soweit dies im Einzelfall zur polizeilichen Aufgabenerfüllung erforderlich ist. Die oder der Anrufende soll auf die Aufzeichnung nach Satz 2 hingewiesen werden, soweit dadurch die Aufgabenerfüllung nicht gefährdet wird. Die Aufzeichnungen nach Satz 1 sind spätestens sechs Monate, die Aufzeichnungen nach Satz 2 spätestens eine Woche nach ihrer Erhebung zu löschen. Dies gilt nicht, sofern die Daten zur Verfolgung von Straftaten oder Ordnungswidrigkeiten oder zur Erfüllung der in § 1 bezeichneten Aufgaben benötigt werden.

§ 27a
Polizeiliche Anhalte- und Sichtkontrollen

Die Polizei darf
1. im öffentlichen Verkehrsraum zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung (§ 49) oder terroristischer Straftaten (§ 67c) oder
2. im Grenzgebiet bis zu einer Tiefe von 30 Kilometern, in öffentlichen Einrichtungen des internationalen Verkehrs mit unmittelbarem Grenzbezug, im Küstenmeer sowie in den inneren Gewässern zur vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität oder zur Unterbindung des unerlaubten Aufenthalts

Personen kurzzeitig anhalten und mitgeführte Fahrzeuge, insbesondere deren Kofferräume und Ladeflächen, in Augenschein nehmen. Maßnahmen nach Satz 1 Nummer 1 werden durch die Leitung der zuständigen Polizeibehörde oder durch eine von ihr besonders beauftragte Beamtin oder einen von ihr besonders beauftragten Beamten angeordnet, soweit polizeiliche Lageerkenntnisse dies rechtfertigen. Die Anordnung ergeht schriftlich, in Fällen von Gefahr im Verzug ist sie unverzüglich nachträglich zu dokumentieren. Sie ist in örtlicher und zeitlicher Hinsicht auf den zur vorbeugenden Bekämpfung der in Satz 1 Nummer 1 aufgeführten Straftaten erforderlichen Umfang zu beschränken. Die Anordnung ist auf höchstens einen Monat zu befristen und unter Angabe der Lageerkenntnisse zu begründen. Eine Verlängerung ist möglich, soweit die Anordnungsvoraussetzungen fortbestehen; Satz 2 bis 5 gelten entsprechend.

§ 28
Befragung und Auskunftspflicht

(1) Personen dürfen befragt werden, wenn aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass sie Angaben machen können, die für die Aufgabenerfüllung nach § 1 erforderlich sind. Für die Dauer der Befragung dürfen diese Personen angehalten werden.

(2) Eine Person, die nach Absatz 1 befragt wird, hat die erforderlichen Angaben zu leisten und auf Frage auch Namen, Vornamen, Tag und Ort der Geburt, Wohnanschrift und Staatsangehörigkeit anzugeben. § 136a Absatz 1 Satz 1 und 3 sowie Absatz 2 und 3 der Strafprozessordnung gilt entsprechend. § 90 findet keine Anwendung. § 26b bleibt unberührt. Unter den in den §§ 52 bis 55 der Strafprozessordnung bezeichneten Voraussetzungen ist die betroffene Person zur Verweigerung der Auskunft zur Sache berechtigt. Dies gilt nicht, soweit die Auskunft zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person erforderlich ist; insoweit erlangte Auskünfte dürfen nur zu Zwecken der Gefahrenabwehr verwendet werden. Ein Berufsgeheimnisträger nach § 53 Absatz 1 Satz 1 Nummer 1, 2 und 4 der Strafprozessordnung sowie ein Rechtsanwalt, eine nach § 206 der Bundesrechtsanwaltsordnung in eine Rechtsanwaltskammer aufgenommene Person oder ein Kammerrechtsbeistand ist auch in den Fällen des Satzes 6 zur Verweigerung der Auskunft berechtigt. Die betroffene Person ist über ihr Recht zur Verweigerung der Auskunft zu belehren.

§ 29
Identitätsfeststellung

(1) Die Identität einer Person darf zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr festgestellt werden. Darüber hinaus dürfen Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte die Identität einer Person feststellen,

1. wenn sie sich an einem Ort aufhält,
   a) für den tatsächliche Anhaltspunkte bestehen, dass
      aa) dort Personen Straftaten verabreden, vorbereiten oder verüben,
      bb) sich dort gesuchte Straftäter verbergen,
      cc) sich dort Personen treffen, die gegen aufenthaltsrechtliche Vorschriften verstoßen, oder
      dd) dort Personen dem unerlaubten Glücksspiel nachgehen oder
   b) an dem Personen der Prostitution nachgehen,
2. wenn sie sich in einer Verkehrs- oder Versorgungsanlage oder -einrichtung, einem öffentlichen Verkehrsmittel, Amtsgebäude oder in deren unmittelbarer Nähe aufhält und tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass in oder an diesem Objekt Straftaten begangen werden sollen, durch die Personen oder diese Objekte gefährdet sind,
3. wenn sie sich in einem gefährdeten Objekt oder in dessen unmittelbarer Nähe aufhält und die zuständige Polizeibehörde für dieses Objekt besondere Schutzmaßnahmen angeordnet hat oder
4. an einer Kontrollstelle, die von der Polizei eingerichtet worden ist, um folgende Straftaten zu verhüten, für deren Begehung tatsächliche Anhaltspunkte bestehen:
   a) die in §§ 125, 125a des Strafgesetzbuches genannten Straftaten,
   b) die in § 129a des Strafgesetzbuches oder die in § 67c genannten Straftaten,
   c) eine Straftat nach § 250 Absatz 1 Nummer 1 Buchstabe a, b oder Absatz 2 des Strafgesetzbuches,
   d) eine Straftat nach § 255 des Strafgesetzbuches in der Begehungsform nach § 250 Absatz 1 Nummer 1 Buchstabe a, b oder Absatz 2 des Strafgesetzbuches oder
   e) eine Straftat nach § 27 des Versammlungsgesetzes.

(2) Es dürfen die zur Feststellung der Identität erforderlichen Maßnahmen getroffen werden. Insbesondere kann verlangt werden, dass die betroffene Person Angaben zur Feststellung ihrer Identität macht sowie mitgeführte Ausweispapiere zur Prüfung aushändigt. Die betroffene Person darf angehalten werden. Vollzugsbeamtinnen und Vollzugsbeamte der Ordnungsbehörden dürfen die betroffene Person nur bis zum Eintreffen der Polizei festhalten, wenn die Identität auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann.

(3) Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte dürfen die betroffene Person festhalten oder zur Dienststelle verbringen, wenn die Identität auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann. Dabei können die betroffene Person sowie die von ihr mitgeführten Sachen zum Zwecke der Identitätsfeststellung durchsucht werden. Die betroffene Person darf nicht länger festgehalten werden, als es zur Feststellung ihrer Identität erforderlich ist. Spätestens am Ende des Tages nach dem Festhalten muss die Entlassung erfolgen, sofern nicht vorher die Fortdauer der Freiheitsentziehung gerichtlich angeordnet worden ist.

(4) § 56 gilt entsprechend mit der Maßgabe, dass die Freiheitsentziehung insgesamt drei Tage nicht überschreiten darf.

§ 30
Prüfung von Berechtigungsscheinen

Es kann verlangt werden, dass ein Berechtigungsschein zur Prüfung ausgehändigt wird, wenn die betroffene Person aufgrund einer Rechtsvorschrift oder einer vollziehbaren Auflage in einem Erlaubnisbescheid verpflichtet ist, diesen Berechtigungsschein mitzuführen. Die betroffene Person darf für die Dauer der Prüfung angehalten werden.

§ 31
Erkennungsdienstliche Maßnahmen

(1) Erkennungsdienstliche Maßnahmen dürfen angeordnet werden, wenn eine nach § 29 zulässige Identitätsfeststellung auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist. Darüber hinaus dürfen Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte die zur Verhütung oder Aufklärung einer künftigen mit Strafe bedrohten Handlung erforderlich erscheinenden erkennungsdienstlichen Maßnahmen anordnen, wenn die betroffene Person verdächtig ist, eine mit Strafe bedrohte Handlung begangen zu haben, und wenn wegen der Art oder Ausführung der Handlung die Gefahr der Begehung weiterer mit Strafe bedrohter Handlungen besteht. Die angeordneten Maßnahmen werden von der Polizei durchgeführt. Sie können auch von Ordnungsbehörden durchgeführt werden, soweit sie über die erforderlichen personellen und materiellen Voraussetzungen verfügen.

(2) Erkennungsdienstliche Maßnahmen sind insbesondere
1. die Abnahme von Fingerabdrücken und Abdrücken von Hand- oder Fußflächen,
2. die Aufnahme von Lichtbildern,
3. die Feststellung äußerer körperlicher Merkmale,
4. Messungen und
5. Tonaufzeichnungen.

(3) Ist die Identität festgestellt, dürfen die in den Fällen des Absatzes 1 Satz 1 im Zusammenhang mit der Feststellung angefallenen erkennungsdienstlichen Daten oder angefertigten Unterlagen nur dann weiterverarbeitet oder verwendet werden, wenn dies für Zwecke nach Absatz 1 Satz 2 oder nach Rechtsvorschriften anderer Gesetze zulässig ist.

(4) Das Ministerium für Inneres und Europa regelt das Nähere durch Verwaltungsvorschrift.

§ 31a
Molekulargenetische Untersuchung zur Identitätsfeststellung

(1) Die Polizei kann zur Feststellung der Identität von hilflosen Personen oder Toten deren DNA-Identifizierungsmuster mit denjenigen vermisster Personen abgleichen, wenn die Feststellung der Identität auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist. Zu diesem Zweck dürfen
1. hilflosen Personen oder Toten Körperzellen entnommen werden,
2. Proben von Gegenständen mit Spurenmaterial vermisster Personen genommen werden und
3. die Proben nach den Nummern 1 und 2 molekulargenetisch untersucht werden.

Für die Entnahme der Körperzellen gilt § 81a Absatz 1 Satz 2 der Strafprozessordnung entsprechend. Die Untersuchungen nach Satz 2 Nummer 3 sind auf die Feststellung des DNA-Identifizierungsmusters und des Geschlechts zu beschränken. Entnommene Körperzellen sind unverzüglich zu vernichten, wenn sie für die Untersuchung nach Satz 2 nicht mehr benötigt werden. Die DNA-Identifizierungsmuster können zum Zweck des Abgleichs in einem Dateisystem gespeichert werden. Sie sind unverzüglich zu löschen, wenn sie zur Identitätsfeststellung nach Satz 1 nicht mehr benötigt werden.

(2) Molekulargenetische Untersuchungen bedürfen der richterlichen Anordnung auf Antrag der Leitung der zuständigen Polizeibehörde. Im Antrag sind anzugeben:

1. soweit wie möglich eine Beschreibung zur Person, gegen die sich die Maßnahme richtet,
2. Art und Umfang der Maßnahme,
3. der Sachverhalt,
4. eine Begründung.

(3) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. soweit wie möglich eine Beschreibung zur Person, gegen die sich die Maßnahme richtet,
2. Art und Umfang der Maßnahme,
3. die Gründe.

Für die Durchführung der Untersuchungen gilt § 81f Absatz 2 der Strafprozessordnung entsprechend.

§ 32
Einsatz technischer Mittel zur offenen Bild- und Tonaufnahme sowie zur Bild- und Tonaufzeichnung

(1) Bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, können personenbezogene Daten offen auch durch den Einsatz technischer Mittel

1. zur Bild- und Tonaufzeichnung über die in § 69 und § 70 genannten Personen erhoben werden, wenn Tatsachen die Annahme rechtfertigen, dass dabei Straftaten begangen werden oder
2. zur Bildaufnahme erhoben werden, wenn Tatsachen die Annahme rechtfertigen, dass dabei Straftaten begangen werden, oder zur Übersichtsaufnahme erhoben werden, wenn dies zur Lenkung und Leitung des Einsatzes erforderlich ist. Übersichtsaufzeichnungen und die gezielte Feststellung der Identität einer auf diesen Aufzeichnungen abgebildeten Person sind nur unter den Voraussetzungen der Nummer 1 zulässig; die Identitätsfeststellung darf nur durch die Polizei erfolgen.

(2) An öffentlich zugänglichen Orten dürfen personenbezogene Daten offen mit technischen Mitteln zur Bildaufnahme erhoben werden, wenn und solange tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass an diesen ein die öffentliche Sicherheit schädigendes Ereignis in absehbarer Zeit mit hinreichender Wahrscheinlichkeit eintreten wird.

(3) Darüber hinaus dürfen personenbezogene Daten offen mit technischen Mitteln zur Bildaufzeichnung erhoben werden, soweit an öffentlich zugänglichen Orten wiederholt Straftaten begangen worden sind und Tatsachen die Annahme rechtfertigen, dass dort künftig mit der Begehung von Straftaten zu rechnen ist.

(4) An oder in den in § 29 Absatz 1 Satz 2 Nummer 2 und 3 genannten Objekten dürfen personenbezogene Daten offen mit technischen Mitteln zur Bild- und Tonaufzeichnung erhoben werden, soweit Tatsachen die Annahme rechtfertigen, dass an oder in Objekten dieser Art Straftaten begangen werden sollen, durch die Personen, diese Objekte oder andere darin befindliche Sachen gefährdet sind.

(5) Maßnahmen nach Absatz 2 bis 4 bedürfen der schriftlichen Anordnung durch die Leitung der zuständigen Behörde. In ihr sind anzugeben:

1. Art, Umfang und Dauer der Maßnahme, einschließlich einer Bezeichnung der Orte beziehungsweise Objekte, auf die sich die Maßnahme erstreckt,
2. die Gründe.

Über die Anordnung ist die oder der Landesbeauftragte für den Datenschutz unverzüglich zu unterrichten.

(6) Die Datenverarbeitung kann auch dann erfolgen, wenn Dritte (§ 3 Absatz 4 Nummer 2) unvermeidbar betroffen sind. Auf eine Datenverarbeitung nach Absatz 1 bis 4 ist in geeigneter Weise hinzuweisen, soweit diese nicht offenkundig ist oder Gefahr im Verzug besteht. Eine wegen Gefahr im Verzug unterbliebene Mitteilung ist unverzüglich nachzuholen.

(7) Aufzeichnungen nach Absatz 1 sind spätestens einen Monat nach ihrer Erhebung zu löschen. Aufzeichnungen nach Absatz 3 und 4 sind spätestens zwei Wochen nach ihrer Erhebung zu löschen. Satz 1 und 2 gelten nicht, soweit nach diesem Gesetz eine Weiterverarbeitung zulässig ist oder § 45 Absatz 3 eine Einschränkung der Verarbeitung vorsieht.

(8) Die Polizei kann an öffentlichen Orten technische Mittel zur offenen Bild- und Tonaufzeichnung in oder an Fahrzeugen der Polizei einsetzen, soweit und solange im Rahmen der Gefahrenabwehr und bei der Verfolgung von Straftaten und Ordnungswidrigkeiten mit hinreichender Wahrscheinlichkeit zu erwarten ist, dass dies zum Schutz der Polizeivollzugsbeamtinnen oder Polizeivollzugsbeamten oder Dritten (§ 3 Absatz 4 Nummer 2) gegen eine Gefahr für Leib oder Leben erforderlich ist. Absatz 6 und Absatz 7 Satz 2 und 3 gelten entsprechend.

(9) Die Polizei kann in den für die Durchführung der Gewahrsamnahme genutzten polizeilichen Räumen durch den offenen Einsatz technischer Mittel Bild- und Tonaufzeichnungen anfertigen, soweit Tatsachen die Annahme rechtfertigen, dass dies zum Schutz der dort befindlichen Personen gegen eine Gefahr für Leib oder Leben erforderlich ist. Absatz 6 und Absatz 7 Satz 2 und 3 gelten entsprechend.

(10) Die Polizei darf durch den offenen Einsatz technischer Mittel Bild- und Tonaufzeichnungen zur Suche von Personen, deren Leben oder Gesundheit gefährdet ist, anfertigen, wenn die Erfüllung der polizeilichen Aufgabe auf andere Weise aussichtslos oder wesentlich erschwert wäre. Absatz 6 gilt entsprechend. Nach Abschluss der Maßnahme sind die erhobenen personenbezogenen Daten unverzüglich zu löschen. Dies gilt nicht, soweit nach diesem Gesetz eine Weiterverarbeitung zulässig ist oder § 45 Absatz 3 eine Einschränkung der Verarbeitung vorsieht.

§ 32a
Einsatz körpernah getragener Aufnahmegeräte

(1) Die Polizei kann an öffentlich zugänglichen Orten für die Dauer von bis zu 60 Sekunden Daten durch Anfertigen von Bild- und Tonaufzeichnungen offen mittels körpernah getragener Aufnahmegeräte im Zwischenspeicher erheben, soweit und solange im Rahmen der Gefahrenabwehr und bei der Verfolgung von Straftaten und Ordnungswidrigkeiten mit hinreichender Wahrscheinlichkeit zu erwarten ist, dass dies zum Schutz der Polizeivollzugsbeamtinnen oder Polizeivollzugsbeamten oder Dritter (§ 3 Absatz 4 Nummer 2) gegen eine Gefahr für Leib oder Leben erforderlich ist. Die im Zwischenspeicher erhobenen Daten werden spätestens nach Ablauf von 60 Sekunden automatisch gelöscht, soweit ihre Speicherung nicht nach Absatz 2 zulässig ist.

(2) Die Polizei kann darüber hinaus an öffentlich zugänglichen Orten im Rahmen der Gefahrenabwehr und bei der Verfolgung von Straftaten und Ordnungswidrigkeiten Daten durch Anfertigen von Bild- und Tonaufzeichnungen offen mittels körpernah getragener Aufnahmegeräte auf einem dauerhaften Speichermedium erheben, soweit und solange Tatsachen die Annahme rechtfertigen, dass dies zum Schutz der Polizeivollzugsbeamtinnen oder Polizeivollzugsbeamten oder Dritter (§ 3 Absatz 4 Nummer 2) gegen eine im Einzelfall bevorstehende Gefahr für Leib oder Leben erforderlich ist. In diesem Fall dürfen die nach Absatz 1 Satz 1 erhobenen Daten auf das dauerhafte Speichermedium übertragen werden.

(3) In Wohn- und Geschäftsräumen sowie in oder von befriedetem Besitztum gilt Absatz 1 entsprechend. Eine dauerhafte Datenerhebung nach Absatz 2 ist in Wohn- und Geschäftsräumen sowie auf einem befriedeten Besitztum nur zulässig, soweit und solange Tatsachen die Annahme rechtfertigen, dass dies zum Schutz der Polizeivollzugsbeamtinnen oder Polizeivollzugsbeamten oder Dritter (§ 3 Absatz 4 Nummer 2) gegen eine gegenwärtige Gefahr für Leib oder Leben erforderlich ist.

(4) § 32 Absatz 6 gilt entsprechend.

(5) Aufzeichnungen sind verschlüsselt sowie manipulationssicher anzufertigen und aufzubewahren. Aufzeichnungen, die nach Absatz 3 oder in Fällen einer Unterbrechung nach § 26a Absatz 3 angefertigt wurden, sind besonders zu kennzeichnen. Auf dem dauerhaften Speichermedium gespeicherte Daten sind nach Ablauf von zwei Wochen nach ihrer Erhebung zu löschen; § 32 Absatz 7 Satz 3 gilt entsprechend.

(6) Das Ministerium für Inneres und Europa regelt das Nähere durch Verwaltungsvorschrift. Die Vorschriften des Versammlungsrechts bleiben unberührt.

§ 33
Besondere Mittel der Datenerhebung

(1) Besondere Mittel der Datenerhebung sind
1. die planmäßig angelegte Beobachtung, die durchgehend länger als 24 Stunden dauert oder an mehr als zwei Tagen stattfinden soll (längerfristige Observation),
2. der verdeckte Einsatz technischer Mittel, insbesondere solcher zur Bild- und Tonaufnahme oder Bild- und Tonaufzeichnung,
3. der Einsatz von Personen, deren Zusammenarbeit mit der Polizei den Betroffenen und Dritten (§ 3 Absatz 4 Nummer 2) nicht bekannt ist (Vertrauenspersonen),
4. der Einsatz von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten unter einer ihnen verliehenen, auf Dauer angelegten, veränderten Identität (verdeckt Ermittelnde).

(2) Mittel des Absatzes 1 können nur angewandt werden, wenn Tatsachen die Annahme der Begehung von Straftaten von erheblicher Bedeutung (§ 49) rechtfertigen und die Aufklärung des Sachverhaltes zum Zwecke der Verhütung solcher Straftaten oder ihrer möglichen Verfolgung ansonsten unmöglich oder wesentlich erschwert wäre. In diesem Fall kann die Polizei mit den Mitteln des Absatzes 1 Daten erheben über
1. Personen, bei denen tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass sie eine Straftat nach Satz 1 begehen oder sich an einer solchen beteiligen werden oder
2. Personen nach § 27 Absatz 3 Nummer 2.

Mittel nach Absatz 1 können bei Vorliegen der Voraussetzungen des § 67a Absatz 1 auch gegenüber den dort genannten Personen sowie Personen nach § 27 Absatz 3 Nummer 2 eingesetzt werden, wenn die Aufklärung des Sachverhaltes zum Zwecke der Verhütung terroristischer Straftaten (§ 67c) oder ihrer möglichen Verfolgung ansonsten unmöglich oder wesentlich erschwert wäre. Brief-, Post- und Fernmeldegeheimnis bleiben unberührt.

(3) Abweichend von Absatz 2 können Mittel nach Absatz 1 Nummer 2 eingesetzt werden, wenn dies ausschließlich dem Schutz der bei einem polizeilichen Einsatz tätigen Personen dient.

(4) Die Maßnahmen nach Absatz 1 und 3 dürfen auch durchgeführt werden, wenn Dritte (§ 3 Absatz 4 Nummer 2) unvermeidbar betroffen sind.

(5) Verdeckt Ermittelnde dürfen unter der Legende mit Einverständnis der berechtigten Person deren Wohnung betreten. Im Übrigen richten sich die Befugnisse verdeckt Ermittelnder nach diesem Gesetz oder anderen Rechtsvorschriften.

(6) Soweit es für den Aufbau und zur Aufrechterhaltung der Legende verdeckt Ermittelnder unerlässlich ist, können entsprechende Urkunden hergestellt, verändert und gebraucht werden. Die Unerlässlichkeit stellt die Behörde fest, die die verdeckt Ermittelnden einsetzt. Verdeckt Ermittelnde dürfen unter der Legende zur Erfüllung ihres Auftrages am Rechtsverkehr teilnehmen.

§ 33a
Verfahren beim Einsatz besonderer Mittel der Datenerhebung

(1) Maßnahmen nach § 33 bedürfen in den Fällen des
1. Absatz 1 Nummer 1,
2. Absatz 1 Nummer 2, bei denen durchgehend länger als 24 Stunden oder an mehr als zwei Tagen Bildaufzeichnungen bestimmter Personen angefertigt werden sollen,
3. Absatz 1 Nummer 2 zum Abhören oder Aufzeichnen des nicht öffentlich gesprochenen Wortes,
4. Absatz 1 Nummer 2, bei denen für Observationszwecke bestimmte technische Mittel durchgehend länger als 24 Stunden oder an mehr als zwei Tagen zum Einsatz kommen, und
5. Absatz 1 Nummer 3 und 4, die sich gegen eine bestimmte Person richten oder bei denen Vertrauenspersonen oder verdeckt Ermittelnde eine Wohnung betreten, die nicht allgemein zugänglich ist,

der richterlichen Anordnung auf Antrag der Leitung der zuständigen Polizeibehörde. Bei Gefahr im Verzug für Leib, Leben oder Freiheit einer Person kann die Leitung der zuständigen Polizeibehörde diese Maßnahme anordnen; eine richterliche Entscheidung ist unverzüglich nachzuholen. Soweit die Anordnung nach Satz 2 nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung der sonstigen Maßnahmen nach § 33 Absatz 1 erfolgt außer bei Gefahr im Verzug durch die Leitung der zuständigen Polizeibehörde oder durch eine von ihr besonders beauftragte Beamtin oder einen besonders beauftragten Beamten.

(2) Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. Art, Umfang und Dauer der Maßnahme,
3. der Sachverhalt sowie
4. eine Begründung.

(3) Die Anordnung ergeht schriftlich; in Fällen von Gefahr im Verzug ist sie unverzüglich nachträglich zu dokumentieren. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. Art, Umfang und Dauer der Maßnahme sowie
3. die Gründe.

Die Anordnung ist auf höchstens drei Monate zu befristen; im Falle des § 33 Absatz 1 Nummer 3 und 4 ist die Maßnahme auf höchstens sechs Monate zu befristen. Die Verlängerung der Maßnahme um jeweils denselben Höchstzeitraum bedarf einer neuen Anordnung.

(4) Daten, die ausschließlich über andere als die in § 33 Absatz 2, 4 oder in § 26b genannten Personen erhoben worden sind, sind unverzüglich zu löschen. Dies gilt nicht, wenn die nach § 33 Absatz 2 erhobenen Daten zur Verfolgung von Straftaten benötigt werden. Satz 1 gilt ferner nicht, soweit die nach § 26b erhobenen Daten aufgrund gesetzlicher Bestimmungen verwendet werden dürfen.

(5) Maßnahmen nach § 33 Absatz 3 kann die Einsatzleitung anordnen. Aufzeichnungen sind unverzüglich nach Beendigung des Einsatzes zu löschen. Dies gilt nicht, soweit nach diesem Gesetz eine Weiterverarbeitung zulässig ist oder § 45 Absatz 3 eine Einschränkung der Verarbeitung vorsieht.

§ 33b
Einsatz technischer Mittel zur Wohnraumüberwachung

(1) Die Polizei kann zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt, durch den verdeckten Einsatz technischer Mittel in oder aus der Wohnung einer Person, die für diese Gefahr verantwortlich ist, deren nichtöffentlich gesprochenes Wort abhören und aufzeichnen sowie von ihr Lichtbilder und Bildaufzeichnungen herstellen, soweit die Abwehr der Gefahr ansonsten unmöglich oder wesentlich erschwert wäre. Diese Maßnahmen dürfen auch unter den Voraussetzungen des § 67a Absatz 1 gegen die dort genannten Personen durchgeführt werden, soweit die Abwehr der dort bezeichneten Gefahr ansonsten unmöglich oder wesentlich erschwert wäre.

(2) In Wohnungen anderer Personen ist die Maßnahme nur zulässig, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass
1. sich eine Person im Sinne des Absatzes 1 dort aufhält und
2. die Maßnahme in der Wohnung dieser Person allein nicht zur Abwehr der Gefahr oder zur Verhütung einer Straftat nach Absatz 1 führen wird.

(3) Die Maßnahmen nach Absatz 1 und 2 dürfen auch durchgeführt werden, wenn Dritte (§ 3 Absatz 4 Nummer 2) unvermeidbar betroffen sind. Bei der Beurteilung nach § 26a Absatz 1 ist insbesondere auf die Art der zu überwachenden Räumlichkeiten und das Verhältnis der dort anwesenden Personen zueinander abzustellen.

(4) Die Maßnahmen nach Absatz 1 und 2 bedürfen der richterlichen Anordnung auf Antrag der Leitung der zuständigen Polizeibehörde. Bei Gefahr im Verzug kann die Leitung der zuständigen Polizeibehörde die Maßnahme anordnen; eine richterliche Entscheidung ist unverzüglich nachzuholen. Soweit die Anordnung nach Satz 2 nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(5) Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. die zu überwachende Wohnung oder die zu überwachenden Wohnräume,
3. Art, Umfang und Dauer der Maßnahme,
4. der Sachverhalt sowie
5. eine Begründung.

(6) Die Anordnung ergeht schriftlich; in Fällen von Gefahr im Verzug ist sie unverzüglich nachträglich zu dokumentieren. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. die zu überwachende Wohnung oder die zu überwachenden Wohnräume,
3. Art, Umfang und Dauer der Maßnahme sowie
4. die Gründe.

Die Anordnung ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die aufgrund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(7) Das anordnende Gericht ist über den Verlauf und die Ergebnisse zu unterrichten; es entscheidet unverzüglich über die Rechtmäßigkeit der Datenverarbeitung. Sofern die Voraussetzungen der Anordnung nicht mehr vorliegen, ordnet es die Beendigung der Maßnahme an, soweit diese nicht bereits durch die Leitung der zuständigen Polizeibehörde veranlasst wurde.

(8) Bei Gefahr im Verzug entscheidet über die Verwendung erhobener Daten die Leitung der zuständigen Polizeibehörde; eine richterliche Entscheidung nach Absatz 7 Satz 1 ist unverzüglich nachzuholen. Bei der Sichtung der erhobenen Daten kann sie sich der technischen Unterstützung von zwei weiteren Bediensteten der Behörde bedienen. Die Bediensteten sind zur Verschwiegenheit über die ihnen bekannt gewordenen Erkenntnisse, die nicht verwertet werden dürfen, verpflichtet. Sind Daten an andere Stellen übermittelt worden und wurde die Rechtmäßigkeit dieser Datenerhebung nicht richterlich bestätigt, ist § 45 Absatz 5 zu beachten.

(9) § 33 Absatz 3 und § 33a Absatz 5 gelten entsprechend.

§ 33c
Einsatz technischer Mittel zum Eingriff in informationstechnische Systeme

(1) Die Polizei darf durch den verdeckten Einsatz technischer Mittel in von der betroffenen Person genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, wenn Tatsachen die Annahme rechtfertigen, dass eine Gefahr vorliegt für
1. Leib, Leben oder Freiheit einer Person oder
2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt.

Eine Maßnahme nach Satz 1 ist auch zulässig, wenn die Voraussetzungen des § 67a Absatz 1 vorliegen. Die Maßnahme darf sich nur gegen eine Person richten, die für eine Gefahr verantwortlich ist. In informationstechnische Systeme anderer Personen darf die Maßnahme nur eingreifen, wenn Tatsachen die Annahme rechtfertigen, dass eine nach Satz 1 oder 2 betroffene Person dort ermittlungsrelevante Informationen speichert.

(2) Die Maßnahme darf nur durchgeführt werden, wenn die Abwehr der Gefahr ansonsten aussichtslos oder wesentlich erschwert wäre. Sie darf auch durchgeführt werden, wenn Dritte (§ 3 Absatz 4 Nummer 2) unvermeidbar betroffen sind. § 26a gilt mit der zusätzlichen Maßgabe, dass, soweit möglich, technisch sicherzustellen ist, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.

(3) 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.

(4) 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 (§ 3 Absatz 4 Nummer 2) dürfen dabei nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist.

(5) Das verdeckte Durchsuchen von Sachen sowie das verdeckte Betreten und Durchsuchen von Räumlichkeiten der betroffenen Personen sind zulässig, soweit dies zur Durchführung von Maßnahmen nach Absatz 1 und 4 erforderlich ist.

(6) Die Maßnahmen nach Absatz 1 und 4, auch soweit ein Fall des Absatzes 5 vorliegt, bedürfen der richterlichen Anordnung auf Antrag der Leitung der zuständigen Polizeibehörde.

(7) Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
3. in Fällen des Absatzes 5, soweit möglich, auch eine Bezeichnung der Sachen und die Anschrift der Räumlichkeiten der betroffenen Personen,
4. Art, Umfang und Dauer der Maßnahme,
5. der Sachverhalt sowie
6. eine Begründung.

(8) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
3. in Fällen des Absatzes 5, soweit möglich, auch eine Bezeichnung der Sachen und die Anschrift der Räumlichkeiten der betroffenen Personen,
4. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie
5. die Gründe.

Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Anordnungsvoraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die aufgrund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(9) Das anordnende Gericht ist über den Verlauf und die Ergebnisse zu unterrichten; es entscheidet unverzüglich über die Rechtmäßigkeit der Datenverarbeitung. Sofern die Voraussetzungen der Anordnung nicht mehr vorliegen, ordnet es die Beendigung der Maßnahme an, soweit diese nicht bereits durch die Leitung der zuständigen Polizeibehörde veranlasst wurde.

(10) Bei Gefahr im Verzug entscheidet über die Verwendung erhobener Daten die Leitung der zuständigen Polizeibehörde; eine richterliche Entscheidung nach Absatz 9 Satz 1 ist unverzüglich nachzuholen. Bei der Sichtung der erhobenen Daten kann sie sich der technischen Unterstützung von zwei weiteren Bediensteten der Behörde bedienen. Die Bediensteten sind zur Verschwiegenheit über die ihnen bekannt gewordenen Erkenntnisse, die nicht verwertet werden dürfen, verpflichtet. Sind Daten an andere Stellen übermittelt worden und wurde die Rechtmäßigkeit dieser Datenerhebung nicht richterlich bestätigt, ist § 45 Absatz 5 zu beachten.

§ 33d
Einsatz technischer Mittel zur Überwachung der Telekommunikation

(1) Die Polizei kann ohne Wissen der betroffenen Person personenbezogene Daten durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation erheben über

1. die für eine Gefahr Verantwortlichen, wenn dies zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt, erforderlich ist oder
2. Verantwortliche für eine Gefahr nach § 67a Absatz 1 oder
3. Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie für eine Person nach Nummer 1 oder 2 bestimmte oder von dieser herrührende Mitteilungen entgegennehmen oder weitergeben oder
4. Personen, bei denen Tatsachen die Annahme rechtfertigen, dass eine Person nach Nummer 1 oder 2 deren Telekommunikationsanschluss oder Endgerät benutzen wird oder
5. Personen, deren Leben oder Gesundheit gefährdet ist.

Datenerhebungen nach Satz 1 dürfen nur durchgeführt werden, wenn die Erfüllung der polizeilichen Aufgabe auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Maßnahme darf auch durchgeführt werden, wenn Dritte (§ 3 Absatz 4 Nummer 2) unvermeidbar betroffen sind.

(2) Eine Datenerhebung nach Absatz 1 kann sich auf

a) die Inhalte und Umstände der Telekommunikation und
b) Verkehrs- und Standortdaten im Sinne des Telekommunikationsgesetzes

beziehen. Unter den Voraussetzungen des Absatzes 1 kann die Polizei auch Auskunft über die Verkehrs- und Standortdaten in einem zurückliegenden Zeitraum verlangen. Die Erhebung aller in einer Funkzelle angefallenen Verkehrsdaten (Funkzellenabfrage) ist nicht zulässig.

(3) Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass verdeckt mit technischen Mitteln in von der betroffenen Person 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.

Auf dem informationstechnischen System der betroffenen Person gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können. § 33c Absatz 3 und 5 gilt entsprechend. § 33c bleibt im Übrigen unberührt.

(4) Die Maßnahmen bedürfen der richterlichen Anordnung auf Antrag der Leitung der zuständigen Polizeibehörde. Bei Gefahr im Verzug für Leib, Leben oder Freiheit einer Person kann die Leitung der zuständigen Polizeibehörde oder eine von ihr besonders beauftragte Beamtin oder ein von ihr besonders beauftragter Beamter die Maßnahme anordnen; eine richterliche Entscheidung ist unverzüglich nachzuholen. Soweit die Anordnung nach Satz 2 nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(5) Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. soweit möglich die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts, sofern nicht Tatsachen die Annahme rechtfertigen, dass diese Rufnummer oder andere Kennung zugleich einem anderen Endgerät zugeordnet ist,
3. Art, Umfang und Dauer der Maßnahme,
4. im Falle des Absatzes 3 auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll, und in den Fällen der entsprechenden Anwendung des § 33c Absatz 5, soweit möglich, auch eine Bezeichnung der Sachen und die Anschrift der Räumlichkeiten der betroffenen Person,
5. der Sachverhalt sowie
6. eine Begründung.

(6) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts, sofern nicht Tatsachen die Annahme rechtfertigen, dass diese Rufnummer oder andere Kennung zugleich einem anderen Endgerät zugeordnet ist,
3. Art, Umfang und Dauer der Maßnahme einschließlich der Uhrzeit der Anordnung,
4. im Falle des Absatzes 3 auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll, und in den Fällen der entsprechenden Anwendung des § 33c Absatz 5, soweit möglich, auch eine Bezeichnung der Sachen und die Anschrift der Räumlichkeiten der betroffenen Person sowie
5. die Gründe.

Bei Gefahr im Verzug kann die Angabe der Gründe unterbleiben; sie ist unverzüglich nachzuholen. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die aufgrund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(7) Aufgrund der Anordnung hat jeder Diensteanbieter im Sinne des Telekommunikationsgesetzes der Polizei nach Maßgabe des Telekommunikationsgesetzes und der Telekommunikations-Überwachungsverordnung die Maßnahmen unverzüglich zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Die in Anspruch genommenen Diensteanbieter werden entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes entschädigt.

(8) Über die Rechtmäßigkeit erhobener Daten, die im Wege einer automatischen Aufzeichnung ohne zeitgleiche Prüfung, ob der Kernbereich privater Lebensgestaltung berührt ist, erlangt wurden, entscheidet die oder der behördliche Datenschutzbeauftragte. Satz 1 gilt entsprechend, wenn sich bei zeitgleicher Prüfung Tatsachen ergeben, die die Annahme rechtfertigen, dass Erkenntnisse aus dem Kernbereich erfasst werden. Bei Gefahr im Verzug entscheidet über die Verwendung erhobener Daten die Leitung der zuständigen Polizeibehörde oder eine von ihr besonders beauftragte Beamtin oder ein von ihr besonders beauftragter Beamter; eine Entscheidung der oder des behördlichen Datenschutzbeauftragten ist unverzüglich nachzuholen. Soweit personenbezogene Daten Dritter (§ 3 Absatz 4 Nummer 2) erhoben worden sind, sind diese unverzüglich nach der Entscheidung zur Datenweiterverarbeitung zu löschen, soweit dies technisch möglich ist. Sind in den Fällen des Satzes 3 Daten an andere Stellen übermittelt worden und wurde die Rechtmäßigkeit dieser Datenerhebung nicht von der oder dem behördlichen Datenschutzbeauftragten festgestellt, ist § 45 Absatz 5 anzuwenden.

§ 33e
Auskunft über Nutzungsdaten

(1) Die Polizei kann unter den Voraussetzungen des § 33d Absatz 1 über die dort genannten Personen Auskünfte über Nutzungsdaten gemäß § 15 Absatz 1 Satz 2 Nummer 2 und 3 des Telemediengesetzes verlangen. Die Auskunft kann auch über zukünftige Nutzungsdaten angeordnet werden.

(2) Für die Anordnung der Maßnahme gilt § 33d Absatz 4 bis 6 entsprechend.

(3) Aufgrund der Anordnung hat jeder Diensteanbieter im Sinne des Telemediengesetzes der Polizei unverzüglich Auskunft über die Nutzungsdaten auf dem von ihr bestimmten Weg zu erteilen. § 33d Absatz 7 Satz 2 gilt entsprechend.

§ 33f
Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten

(1) Die Polizei kann unter den Voraussetzungen des § 33d Absatz 1 durch technische Mittel
1. die Gerätenummer eines Mobilfunkendgeräts und die Kartennummer der darin verwendeten Karte sowie
2. den Standort eines Mobilfunkendgeräts

ermitteln. Personenbezogene Daten Dritter (§ 3 Absatz 4 Nummer 2) dürfen anlässlich einer Maßnahme nach Satz 1 nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zwecks nach Satz 1 unvermeidbar ist. Über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer hinaus dürfen sie nicht verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen.

(2) Für die Anordnung der Maßnahme gilt § 33d Absatz 4 bis 6 entsprechend.

(3) Aufgrund der Anordnung einer Maßnahme nach Absatz 1 Satz 1 Nummer 2 hat jeder Diensteanbieter im Sinne des Telekommunikationsgesetzes der Polizei unverzüglich die für die Ermittlung des Standortes des Mobilfunkendgeräts erforderliche Geräte- und Kartennummer mitzuteilen. § 33d Absatz 7 Satz 2 gilt entsprechend.

§ 33g
Unterbrechung oder Verhinderung der Telekommunikation

(1) Die Polizei kann unter den Voraussetzungen des § 33d Absatz 1 Satz 1 Nummer 1 bis 4 und Satz 2 durch technische Mittel Telekommunikationsverbindungen unterbrechen oder verhindern. Die Maßnahme darf auch durchgeführt werden, wenn Telekommunikationsverbindungen Dritter (§ 3 Absatz 4 Nummer 2) 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 auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(3) Für die Anordnung gilt § 33d Absatz 4 entsprechend.

(4) Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. soweit möglich die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts, sofern nicht Tatsachen die Annahme rechtfertigen, dass diese Rufnummer oder andere Kennung zugleich einem anderen Endgerät zugeordnet ist,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunkts,
4. im Fall des Absatzes 2 die möglichst genaue räumliche und zeitliche Bezeichnung der Telekommunikationsverbindungen, die unterbrochen oder verhindert werden sollen,
5. der Sachverhalt sowie
6. eine Begründung.

(5) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

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

§ 33d Absatz 6 Satz 3 bis 6 gilt entsprechend.

§ 33h
Auskunft über Bestandsdaten

(1) Die Polizei kann zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr von Diensteanbietern im Sinne des Telekommunikationsgesetzes Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes oder von Diensteanbietern im Sinne des Telemediengesetzes Auskunft über die nach § 14 Absatz 1 und § 15 Absatz 1 Satz 2 Nummer 1 des Telemediengesetzes erhobenen personenbezogenen Daten verlangen. Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

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

(3) Aufgrund eines Auskunftsverlangens nach Absatz 1 oder Absatz 2 haben die Diensteanbieter die zur Auskunftserteilung erforderlichen Daten unverzüglich, vollständig und richtig zu übermitteln. § 33d Absatz 7 Satz 2 gilt entsprechend.

§ 34
Einsatz unbemannter Luftfahrtsysteme

Bei den nachfolgenden Maßnahmen dürfen unter Beachtung der dort bestehenden Regelungen Daten auch durch den Einsatz unbemannter Luftfahrtsysteme erhoben werden:

1. offene Bild- und Tonaufnahmen oder -aufzeichnungen nach § 32 Absatz 1, 3, 4 und 10,
2. Einsatz besonderer Mittel der Datenerhebung nach § 33,
3. Einsatz technischer Mittel in Wohnungen nach § 33b,
4. Einsatz technischer Mittel zum Eingriff in informationstechnische Systeme nach § 33c,
5. Einsatz technischer Mittel zur Telekommunikationsüberwachung nach den §§ 33d, 33f und 33g.

Eine Datenerhebung mittels unbemannter Luftfahrtsysteme durch eine Vertrauensperson ist unzulässig.

§ 35
Ausschreibung zur polizeilichen Beobachtung und gezielten Kontrolle

(1) Rechtfertigen tatsächliche Anhaltspunkte die Annahme dafür, dass bestimmte Personen Straftaten von erheblicher Bedeutung (§ 49) oder terroristische Straftaten (§ 67c) begehen werden, kann die Polizei zur Verhütung oder zur vorbeugenden Bekämpfung solcher Straftaten personenbezogene Daten, insbesondere die Personalien dieser Personen oder die amtlichen Kennzeichen, die Identifizierungsnummern oder die äußeren Kennzeichnungen der von solchen Personen benutzten oder eingesetzten Kraftfahrzeuge, Wasserfahrzeuge, Luftfahrzeuge oder Container, in einem Dateisystem speichern, damit andere Polizeibehörden Erkenntnisse über das Antreffen sowie über Personen nach § 27 Absatz 3 Nummer 2 bei Gelegenheit einer Überprüfung aus anderem Anlass übermitteln (Ausschreibung zur polizeilichen Beobachtung). Die Maßnahme kann auch durchgeführt werden, wenn die Voraussetzungen des § 67a Absatz 1 vorliegen.

(2) Unter den Voraussetzungen des Absatzes 1 ist auch die Ausschreibung zur gezielten Kontrolle zulässig. Unbeschadet anderer Vorschriften kann die Polizei im Rahmen der gezielten Kontrolle

1. die Identität von Personen feststellen, die sich in einem zur gezielten Kontrolle ausgeschriebenen Fahrzeug oder Container befinden,
2. das zur gezielten Kontrolle ausgeschriebene Fahrzeug oder den Container sowie die darin befindlichen Sachen durchsuchen sowie
3. die zur gezielten Kontrolle ausgeschriebene Person durchsuchen

und die daraus gewonnenen Erkenntnisse an die ausschreibende Polizeibehörde übermitteln. Die für die Identitätsfeststellung sowie die Durchsuchung von Personen und Sachen geltenden Vorschriften sind im Übrigen anzuwenden.

(3) Die Maßnahmen nach Absatz 1 und 2 bedürfen der Anordnung durch die Leitung der zuständigen Polizeibehörde.

(4) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. sonstige Angaben nach Absatz 1,
3. Art, Umfang und Dauer der Maßnahme sowie
4. die Gründe.

(5) Die Anordnung ist auf höchstens sechs Monate zu befristen. Liegen die Voraussetzungen für die Anordnung nicht mehr vor oder ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, ist die Ausschreibung unverzüglich zu löschen. Eine Verlängerung um jeweils nicht mehr als sechs weitere Monate ist zulässig, soweit die Voraussetzungen der Anordnung fortbestehen. Eine Verlängerung bedarf der gerichtlichen Anordnung nach Maßgabe des Absatzes 4 auf Antrag der Leitung der zuständigen Polizeibehörde; der Antrag muss die Angaben nach Absatz 4 Satz 2 Nummer 1 bis 3 sowie den Sachverhalt und eine Begründung enthalten.

Unterabschnitt 3
Speicherung, Übermittlung und sonstige Verarbeitung personenbezogener Daten (§§ 36 - 44)

§ 36
Zweckbindung, Grundsatz der hypothetischen Datenneuerhebung

(1) Soweit in diesem Gesetz nichts Besonderes geregelt ist, können personenbezogene Daten, die zu Zwecken dieses Gesetzes erhoben wurden, weiterverarbeitet werden, soweit dies zur Erfüllung derselben Aufgabe und zum Schutz derselben Rechtsgüter oder zur Verhütung derselben Straftaten oder Ordnungswidrigkeiten erforderlich ist. Bei personenbezogenen Daten, die durch Maßnahmen zur Wohnraumüberwachung (§ 33b) oder zum Eingriff in informationstechnische Systeme (§ 33c) erlangt wurden, gilt dies mit der Maßgabe, dass im Einzelfall eine Gefahrenlage im Sinne dieser Vorschriften vorliegt.

(2) Personenbezogene Daten, die zu Zwecken dieses Gesetzes erhoben wurden, können zu anderen Zwecken weiterverarbeitet werden, wenn unter Berücksichtigung der jeweiligen Datenerhebungsvorschrift

1. mindestens
   a) vergleichbar schwerwiegende Straftaten oder Ordnungswidrigkeiten verhütet, aufgedeckt oder verfolgt oder
   b) vergleichbar bedeutsame Rechtsgüter geschützt

werden sollen und

2. sich im Einzelfall konkrete Ermittlungsansätze
   a) zur Verhütung, Aufdeckung oder Verfolgung solcher Straftaten oder Ordnungswidrigkeiten ergeben oder
   b) zur Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter erkennen lassen,

soweit Rechtsvorschriften dieses Gesetzes oder anderer Gesetze die zweckändernde Weiterverarbeitung nicht besonders regeln oder wenn andere Rechtsvorschriften dieses Gesetzes oder anderer Gesetze eine Datenerhebung zu dem anderen Zweck mit vergleichbaren Mitteln zulassen. § 37a bleibt unberührt.

(3) Für die Weiterverarbeitung von personenbezogenen Daten, die durch Maßnahmen zur Wohnraumüberwachung (§ 33b) oder zum Eingriff in informationstechnische Systeme (§ 33c) erlangt wurden, gilt Absatz 2 Satz 1 Nummer 2 Buchstabe b mit der Maßgabe entsprechend, dass im Einzelfall eine Gefahrenlage im Sinne dieser Vorschriften vorliegen muss. Lichtbilder oder Bildaufzeichnungen von einer Person, die durch eine Maßnahme zur Wohnraumüberwachung (§ 33b) erlangt wurden, dürfen nicht zu Strafverfolgungszwecken weiterverarbeitet werden.

(4) Abweichend von Absatz 2 können die vorhandenen Grunddaten nach § 3 Absatz 5 Nummer 2 einer Person auch weiterverarbeitet werden, um diese Person zu identifizieren.

(5) Bei der Weiterverarbeitung von personenbezogenen Daten ist durch organisatorische und technische Vorkehrungen sicherzustellen, dass die Absätze 1 bis 4 beachtet werden.

§ 37
Voraussetzungen der Verarbeitung personenbezogener Daten aus Strafermittlungsverfahren

(1) Die Polizei kann personenbezogene Daten, die sie im Rahmen von Strafermittlungsverfahren über Personen gewonnen hat, die einer Straftat verdächtig sind, unter Beachtung des § 36 Absatz 2 und 3 verarbeiten, soweit dies zur vorbeugenden Bekämpfung von Straftaten erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse die Gefahr der Begehung einer weiteren Straftat besteht. § 37a bleibt unberührt.

(2) Ist der Ausgang des Strafermittlungsverfahrens zum Zeitpunkt der Entscheidung über eine Speicherung nicht bekannt, darf die Dauer der Speicherung zunächst drei Jahre nicht überschreiten. Eine weitere Speicherung darf nur nach erneuter Prüfung des Sachverhalts und nur unter der Voraussetzung erfolgen, dass die Polizei Erkundigungen hinsichtlich des Ausgangs des Verfahrens einholt; entfällt der dem Strafermittlungsverfahren zu Grunde liegende Verdacht, so sind die Daten zu löschen.

(3) Die Polizei kann die nach § 27 Absatz 3 erhobenen Daten unter Beachtung des § 36 Absatz 1 bis 3 verarbeiten. Die Speicherungsdauer dieser Daten darf drei Jahre nicht überschreiten. Nach jeweils einem Jahr, gerechnet vom Zeitpunkt ihrer Speicherung, ist zu prüfen, ob die Voraussetzungen einer weiteren Nutzung noch vorliegen; die Entscheidung trifft die Leitung der zuständigen Polizeibehörde oder eine von ihr besonders beauftragte Beamtin oder ein von ihr besonders beauftragter Beamter.

(4) § 36 Absatz 5 gilt entsprechend.

§ 37a
Verarbeitung zu Zwecken der wissenschaftlichen und historischen Forschung, Aus- und Fortbildung und Statistik

(1) Personenbezogene Daten, die in oder aus Wohn- oder Geschäftsräumen oder befriedetem Besitztum oder durch eine Maßnahme nach § 33c oder in Fällen des § 26a Absatz 3 oder des § 26b erhoben wurden, dürfen nicht zu Zwecken der wissenschaftlichen oder historischen Forschung oder der Aus- und Fortbildung weiterverarbeitet werden.

(2) Personenbezogene Daten, die nicht unter Absatz 1 fallen, dürfen zu Zwecken der wissenschaftlichen oder historischen Forschung nach Maßgabe des § 9 des Landesdatenschutzgesetzes weiterverarbeitet werden.

(3) Die Polizei und Ordnungsbehörden können personenbezogene Daten, die nicht unter Absatz 1 fallen, zu Zwecken der Aus- und Fortbildung weiterverarbeiten und an die mit der Aus- und Fortbildung ihrer Beschäftigten beauftragten öffentlichen Stellen übermitteln, wenn auf andere Weise das Ziel der Aus- oder Fortbildung nicht erreichbar ist und nicht überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen. Soweit der Zweck der Weiterverarbeitung dieses zulässt und kein unvertretbarer Verwaltungsaufwand entgegensteht, sind diese Daten zu anonymisieren. Für die Übermittlung personenbezogener Daten gilt § 9 Absatz 4 des Landesdatenschutzgesetzes entsprechend.

(4) Personenbezogene Daten dürfen zu statistischen Zwecken nur in anonymisierter Form weiterverarbeitet werden.

§ 38
Weiterverarbeitung personenbezogener Daten zur Vorgangsverwaltung und befristeten Dokumentation

Zur Vorgangsverwaltung oder zur befristeten Dokumentation behördlichen Handelns können personenbezogene Daten gespeichert und nur zu diesem Zweck weiterverarbeitet werden. Die §§ 36 bis 37a sind nicht anzuwenden. Mittel und Umfang der Vorgangsverwaltung werden vom Ministerium für Inneres und Europa im Benehmen mit der oder dem Landesbeauftragten für den Datenschutz durch Verwaltungsvorschrift bestimmt.

§ 39
Grundsätze der Datenübermittlung

(1) Die verantwortliche Stelle hat angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig oder nicht mehr aktuell sind, nicht übermittelt oder sonst zur Verfügung gestellt werden. Zu diesem Zweck hat sie, soweit dies mit angemessenem Aufwand möglich ist, die Qualität der Daten vor ihrer Übermittlung oder Bereitstellung zu überprüfen. Bei jeder Übermittlung personenbezogener Daten hat sie zudem, soweit dies möglich und angemessen ist, Informationen beizufügen, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der Daten sowie deren Aktualität zu beurteilen.

(2) Gelten für die Verarbeitung von personenbezogenen Daten besondere Bedingungen, so hat bei Datenübermittlungen die übermittelnde Stelle den Empfänger auf diese Bedingungen und die Pflicht zu ihrer Beachtung hinzuweisen. Die Hinweispflicht kann dadurch erfüllt werden, dass die Daten entsprechend gekennzeichnet werden.

(3) Die übermittelnde Stelle darf auf Empfänger in anderen Mitgliedstaaten der Europäischen Union und auf Einrichtungen und sonstige Stellen, die nach den Kapiteln 4 und 5 des Titels V des Dritten Teils des Vertrags über die Arbeitsweise der Europäischen Union errichtet wurden, keine Bedingungen anwenden, die nicht auch für entsprechende innerstaatliche Datenübermittlungen gelten.

§ 39a
Datenübermittlungsverbote und Verweigerungsgründe

(1) Die Übermittlung personenbezogener Daten unterbleibt, wenn
1 für die übermittelnde Stelle erkennbar ist, dass unter Berücksichtigung der Art der Daten und ihrer Erhebung die schutzwürdigen Interessen der betroffenen Person das Allgemeininteresse an der Übermittlung überwiegen, oder
2. Weiterverarbeitungsregelungen entgegenstehen; die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

Satz 1 Nummer 1 gilt nicht für Übermittlungen an die Staatsanwaltschaften.

(2) Die Datenübermittlung an Stellen außerhalb der Bundesrepublik Deutschland unterbleibt darüber hinaus,

1. wenn hierdurch wesentliche Sicherheitsinteressen des Bundes oder der Länder beeinträchtigt würden,
2. wenn hierdurch der Erfolg laufender Ermittlungen oder Leib, Leben oder Freiheit einer Person gefährdet würde,
3. soweit Grund zu der Annahme besteht, dass durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde, oder
4. wenn Tatsachen die Annahme rechtfertigen, dass die Übermittlung der Daten zu den in der Charta der Grundrechte der Europäischen Union enthaltenen Grundsätzen, insbesondere dadurch, dass durch die Weiterverarbeitung der übermittelten Daten im Empfängerstaat Verletzungen von elementaren rechtsstaatlichen Grundsätzen oder Menschenrechtsverletzungen drohen, in Widerspruch stünde.

(3) Bei der Beurteilung von Ausschluss- und Verweigerungsgründen haben die Behörden insbesondere die nach § 28 Absatz 3 des Bundeskriminalamtgesetzes für den polizeilichen Informationsaustausch und Rechtshilfeverkehr geführte Aufstellung über die Einhaltung der elementaren rechtsstaatlichen Grundsätze und Menschenrechtsstandards sowie das Datenschutzniveau in den jeweiligen Drittstaaten, die die speziellen Erfordernisse des polizeilichen Informationsaustauschs berücksichtigt, zu beachten.

§ 39b
Datenübermittlung im innerstaatlichen Bereich

(1) Personenbezogene Daten können unter Beachtung des § 36 Absatz 2 bis 4 und der §§ 39 und 39a innerhalb des Landes an Polizeibehörden und Ordnungsbehörden und darüber hinaus auch an andere Polizeien und Ordnungsbehörden des Bundes und der Länder übermittelt werden, soweit dies zur Erfüllung der polizeilichen oder ordnungsbehördlichen Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist. Die über Personen nach § 27 Absatz 3 Nummer 2 bis 4 gespeicherten personenbezogenen Daten dürfen nur an andere Polizeidienststellen übermittelt werden.

(2) Für die Einrichtung von automatisierten Verfahren gilt § 42.

(3) Personenbezogene Daten können an andere als die in Absatz 1 genannten Behörden und sonstige öffentliche Stellen übermittelt werden, soweit dies

1. in anderen Rechtsvorschriften vorgesehen ist oder
2. unter Beachtung des § 36 Absatz 2 bis 4 und der §§ 39 und 39a zulässig und erforderlich ist
   a) zur Aufgabenerfüllung nach diesem Gesetz,
   b) für Zwecke der Verfolgung von Straftaten oder Ordnungswidrigkeiten,
   c) für Zwecke der Gefahrenabwehr oder
   d) zur Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Einzelner

   und Zwecke des Verfahrens, zu dem die Daten erhoben wurden, nicht entgegenstehen.

Persönliche Einschätzungen oder Beurteilungen sowie gespeicherte personenbezogene Daten über Personen nach § 27 Absatz 3 Nummer 2 bis 4 dürfen nicht übermittelt werden. Die Übermittlung personenbezogener Daten zwischen der Verfassungsschutzbehörde und den Ordnungsbehörden oder der Polizei des Landes richtet sich nach den Vorschriften des Landesverfassungsschutzgesetzes.

(4) Unter den Voraussetzungen des Absatzes 3 können personenbezogene Daten auch an nichtöffentliche Stellen übermittelt werden. Die Übermittlung unterbleibt, wenn der der Erhebung dieser Daten zugrundeliegende Zweck gefährdet würde oder schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. Sind personenbezogene Daten durch eine andere Stelle übermittelt worden und besteht Grund zu der Annahme, dass durch die Übermittlung nach Satz 1 der der Erhebung dieser Daten zugrundeliegende Zweck gefährdet würde, ist vor der Übermittlung die Zustimmung dieser Stelle einzuholen. Verarbeitungsbedingungen der übermittelnden Stelle sind zu beachten.

(5) Der Empfänger darf die übermittelten personenbezogenen Daten nur zu dem Zweck verarbeiten, für den sie ihm übermittelt worden sind. Eine Verarbeitung für andere Zwecke ist unter Beachtung des § 36 Absatz 2 bis 4 zulässig; im Falle des Absatzes 4 gilt dies nur, soweit die übermittelnde Stelle der Zweckänderung zustimmt.

(6) Die Verantwortung für die Zulässigkeit der Datenübermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung in den Fällen von Absatz 1 oder 3 Nummer 2 auf Ersuchen des Empfängers, trägt dieser die Verantwortung. In diesen Fällen prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. Im Übrigen hat die ersuchende Stelle der übermittelnden Stelle die zur Prüfung der Zulässigkeit der Übermittlung erforderlichen Angaben zu machen.

(7) Sind mit personenbezogenen Daten, die nach Absatz 1 oder 3 übermittelt werden dürfen, weitere personenbezogene Daten der betroffenen Person oder eines Dritten (§ 3 Absatz 4 Nummer 2) in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen der betroffenen Person oder eines Dritten (§ 3 Absatz 4 Nummer 2) an der Geheimhaltung offensichtlich überwiegen; eine Verwendung dieser Daten durch den Empfänger ist unzulässig.

§ 39c
Übermittlung an Mitgliedstaaten und Organisationen der Europäischen Union

(1) § 39b gilt, mit Ausnahme des § 39b Absatz 6, entsprechend für die Übermittlung von personenbezogenen Daten an

1. öffentliche und nichtöffentliche Stellen in Mitgliedstaaten der Europäischen Union und
2. zwischen- und überstaatliche Stellen der Europäischen Union oder deren Mitgliedstaaten, die mit Aufgaben im Sinne dieses Gesetzes befasst sind.

Die Verantwortung für die Zulässigkeit der Datenübermittlung trägt die übermittelnde Stelle. Für die Übermittlung an Polizei- und Justizbehörden sowie an sonstige für die Verhütung oder Verfolgung von Straftaten zuständige öffentliche Stellen zum Zwecke der Verfolgung von Straftaten und zur Strafvollstreckung bleiben die Vorschriften über die internationale Rechtshilfe in strafrechtlichen Angelegenheiten unberührt. Die Zulässigkeit der Übermittlung personenbezogener Daten an eine Polizeibehörde oder eine sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stelle eines Mitgliedstaates der Europäischen Union auf der Grundlage besonderer völkerrechtlicher Vereinbarungen bleibt unberührt.

(2) Absatz 1 findet auch Anwendung auf die Übermittlung von personenbezogenen Daten an Polizeibehörden oder sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stellen von Staaten, welche die Bestimmungen des Schengen-Besitzstandes aufgrund eines Assoziierungsübereinkommens mit der Europäischen Union über die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes anwenden.

§ 39d
Datenübermittlung in Drittstaaten im Anwendungsbereich der Richtlinie (EU) 2016/680

(1) Personenbezogene Daten können unter Beachtung des § 36 Absatz 2 bis 4, der §§ 39 und 39a sowie der §§ 39e bis 39g an Polizei- und Justizbehörden sowie an sonstige für die Verhütung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten zuständige öffentliche Stellen in anderen als den in § 39c genannten Staaten (Drittstaaten) und an andere als dort genannten zwischen- und überstaatlichen Stellen, die mit Aufgaben der Verhütung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten befasst sind, übermittelt werden, soweit dies erforderlich ist

1. zur Erfüllung einer Aufgabe nach § 4 Absatz 1 Satz 2 und § 7 Absatz 1 Nummer 4 oder
2. zu den Zwecken nach § 39g Absatz 1 Satz 1 Nummer 1 bis 3 und 5.

§ 39b Absatz 1 Satz 2 gilt entsprechend.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Der Empfänger personenbezogener Daten ist darauf hinzuweisen, dass die Daten nur zu dem Zweck verarbeitet werden dürfen, zu dem sie übermittelt worden sind. Ferner ist ihm der bei der übermittelnden Stelle vorgesehene Löschungszeitpunkt mitzuteilen.

§ 39e
Grundsätze der Datenübermittlung in Drittstaaten im Anwendungsbereich der Richtlinie (EU) 2016/680

(1) Die Übermittlung personenbezogener Daten nach § 39d ist zulässig, wenn die Europäische Kommission gemäß Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 einen Angemessenheitsbeschluss gefasst hat.

(2) Die Übermittlung personenbezogener Daten hat trotz des Vorliegens eines Angemessenheitsbeschlusses im Sinne des Absatzes 1 zu unterbleiben, wenn im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist oder sonst überwiegende schutzwürdige Interessen einer betroffenen Person entgegenstehen. Bei der Beurteilung hat die übermittelnde Stelle maßgeblich zu berücksichtigen, ob der Empfänger im Einzelfall einen angemessenen Schutz der übermittelten Daten garantiert.

(3) Wenn personenbezogene Daten, die aus einem anderen Mitgliedstaat der Europäischen Union übermittelt oder zur Verfügung gestellt wurden, nach § 39d Absatz 1 übermittelt werden sollen, muss dieser Übermittlung zuvor von der zuständigen Stelle des anderen Mitgliedstaats zugestimmt werden. Übermittlungen ohne vorherige Zustimmung sind nur dann zulässig, wenn die Übermittlung erforderlich ist, um eine gegenwärtige Gefahr für die öffentliche Sicherheit eines Staates oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Zustimmung nicht rechtzeitig eingeholt werden kann. Im Fall des Satzes 2 ist die Stelle des anderen Mitgliedstaats, die für die Erteilung der Zustimmung zuständig gewesen wäre, unverzüglich über die Übermittlung zu unterrichten.

(4) Die Stelle, die Daten nach Absatz 1 übermittelt, hat durch geeignete Maßnahmen sicherzustellen, dass der Empfänger die übermittelten Daten nur dann an andere Drittstaaten oder andere als die in § 39c genannten zwischen- und überstaatlichen Stellen weiterübermittelt, wenn die übermittelnde Stelle dieser Übermittlung zuvor zugestimmt hat. Bei der Entscheidung über die Erteilung der Zustimmung sind alle maßgeblichen Faktoren zu berücksichtigen, insbesondere die Schwere der Straftat, der Zweck der ursprünglichen Übermittlung und das in dem Drittstaat oder der anderen als in § 39c genannten zwischen- und überstaatlichen Stelle, an das oder an die die Daten weiterübermittelt werden sollen, bestehende Schutzniveau für personenbezogene Daten. Eine Zustimmung darf nur dann erfolgen, wenn auch eine direkte Übermittlung an den anderen Drittstaat oder an die andere als in § 39c genannte zwischen- und überstaatliche Stelle zulässig wäre. Die Zuständigkeit für die Erteilung der Zustimmung kann auch abweichend geregelt werden.

§ 39f
Datenübermittlung in Drittstaaten bei geeigneten Garantien im Anwendungsbereich der Richtlinie (EU) 2016/680

(1) Liegt entgegen § 39e Absatz 1 kein Angemessenheitsbeschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor, ist eine Übermittlung nach § 39d unter Beachtung der übrigen Maßgaben des § 39e auch dann zulässig, wenn

1. in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder
2. die übermittelnde Stelle nach Beurteilung aller Umstände, die bei der Übermittlung eine Rolle spielen, zu der Auffassung gelangt ist, dass geeignete Garantien für den Schutz personenbezogener Daten bestehen.

(2) Die verantwortliche Stelle hat die oder den Landesbeauftragten für den Datenschutz zu unterrichten, wenn aufgrund einer Beurteilung nach Absatz 1 Nummer 2 eine Datenübermittlung erfolgt ist; die Beurteilung ist zu dokumentieren und der Aufsichtsbehörde auf Anforderung zur Verfügung zu stellen.

§ 39g
Datenübermittlung in Drittstaaten ohne geeignete Garantien im Anwendungsbereich der Richtlinie (EU) 2016/680

(1) Liegt entgegen § 39e Absatz 1 kein Angemessenheitsbeschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor und liegen auch keine geeigneten Garantien im Sinne des § 39f Absatz 1 vor, ist eine Übermittlung nach § 39d unter Beachtung der übrigen Maßgaben des § 39e nur dann zulässig, wenn die Übermittlung erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer natürlichen Person,
2. zur Wahrung berechtigter Interessen der betroffenen Person,
3. zur Abwehr einer gegenwärtigen erheblichen Gefahr für die öffentliche Sicherheit eines Staates,
4. im Einzelfall für die in § 39d genannten Zwecke oder
5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 39d genannten Zwecken.

(2) Die verantwortliche Stelle hat von einer Übermittlung nach Absatz 1 abzusehen, wenn die Grundrechte der betroffenen Person das öffentliche Interesse an der Übermittlung überwiegen.

§ 39h
Sonstige Datenübermittlung an Empfänger in Drittstaaten im Anwendungsbereich der Richtlinie (EU) 2016/680

(1) Bei Vorliegen der übrigen für die Datenübermittlung in Drittstaaten geltenden Voraussetzungen können im besonderen Einzelfall personenbezogene Daten unmittelbar an andere als die in § 39d Absatz 1 genannten Stellen in Drittstaaten übermitteln, wenn die Übermittlung für die Erfüllung ihrer Aufgaben unbedingt erforderlich ist und

1. im konkreten Fall keine Grundrechte der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen,
2. die Übermittlung an die in § 39d Absatz 1 genannten Stellen wirkungslos oder ungeeignet wäre, insbesondere, weil sie nicht rechtzeitig durchgeführt werden kann, und
3. die übermittelnde Stelle dem Empfänger die Zwecke der Verarbeitung mitteilt und ihn darauf hinweist, dass die übermittelten Daten nur in dem Umfang verarbeitet werden dürfen, in dem ihre Verarbeitung für diese Zwecke erforderlich ist.

§ 39b Absatz 3 Satz 2 gilt entsprechend.

(2) Die übermittelnde Stelle hat die in § 39d Absatz 1 genannten Stellen unverzüglich über die Datenübermittlung zu unterrichten, sofern dies nicht wirkungslos oder ungeeignet ist.

(3) Die verantwortliche Stelle hat die oder den Landesbeauftragten für den Datenschutz jährlich über die Datenübermittlung zu unterrichten. In der Unterrichtung kann sie die Empfänger und die Übermittlungszwecke angemessen kategorisieren.

(4) Bei Datenübermittlungen nach Absatz 1 hat die übermittelnde Stelle den Empfänger zu verpflichten, die übermittelten personenbezogenen Daten nur für den Zweck zu verarbeiten, für den sie übermittelt worden sind.

(5) Abkommen im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit bleiben unberührt.

§ 40
Datenübermittlung zum Zwecke einer Zuverlässigkeitsüberprüfung

(1) Sofern vor Veranstaltungen Tatsachen die Annahme rechtfertigen, dass bei deren Durchführung eine besondere Gefahrenlage eintreten könnte, kann die Polizei personenbezogene Daten einer Person mit ihrer schriftlichen Einwilligung nach § 26 an öffentliche und nichtöffentliche Stellen übermitteln, wenn es für die Überprüfung ihrer Zuverlässigkeit erforderlich ist und im Hinblick auf den Anlass dieser Überprüfung, insbesondere den Zugang der betroffenen Person zu der Veranstaltung, sowie wegen der Art und des Umfangs der Erkenntnisse über sie und mit Rücksicht auf das berechtigte Sicherheitsinteresse des Empfängers angemessen ist. Die Rückmeldung an eine nichtöffentliche Stelle beschränkt sich auf die Auskunft zum Vorliegen von Zuverlässigkeitsbedenken.

(2) Der Empfänger darf die übermittelten Daten nur für den Zweck der Zuverlässigkeitsüberprüfung verarbeiten. Die Polizei hat den Empfänger schriftlich zu verpflichten, diese Zweckbestimmung einzuhalten und eine Löschung der Daten spätestens nach Beendigung der Veranstaltung vorzunehmen. Die betroffene Person ist durch die Polizei über den Inhalt der Übermittlung zu informieren, soweit dies nicht bereits auf andere Weise sichergestellt ist.

(3) Die Vorschriften des Sicherheitsüberprüfungsgesetzes des Landes Mecklenburg-Vorpommern bleiben unberührt.

§ 41
Bekanntgabe an die Öffentlichkeit

Die Ordnungsbehörden und die Polizei können Daten einer Person zum Zwecke der Ermittlung der Identität oder des Aufenthaltsortes oder zur Warnung öffentlich bekannt geben oder an andere Stellen zur Bekanntgabe an die Öffentlichkeit übermitteln, wenn

1. die Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person auf andere Weise nicht möglich erscheint oder
2. Tatsachen die Annahme rechtfertigen, dass diese Person eine Straftat von erheblicher Bedeutung (§ 49) oder eine terroristische Straftat (§ 67c) begehen wird und die Verhütung oder die Vorsorge für die Verfolgung dieser Straftat auf andere Weise nicht möglich erscheint.

§ 42
Automatisierte Verfahren, Verfahrensbeschreibung

(1) Automatisierte Verfahren zur Verarbeitung personenbezogener Daten dürfen unter Beachtung des § 36 Absatz 1 bis 4 nur eingeführt werden, wenn dies unter Berücksichtigung der schutzwürdigen Interessen der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist.

(2) Ein automatisiertes Verfahren nach Absatz 1 kann auch in Form eines Verfahrens,
1. das die Übermittlung personenbezogener Daten durch Abruf ermöglicht (Abrufverfahren),
2. bei dem mehrere verantwortliche Stellen gemeinsam die Verarbeitung personenbezogener Daten ermöglichen (Verbundverfahren) oder
3. das aus mindestens zwei eigenständigen automatisierten Teilverfahren mit jeweils eigenen verantwortlichen Stellen besteht (gemeinsames Verfahren),

eingerichtet werden. Abrufverfahren können insbesondere zwischen Polizeidienststellen, zwischen Ordnungsbehörden sowie zwischen Ordnungsbehörden und der Polizei vereinbart werden; der Abruf durch andere als die genannten Stellen ist nur aufgrund besonderer Rechtsvorschriften zulässig. Der Empfänger trägt die Verantwortung für die Rechtmäßigkeit des Abrufs. Einen Datenverbund, der eine automatisierte Datenübermittlung zwischen Polizeidienststellen des Landes und Polizeidienststellen des Bundes und der Länder ermöglicht und zur Erfüllung polizeilicher Aufgaben, die überörtliche Bedeutung haben, erforderlich ist, darf nur durch das Ministerium für Inneres und Europa als oberste Landesbehörde vereinbart werden.

(3) Werden in automatisierten Verfahren die Zwecke und die Mittel der Verarbeitung von zwei oder mehr verantwortlichen Stellen gemeinsam festgelegt, gelten sie als gemeinsam verantwortliche Stellen. Gemeinsam verantwortliche Stellen haben ihre jeweiligen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten in transparenter Form in einer Vereinbarung festzulegen, soweit diese nicht bereits in Rechtsvorschriften festgelegt sind. Aus der Vereinbarung muss insbesondere hervorgehen, wer welchen allgemeinen Informationspflichten gemäß § 46 nachzukommen hat und wie und gegenüber wem betroffene Personen ihre Rechte wahrnehmen können. In der Vereinbarung ist eine Anlaufstelle für die betroffenen Personen anzugeben. Eine entsprechende Vereinbarung hindert die betroffene Person nicht, ihre Rechte gegenüber jeder der gemeinsam verantwortlichen Stellen geltend zu machen. Soweit Anliegen nicht bei der Anlaufstelle eingehen, sind diese ihr zuzuleiten. Betrifft die Vereinbarung die Verarbeitung von Daten außerhalb des Anwendungsbereichs der Richtlinie (EU) 2016/680, ist der wesentliche Inhalt der Vereinbarung den betroffenen Personen öffentlich zur Verfügung zu stellen. Wesentlich sind dabei nur solche Teile der Vereinbarung, die die betroffenen Personen zur Wahrnehmung ihrer Rechte benötigen und deren Kenntnis die Aufgabenwahrnehmung der verantwortlichen Stellen nicht wesentlich erschweren.

(4) Die verantwortliche Stelle ist verpflichtet, für jedes von ihr eingesetzte automatisierte Verfahren, bei dem personenbezogene Daten verarbeitet werden, in einer Verfahrensbeschreibung festzulegen:

1. die Bezeichnung des Verfahrens und der verarbeitenden Stelle,
2. den Zweck und die Rechtsgrundlage der Verarbeitung,
3. die Kategorien der personenbezogenen Daten,
4. die Kategorien der Betroffenen,

5. Prüffristen nach § 45a oder Speicherungsdauer,
6. die Kategorien der Empfänger, denen die Daten übermittelt werden,
7. geplante Datenübermittlungen an Staaten und Stellen nach § 39d Absatz 1, einschließlich deren Bezeichnung,
8. Angaben nach § 45b Absatz 4,
9. eine Beschreibung der technischen und organisatorischen Maßnahmen nach den §§ 46d bis 46i und
10. besondere Regelungen über die Verarbeitung von Daten, die nach dem 2. Unterabschnitt (§§ 27 bis 35) erhoben wurden, insbesondere zum Verhältnis von Speicherinhalt und Abrufberechtigung.

Die Verfahrensbeschreibung ist elektronisch zu führen und laufend auf dem neuesten Stand zu halten.

(5) Vor dem erstmaligen Einsatz eines Verfahrens nach Absatz 1 oder dessen wesentlicher Änderung ist die oder der Landesbeauftragte für den Datenschutz zu beteiligen.

(6) Die Verfahrensbeschreibung ist in das Verzeichnis der Verarbeitungstätigkeiten der verantwortlichen Stelle (§ 45c) aufzunehmen.

(7) Das Ministerium für Inneres und Europa regelt das Nähere durch Verwaltungsvorschrift.

§ 43
Datenabgleich

(1) Die Polizei kann personenbezogene Daten der in den §§ 69, 70 sowie § 27 Absatz 3 Nummer 1 und Nummer 2 genannten Personen mit dem Inhalt polizeilicher Dateisysteme im Rahmen der Zweckbindung dieser Dateisysteme abgleichen. Personenbezogene Daten anderer Personen kann die Polizei abgleichen, wenn tatsächliche Anhaltspunkte dafür bestehen, dass dies zur Erfüllung polizeilicher Aufgaben erforderlich ist. Die Polizei kann ferner im Rahmen ihrer Aufgabenerfüllung erlangte personenbezogene Daten mit dem Fahndungsbestand abgleichen. Die betroffene Person kann für die Dauer des Datenabgleichs angehalten werden. Ein Abgleich der nach § 27 Absatz 2 erlangten personenbezogenen Daten ist nur mit Zustimmung der betroffenen Personen zulässig.

(2) Die Ordnungsbehörden können personenbezogene Daten der in den §§ 69 und 70 genannten Personen mit dem Inhalt anderer von ihnen geführter Dateisysteme im Rahmen der Zweckbestimmung dieser Dateisysteme abgleichen. Personenbezogene Daten anderer Personen können die Ordnungsbehörden abgleichen, wenn tatsächliche Anhaltspunkte dafür bestehen, dass dies zur Erfüllung ordnungsbehördlicher Aufgaben erforderlich ist. Absatz 1 Satz 5 gilt entsprechend.

(3) Rechtsvorschriften über den Datenabgleich in anderen Fällen bleiben unberührt.

§ 43a
Datenerhebung und Datenabgleich zur Erkennung von Kraftfahrzeugkennzeichen

(1) Die Polizei kann im öffentlichen Verkehrsraum technische Mittel zur Erkennung von Kraftfahrzeugkennzeichen auch ohne Wissen der betroffenen Person einsetzen,

1. wenn dies zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist,
2. wenn dies zur Abwehr einer gegenwärtigen Gefahr erforderlich ist und die Voraussetzungen für eine Identitätsfeststellung nach § 29 Absatz 1 Satz 2 vorliegen,
3. wenn eine Person oder ein Fahrzeug zur polizeilichen Beobachtung ausgeschrieben wurde und Tatsachen die Annahme rechtfertigen, dass die für die Ausschreibung relevante Begehung von Straftaten in absehbarer Zeit mit hinreichender Wahrscheinlichkeit bevorsteht,
4. wenn eine Person oder ein Fahrzeug zur gezielten Kontrolle ausgeschrieben wurde und Tatsachen die Annahme rechtfertigen, dass die für die Ausschreibung relevante Begehung von Straftaten in absehbarer Zeit mit hinreichender Wahrscheinlichkeit bevorsteht,
5. wenn dokumentierte polizeiliche Lageerkenntnisse über Kriminalitätsschwerpunkte eine Überwachung des öffentlichen Verkehrsraumes zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung (§ 49) oder terroristischer Straftaten (§ 67c) erfordern oder
6. zur vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität oder zur Unterbindung des unerlaubten Aufenthalts in dem Gebiet von der Bundesgrenze bis einschließlich der Bundesautobahn A 20.

Dabei können das Kennzeichen und Angaben zum Ort, zur Fahrtrichtung, zum Datum und zur Uhrzeit automatisiert erhoben werden. Die automatisierte Datenerhebung kann sich auch auf das Bild des Fahrzeuges erstrecken. Sie darf auch durchgeführt werden, wenn Dritte (§ 3 Absatz 4 Nummer 2) unvermeidbar betroffen sind. Der Einsatz technischer Mittel zur Erkennung von Kraftfahrzeugkennzeichen darf nicht flächendeckend durchgeführt werden; er ist für Kontrollzwecke zu dokumentieren.

(2) Die erhobenen Daten dürfen nur mit polizeilichen Dateisystemen abgeglichen werden, die auf dasselbe Schutzziel ausgerichtet sind wie die Datenerhebung nach Absatz 1. Es können für den Datenabgleich nach Satz 1 auch solche polizeilichen Dateisysteme genutzt werden, die neben präventiven auch repressiven Zwecken dienen. Automatisierte Abgleiche dürfen nicht protokolliert werden.

(3) Nach Absatz 1 erhobene Daten, die nicht in den zum Datenabgleich genutzten Dateisystemen enthalten sind (Nichttreffer), sind sofort zu löschen.

(4) Sind die nach Absatz 1 erhobenen Daten in den zum Datenabgleich genutzten Dateisystemen enthalten (Treffer), können die Daten gespeichert werden. Außer im Falle des Absatzes 1 Satz 1 Nummer 3 ist das von einem Treffer betroffene Fahrzeug unmittelbar durch die Polizei anzuhalten und die betroffene Fahrzeugführerin oder der betroffene Fahrzeugführer ist über die durchgeführte Maßnahme zu informieren. Weitere Maßnahmen dürfen erst nach einer Überprüfung des Treffers vorgenommen werden.

Die nach Satz 1 gespeicherten Daten sind außer im Falle des Absatzes 1 Satz 1 Nummer 3 und 4 spätestens 48 Stunden nach ihrer Erhebung unwiderruflich zu löschen. Die im Falle des Absatzes 1 Satz 1 Nummer 3 und 4 gespeicherten Daten können polizeilich genutzt und zusammen mit den gewonnenen Erkenntnissen an die ausschreibende Stelle übermittelt werden. Außer im Fall des Absatzes 1 Satz 1 Nummer 3 und 4 dürfen die nach Satz 1 gespeicherten Daten nicht zu einem Bewegungsbild verbunden werden.

(5) Die Polizei kann im öffentlichen Verkehrsraum technische Mittel zur Erkennung von Kraftfahrzeugkennzeichen ohne Wissen der Person auch zur Unterstützung einer Observation gemäß § 33 Absatz 1 Nummer 1 einsetzen. Absatz 1 Satz 2 bis 5 gilt entsprechend. Die erhobenen Daten können mit einem polizeilichen Dateisystem, in dem Kennzeichen von Fahrzeugen gespeichert sind, die auf die observierte Person zugelassen sind oder durch diese Person genutzt werden, abgeglichen werden. Absatz 3 und Absatz 4 Satz 1 gelten entsprechend. Die gespeicherten Daten dürfen zu einem Bewegungsbild verbunden werden. Im Übrigen sind die für die Observation gemäß § 33 Absatz 1 Nummer 1 geltenden Vorschriften zur Datenverarbeitung anzuwenden.

§ 44
Rasterfahndung

(1) Die Polizei kann von Behörden, anderen öffentlichen Stellen und von Stellen außerhalb der öffentlichen Verwaltung

1. unter den Voraussetzungen des § 67a Absatz 1 oder
2. zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist,

die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateisystemen zum Zweck des Abgleichs mit anderen Datenbeständen verlangen (Rasterfahndung), wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Abwehr der Gefahr erforderlich ist. Von den Verfassungsschutzbehörden des Bundes oder der Länder, dem Bundesnachrichtendienst sowie dem Militärischen Abschirmdienst kann die Übermittlung nach Satz 1 nicht verlangt werden.

(2) Das Übermittlungsersuchen ist auf Namen, Anschrift, Tag und Ort der Geburt sowie auf im einzelnen Falle festzulegende Merkmale zu beschränken; es darf sich nicht auf personenbezogene Daten erstrecken, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Von Übermittlungsersuchen nicht erfasste personenbezogene Daten dürfen übermittelt werden, wenn wegen erheblicher technischer Schwierigkeiten oder wegen eines unangemessenen Zeit- oder Kostenaufwands eine Beschränkung auf die angeforderten Daten nicht möglich ist; diese Daten dürfen nicht verwendet werden.

(3) Die Maßnahme bedarf der richterlichen Anordnung auf Antrag der Leitung der zuständigen Polizeibehörde. Bei Gefahr im Verzug kann die Leitung der zuständigen Polizeibehörde die Maßnahme anordnen; eine richterliche Entscheidung ist unverzüglich nachzuholen. Soweit die Anordnung nach Satz 2 nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(4) Im Antrag sind anzugeben:

1. soweit möglich die Angaben nach Absatz 2 Satz 1,
2. die zur Übermittlung zu Verpflichtenden,
3. der Sachverhalt,
4. eine Begründung.

(5) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. soweit möglich die Angaben nach Absatz 2 Satz 1,
2. die zur Übermittlung Verpflichteten,
3. der Sachverhalt,
4. die Gründe.

(6) Die oder der Landesbeauftragte für den Datenschutz ist unverzüglich über die Maßnahme zu unterrichten.

(7) Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen personenbezogenen Daten auf dem Datenträger zu löschen und die Unterlagen zurückzugeben oder zu vernichten, soweit sie nicht zur Abwehr einer anderen Gefahr im Sinne des Absatzes 1 Satz 1 oder für ein mit dem Sachverhalt zusammenhängendes Strafverfahren erforderlich sind.

Unterabschnitt 4
Pflichten der verantwortlichen Stelle und des Auftragsverarbeiters (§§ 45 - 46k)

§ 45
Berichtigung, Ergänzung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten

(1) Die verantwortliche Stelle hat personenbezogene Daten unverzüglich zu berichtigen, wenn sie unrichtig sind. Die Daten sind zu ergänzen, wenn der Zweck der Speicherung oder ein berechtigtes Interesse der betroffenen Person dies erfordert.

(2) Personenbezogene Daten sind unverzüglich zu löschen, sobald aus Anlass einer Einzelfallprüfung, die insbesondere nach Beendigung einer Datenerhebungsmaßnahme unverzüglich durchzuführen ist, oder im Rahmen einer Überprüfung nach § 45a festgestellt wird, dass

1. ihre Verarbeitung nach diesem Gesetz unzulässig war oder ist, es sei denn, die Verarbeitung ist durch Rechtsvorschriften anderer Gesetze zugelassen,
2. sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen,
3. sie unrichtig sind und die speichernde Stelle keine Kenntnis der richtigen Daten erlangen kann,
4. ihre Kenntnis zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgabe nicht mehr erforderlich ist, es sei denn, die Daten dürfen nach § 36 Absatz 2 bis 4 weiterverarbeitet werden, oder
5. eine Einwilligung nach § 26 widerrufen wird, es sei denn, die Verarbeitung ist durch Rechtsvorschriften dieses Gesetzes oder anderer Gesetze zugelassen.

Kommt eine Löschung zum Zeitpunkt der Überprüfung nicht in Betracht, ist eine neue Prüffrist festzulegen.

(3) Anstelle der Löschung tritt die Einschränkung der Verarbeitung, solange
1. Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange der betroffenen Person beeinträchtigt werden,
2. die Nutzung der personenbezogenen Daten zur Behebung einer bestehenden Beweisnot in einem gerichtlichen Verfahren oder einem Verwaltungsverfahren unerlässlich ist, oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

In ihrer Verarbeitung nach Satz 1 eingeschränkte Daten dürfen nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand; in Fällen der Nummer 1 nur mit Einwilligung der betroffenen Person. Im Übrigen dürfen solche Daten zu wissenschaftlichen Zwecken nach Maßgabe des § 37a Absatz 2 verwendet werden. Bei automatisierten Dateisystemen ist technisch sicherzustellen, dass eine Einschränkung der Verarbeitung eindeutig erkennbar ist und eine Verarbeitung für andere Zwecke nicht ohne weitere Prüfung möglich ist.

(4) Für die Übergabe der Daten an ein Archiv gelten anstelle einer Löschung aus dem in Absatz 2 Satz 1 Nummer 4 genannten Grund die Vorschriften des Landesarchivgesetzes.

(5) Nach einer Übermittlung personenbezogener Daten ist in den Fällen des Absatzes 1 bis 3 der Empfänger unverzüglich über die Berichtigung, Ergänzung, Löschung oder Einschränkung der Verarbeitung in Kenntnis zu setzen; im Fall der Ergänzung nach Absatz 1 gilt dies nur, wenn im Zeitpunkt der Übermittlung auch diese ergänzten Daten übermittelt worden wären. Die Berichtigung von unrichtigen personenbezogenen Daten ist, sofern die Daten nicht selbst erhoben wurden, der zuständigen Stelle, von der die unrichtigen Daten stammen, mitzuteilen.

§ 45a
Festlegung von Prüffristen

(1) Unbeschadet in Rechtsvorschriften festgesetzter Höchstspeicher- oder Löschfristen hat die verantwortliche Stelle für die Löschung von personenbezogenen Daten oder für eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen und durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden.

(2) Die Prüffristen dürfen

1. bei Erwachsenen fünf Jahre, in besonderen Fällen zehn Jahre,
2. bei Erwachsenen nach Vollendung des 70. Lebensjahres und bei Jugendlichen fünf Jahre,
3. bei Kindern zwei Jahre sowie
4. abweichend von Nummer 1 und Nummer 2 bei einer Sexualstraftat nach den §§ 174 bis 180, 182 oder einer Straftat nach den §§ 211 bis 213, 223 bis 227 des Strafgesetzbuches, die sexuell bestimmt ist, 15 Jahre

nicht überschreiten, wobei nach dem Zweck der Speicherung sowie der Art und Bedeutung des Sachverhaltes zu unterscheiden ist. Die Frist beginnt regelmäßig mit dem Tag der letzten behördlichen Speicherung eines für die Gefahrenprognose maßgebenden personenbezogenen Datums, jedoch nicht vor der Entlassung der betroffenen Person aus der Justizvollzugsanstalt oder Jugendanstalt, der Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung oder Sicherung oder dem Ablauf einer gerichtlich bestimmten Bewährungszeit. Gibt eine Person innerhalb der Frist des Satzes 1 Anlass zur Speicherung weiterer personenbezogener Daten über sie, die für die Gefahrenprognose maßgebend sind, so gilt für alle zu ihr gespeicherten Daten gemeinsam der Prüfungstermin, der als letzter eintritt, oder die Aufbewahrungsfrist, die als letzte endet.

(3) Ist eine weitere Aufbewahrung erforderlich, ist in regelmäßigen Abständen, spätestens bei Änderung des die Speicherung begründenden Sachverhaltes, eine erneute Prüfung durchzuführen.

§ 45b
Durchführung einer Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechtsgüter betroffener Personen zur Folge, so hat die verantwortliche Stelle vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen durchzuführen.

(2) Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohem Gefahrenpotential kann eine gemeinsame Datenschutz-Folgenabschätzung vorgenommen werden.

(3) Die verantwortliche Stelle hat die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten an der Durchführung der Folgenabschätzung zu beteiligen.

(4) Die Folgenabschätzung hat den Rechten der von der Verarbeitung betroffenen Personen Rechnung zu tragen und zumindest Folgendes zu enthalten:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,
2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck,
3. eine Bewertung der Gefahren für die Rechtsgüter der betroffenen Personen und

4. die Maßnahmen, mit denen bestehenden Gefahren abgeholfen werden soll, einschließlich der Garantien, der Sicherheitsvorkehrungen und der Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden sollen.

Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 der Verordnung (EU) 2016/679 durch die verantwortliche Stelle oder den Auftragsverarbeiter ist im Rahmen der Folgenabschätzung zu berücksichtigen.

(5) Soweit es erforderlich ist, hat die verantwortliche Stelle eine Überprüfung durchzuführen, ob die Verarbeitung den Maßgaben folgt, die sich aus der Folgenabschätzung ergeben haben.

§ 45c
Verzeichnis von Verarbeitungstätigkeiten

(1) Die verantwortliche Stelle hat ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die in ihre Zuständigkeit fallen. Dieses Verzeichnis hat hinsichtlich der Datenverarbeitung zu Zwecken der Richtlinie (EU) 2016/680 die folgenden Angaben zu enthalten:

1. den Namen und die Kontaktdaten der verantwortlichen Stelle und gegebenenfalls der gemeinsam mit ihr verantwortlichen Stellen sowie den Namen und die Kontaktdaten der oder des behördlichen Datenschutzbeauftragten,
2. die Zwecke und die Rechtsgrundlagen der Verarbeitung,
3. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen,
4. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
5. gegebenenfalls die Verwendung von Profiling,
6. gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an Staaten und Stellen nach § 39d Absatz 1, einschließlich deren Bezeichnung,
7. die Prüffristen nach § 45a oder die Aufbewahrungs- oder Speicherungsdauer und
8. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach den §§ 46d bis 46i.

Bei automatisierten Verfahren gemäß § 42 sind im Verzeichnis alle verantwortlichen Stellen zu benennen. Ferner ist bei Vorliegen einer Vereinbarung nach § 42 Absatz 3 zu ergänzen, für welchen konkreten Bereich der Datenverarbeitung jede der beteiligten Stellen verantwortlich ist.

(2) Der Auftragsverarbeiter hat ein Verzeichnis aller Kategorien von Verarbeitungen, die er im Auftrag einer verantwortlichen Stelle durchführt, zu führen, das hinsichtlich der Datenverarbeitung zu Zwecken der Richtlinie (EU) 2016/680 Folgendes zu enthalten hat:

1. den Namen und die Kontaktdaten des Auftragsverarbeiters, jeder verantwortlichen Stelle, in deren Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls der oder des behördlichen Datenschutzbeauftragten,
2. gegebenenfalls Übermittlungen von personenbezogenen Daten an Staaten und Stellen nach § 39d Absatz 1, einschließlich deren Bezeichnung,

3. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach den §§ 46d bis 46h.

(3) Die in den Absätzen 1 und 2 genannten Verzeichnisse sind elektronisch zu führen. Dies gilt auch für die nach Artikel 30 der Verordnung (EU) 2016/679 zu führenden Verzeichnisse.

(4) Die verantwortlichen Stellen und die Auftragsverarbeiter haben auf Anforderung ihre Verzeichnisse der oder dem Landesbeauftragten für den Datenschutz zur Verfügung zu stellen.

§ 46
Allgemeine Informationspflicht

(1) Im Anwendungsbereich der Richtlinie (EU) 2016/680 hat die verantwortliche Stelle in allgemeiner Form und für jede Person zugänglich Informationen zur Verfügung zu stellen über

1. die Zwecke der von ihr vorgenommenen Verarbeitungen,
2. die im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten bestehenden Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung,
3. den Namen und die Kontaktdaten der verantwortlichen Stelle und der oder des behördlichen Datenschutzbeauftragten,
4. das Recht, die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz anzurufen, und
5. die Erreichbarkeit der oder des Landesbeauftragten für den Datenschutz.

(2) Im Anwendungsbereich der Verordnung (EU) 2016/679 gilt unter Beachtung der Artikel 13 und 14 der Verordnung (EU) 2016/679 § 5 des Landesdatenschutzgesetzes.

§ 46a
Benachrichtigungspflichten bei verdeckten und eingriffsintensiven Maßnahmen

(1) Bei folgenden Maßnahmen sind die dort jeweils benannten Personen durch die durchführende Stelle zu benachrichtigen:

1. bei Feststellung der Identität von Personen auf Übersichtsaufzeichnungen nach§ 32 Absatz 1 Satz 1 Nummer 2 Satz 2 die Adressaten der Maßnahme,
2. bei Einsatz besonderer Mittel der Datenerhebung nach § 33 Absatz 1
   a) die Adressaten der Maßnahme,
   b) diejenigen, deren personenbezogene Daten verarbeitet wurden und
   c) diejenigen, deren nicht allgemein zugängliche Wohnung betreten wurde,
3. bei Einsatz technischer Mittel in Wohnungen nach § 33b die von der Maßnahme betroffenen Personen, auch wenn die Maßnahme nach § 33b Absatz 9 als Personenschutzmaßnahme erfolgt ist,

4. bei verdecktem Zugriff auf informationstechnische Systeme nach § 33c, Eingriffen in den Telekommunikationsbereich nach § 33d oder Inanspruchnahme von Diensteanbietern nach den §§ 33e bis 33g und § 33h Absatz 1 Satz 2 und Absatz 2,
   a) die Adressaten der Maßnahme und
   b) diejenigen, deren personenbezogene Daten im Rahmen einer solchen Maßnahme verarbeitet wurden,
5. bei Ausschreibung zur polizeilichen Beobachtung oder gezielten Kontrolle nach § 35
   a) die Adressaten der Maßnahme und
   b) diejenigen, deren personenbezogene Daten verarbeitet wurden,
6. bei Rasterfahndung nach § 44 die Personen, gegen die nach Auswertung der Daten weitere Maßnahmen durchgeführt wurden,
7. bei elektronischer Aufenthaltsüberwachung nach § 67a die Adressaten der Maßnahme, wenn Bewegungsbilder erstellt wurden, wobei die Benachrichtigung spätestens zwei Monate nach deren Beendigung zu erfolgen hat.

Erfolgen Maßnahmen mit Mitteln des § 33d Absatz 3, sind die in Satz 1 Nummer 4 genannten Personen auch darüber zu unterrichten, dass mit technischen Mitteln verdeckt auf informationstechnische Systeme zugegriffen wurde. Die Benachrichtigung unterbleibt, soweit überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen. Zudem kann die Benachrichtigung einer in Satz 1 Nummer 2, 4 und 5 bezeichneten Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen wurde. Nachforschungen zur Feststellung der Identität oder des Aufenthaltsortes einer in Satz 1 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist. Bezieht sich die Benachrichtigung auf Daten, die an oder von Verfassungsschutzbehörden des Bundes oder der Länder oder die an den oder von dem Bundesnachrichtendienst oder Militärischen Abschirmdienst übermittelt wurden, ist sie nur nach Zustimmung dieser Stellen zulässig.

(2) Die Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Zwecks der Maßnahme, der eingesetzten Polizeibeamtinnen und Polizeibeamten oder Vertrauenspersonen oder der in der jeweiligen Befugnisnorm genannten Rechtsgüter geschehen kann. In den Fällen des Absatzes 1 Satz 1 Nummer 2 und bei Maßnahmen nach § 33b Absatz 9 ist auch eine Gefährdung der weiteren Verwendung von Vertrauenspersonen und verdeckt Ermittelnden als bedeutender Belang zu berücksichtigen. Ist wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen die betroffene Person eingeleitet worden, ist die Benachrichtigung in Abstimmung mit der Staatsanwaltschaft zurückzustellen, solange der Stand des Ermittlungsverfahrens eine Benachrichtigung nicht zulässt.

(3) Die Benachrichtigung hat zumindest zu enthalten:

1. die Angaben nach § 46 Absatz 1,
2. die Rechtsgrundlage der Datenerhebung und gegebenenfalls der weiteren Verarbeitung,
3. Informationen über die mutmaßliche Dauer der Datenspeicherung oder, falls diese Angabe nicht möglich ist, Kriterien hierfür sowie
4. gegebenenfalls über die Kategorien der Empfänger der Daten.

(4) Wird die Benachrichtigung aus einem der in Absatz 2 genannten Gründe zurückgestellt, bedarf die weitere Zurückstellung der richterlichen Zustimmung, wenn sie nicht innerhalb des folgenden Zeitraums erfolgt:

1. sechs Monate nach Beendigung des Einsatzes technischer Mittel in Wohnungen nach § 33b oder des verdeckten Zugriffs auf informationstechnische Systeme nach § 33c oder § 33d Absatz 3 oder
2. ein Jahr nach Beendigung einer der übrigen in Absatz 1 Satz 1 Nummer 1 bis 6 bezeichneten Maßnahmen.

Sind mehrere Maßnahmen in einem engen zeitlichen Zusammenhang durchgeführt worden, so beginnt die in Satz 1 genannte Frist mit der Beendigung der letzten Maßnahme. Die richterliche Entscheidung ist vorbehaltlich einer anderen richterlichen Anordnung jeweils nach einem Jahr erneut einzuholen. Eine Benachrichtigung kann mit richterlicher Zustimmung frühestens nach dem Ablauf von fünf Jahren auf Dauer unterbleiben, wenn
1. überwiegende Interessen einer betroffenen Person entgegenstehen oder
2. die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden

und eine Verwendung der Daten gegen die betroffene Person ausgeschlossen ist. In diesem Fall sind die Daten zu löschen.

§ 46b
Benachrichtigung über die Speicherung personenbezogener Daten von Kindern und unter Betreuung stehenden Personen

Werden personenbezogene Daten von Kindern ohne Kenntnis der Sorgeberechtigten verarbeitet, sind die Sorgeberechtigten durch die verantwortliche Stelle zu benachrichtigen, sobald die Aufgabenerfüllung hierdurch nicht mehr gefährdet wird. Die Benachrichtigung kann zurückgestellt werden, solange zu besorgen ist, dass die Benachrichtigung zu erheblichen Nachteilen für das Kind führt; § 46a Absatz 4 gilt entsprechend. Satz 1 und 2 gelten sinngemäß für unter Betreuung stehende Personen.

§ 46c
Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten

(1) Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich eine hohe Gefährdung für Rechtsgüter betroffener Personen zur Folge, hat die verantwortliche Stelle diese Personen unverzüglich über den Vorfall zu benachrichtigen.

(2) Die Benachrichtigung nach Absatz 1 hat in allgemein verständlicher Weise die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und zumindest die folgenden Angaben zu enthalten:

1. den Namen und die Kontaktdaten der oder des behördlichen Datenschutzbeauftragten oder einer sonstigen Person oder Stelle, die weitere Informationen erteilen kann,
2. eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
3. eine Beschreibung der von der verantwortlichen Stelle ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung und der getroffenen Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(3) Die Benachrichtigung der betroffenen Personen nach Absatz 1 kann zurückgestellt oder eingeschränkt werden oder unterbleiben, soweit und solange

1. die Benachrichtigung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
2. die personenbezogenen Daten oder die Tatsache ihrer Verarbeitung nach einer Rechtsvorschrift geheim zu halten sind,
3. die Benachrichtigung die Sicherheit von Datenverarbeitungssystemen gefährden würde,
4. die Benachrichtigung die Rechtsgüter einer anderen Person gefährden würde oder
5. die Benachrichtigung die Erfüllung der Aufgaben nach diesem Gesetz gefährden oder wesentlich erschweren würde

und soweit nicht die Interessen der betroffenen Person aufgrund der von der Verletzung ausgehenden Gefährdung im Sinne des Absatzes 1 überwiegen.

(4) Die Benachrichtigung nach Absatz 1 kann unterbleiben, wenn

1. die verantwortliche Stelle für die von der Verletzung betroffenen Daten geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat; dies gilt insbesondere für Vorkehrungen wie Verschlüsselungen, durch die die Daten für unbefugte Personen unzugänglich gemacht wurden;
2. die verantwortliche Stelle durch unmittelbar im Anschluss an die Verletzung getroffene Maßnahmen sichergestellt hat, dass aller Wahrscheinlichkeit nach keine Gefährdung im Sinne des Absatzes 1 mehr besteht, oder
3. dies, insbesondere wegen der Vielzahl betroffener Personen, mit einem unverhältnismäßigen Aufwand verbunden wäre; in diesem Fall hat die verantwortliche Stelle die Verletzung nach Maßgabe des Absatzes 2 öffentlich bekannt zu machen oder eine ähnlich wirksame Maßnahme zur Information zu ergreifen.

(5) Wenn die verantwortliche Stelle die betroffenen Personen über eine Verletzung des Schutzes personenbezogener Daten nicht benachrichtigt hat, kann die oder der Landesbeauftragte für den Datenschutz die Nachholung von der verantwortlichen Stelle verlangen oder förmlich feststellen, dass ihrer oder seiner Auffassung nach die in Absatz 4 genannten Voraussetzungen nicht erfüllt sind. Hierbei hat sie oder er die Wahrscheinlichkeit zu berücksichtigen, dass die Verletzung eine Gefährdung im Sinne des Absatzes 1 zur Folge hat.

(6) In einem Straf- oder Ordnungswidrigkeitenverfahren gegen die meldepflichtige oder benachrichtigende Person oder einen ihrer in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen darf eine Benachrichtigung nach Absatz 1 nur mit Zustimmung der meldepflichtigen oder benachrichtigenden Person verwendet werden.

§ 46d
Dokumentationspflichten

(1) Die verantwortliche Stelle und der Auftragsverarbeiter haben zu jeder Maßnahme insbesondere Folgendes zu dokumentieren:

1. die Rechtsgrundlage der Erhebung personenbezogener Daten,
2. die Weiterverarbeitung personenbezogener Daten im Sinne des § 36 Absatz 1 und die Zweckänderung sowie deren Gründe.
3. die sonstige weitere Verwendung personenbezogener Daten, insbesondere die Abfrage, die Offenlegung einschließlich Übermittlung, die Kombination, die Einschränkung der Verarbeitung und die Löschung, sowie die Gründe der weiteren Verwendung; bei einer Berichtigung, Ergänzung und Löschung fehlerhafter, unvollständiger und unrichtiger Daten zusätzlich auch den Zeitraum und die Gründe, die zur Fehlerhaftigkeit, Unvollständigkeit oder Unrichtigkeit geführt haben,
4. den auch nur vorübergehenden Verzicht auf die Löschung personenbezogener Daten sowie deren Gründe,
5. die Benachrichtigung von Datenempfängern in Fällen von § 45 Absatz 5,
6. die Festlegung von Prüffristen nach § 45a sowie deren Bemessungsgründe,
7. die Benachrichtigung betroffener Personen nach den §§ 46a bis 46c, die Zurückstellung sowie das Unterbleiben der Benachrichtigung sowie die Gründe und
8. die Benachrichtigung der oder des Landesbeauftragten für den Datenschutz.

Im Rahmen der Dokumentation sind auch das Datum und soweit erforderlich die Uhrzeit des Verarbeitungsvorgangs festzuhalten. Bei der Übermittlung personenbezogener Daten muss zudem aus der Dokumentation die Aktenfundstelle, die Identität der übermittelnden Person, welche Daten übermittelt wurden und deren Empfänger erkennbar sein.

(2) Dokumentationen zu den in § 46f Absatz 2 genannten verdeckten und eingriffsintensiven Maßnahmen müssen zumindest den in §§ 46e und 46f aufgeführten Protokollierungen entsprechen. Sie sind ebenso wie Dokumentationen zu Datenübermittlungen an Drittstaaten und weitere zwischen- und überstaatliche Stellen nach den §§ 39d bis 39h sowie nach der Verordnung (EU) 2016/679 mindestens bis zum Abschluss der Kontrolle nach § 48b Absatz 6 aufzubewahren.

(3) Soweit die Dokumentationen den Protokollierungen in § 46f entsprechen, dürfen sie nur zu den in § 46f Absatz 4 Satz 1 genannten Zwecken verwendet werden. Im Übrigen dürfen Dokumentationen zu den in § 46e Absatz 4 Satz 1 genannten Zwecken verwendet werden.

§ 46e
Protokollierungspflichten

(1) In automatisierten Verfahren nach § 42 haben die verantwortlichen Stellen und die Auftragsverarbeiter mindestens die folgenden Verarbeitungsvorgänge zu protokollieren:

1. Erhebung,
2. Veränderung,
3. Abfrage,
4. Offenlegung einschließlich Übermittlung,
5. Kombination und
6. Löschung.

(2) Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen.

(3) Die Protokollierung erfolgt in einer Weise, dass die Protokolle

1. der oder dem behördlichen Datenschutzbeauftragten und der oder dem Landesbeauftragten für den Datenschutz in elektronisch auswertbarer Form für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung zur Verfügung stehen und
2. eine Überprüfung ermöglichen, dass Zugriffe auf personenbezogene Daten im automatisierten Verfahren innerhalb festgelegter Zugriffsberechtigungen erfolgen.

(4) Protokollierungen dürfen nur verwendet werden
1. zur Erfüllung von Informationspflichten nach § 46,
2. zur Erfüllung von Benachrichtigungspflichten nach den §§ 46a bis 46c,
3. zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung, auch durch die betroffene Person, einschließlich der Eigenüberwachung,
4. zur Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten,
5. zur Verhütung und Verfolgung von Straftaten oder Ordnungswidrigkeiten,
6. soweit dies nach § 48h zur Erstellung der Berichte und Unterrichtungen erforderlich ist.

Sie sind, soweit gesetzlich nichts anderes bestimmt ist, am Ende des auf deren Generierung folgenden Jahres zu löschen, es sei denn, dass sie für die in Satz 1 genannten Zwecke noch erforderlich sind. Bei den in § 46f Absatz 2 genannten Maßnahmen und bei der Übermittlung personenbezogener Daten an Drittstaaten und weitere zwischen- und überstaatliche Stellen nach den §§ 39d bis 39h sowie nach der Verordnung (EU) 2016/679 tritt an die Stelle der in Satz 2 bestimmten Frist die in § 48b Absatz 6 genannte Frist.

(5) Protokollierungen sind durch technische und organisatorische Maßnahmen zu sichern und der oder dem Landesbeauftragten für den Datenschutz auf Verlangen zur Verfügung zu stellen.

(6) Abweichende Regelungen bestimmt § 115 Absatz 3.

§ 46f
Protokollierungspflichten bei verdeckten und eingriffsintensiven Maßnahmen

(1) Bei den in § 46a Absatz 1 Satz 1 aufgeführten Maßnahmen sind neben den nach § 46e zu protokollierenden Vorgängen zu protokollieren:

1. das zur Datenerhebung eingesetzte Mittel,
2. der Zeitpunkt des Einsatzes,
3. Angaben, die die Feststellung der erhobenen Daten ermöglichen, sowie
4. die Organisationseinheit, die die Maßnahme durchführt.

(2) Zu protokollieren sind auch
1. bei Feststellung der Identität von Personen auf Übersichtsaufzeichnungen nach§ 32 Absatz 1 Satz 1 Nummer 2 Satz 2 die Adressaten der Maßnahme,
2. bei Einsatz besonderer Mittel der Datenerhebung nach § 33 Absatz 1
   a) die Adressaten der Maßnahme,
   b) diejenigen, deren personenbezogene Daten verarbeitet wurden und
   c) diejenigen, deren nicht allgemein zugängliche Wohnung betreten wurde,
3. bei Einsatz technischer Mittel in Wohnungen nach § 33b die von der Maßnahme betroffenen Personen, auch wenn die Maßnahme nach § 33b Absatz 9 als Personenschutzmaßnahme erfolgt ist,
4. bei verdecktem Zugriff auf informationstechnische Systeme nach § 33c und nach § 33d Absatz 3
   a) die Adressaten der Maßnahme,
   b) diejenigen, deren personenbezogene Daten im Rahmen einer solchen Maßnahme verarbeitet wurden und
   c) die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
5. bei sonstigen Eingriffen in den Telekommunikationsbereich nach § 33d oder Inanspruchnahme von Diensteanbietern nach den §§ 33e bis 33g,
   a) die Adressaten der Maßnahme,
   b) diejenigen, deren personenbezogene Daten im Rahmen einer solchen Maßnahme verarbeitet wurden und
6. bei Ausschreibung zur polizeilichen Beobachtung oder gezielten Kontrolle nach § 35
   a) die Adressaten der Maßnahme und
   b) diejenigen, deren personenbezogene Daten verarbeitet wurden,
7. bei Rasterfahndung nach § 44
   a) die im Übermittlungsersuchen nach § 44 Absatz 2 Satz 1 enthaltenen Merkmale und
   b) die Personen, gegen die nach Auswertung der Daten weitere Maßnahmen durchgeführt wurden,
8. bei elektronischer Aufenthaltsüberwachung nach § 67a die Adressaten der Maßnahme, wenn Bewegungsbilder erstellt wurden, wobei die Benachrichtigung spätestens zwei Monate nach deren Beendigung zu erfolgen hat.

(3) Nachforschungen zur Feststellung der Identität einer in Absatz 2 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist. Die Zahl der Personen, deren Protokollierung unterblieben ist, ist im Protokoll anzugeben.

(4) Diese Protokolldaten dürfen nur verwendet werden für Zwecke der Benachrichtigung nach den §§ 46a bis 46c und § 48d, soweit erforderlich für die Erstellung der Berichte und Unterrichtungen nach § 48h oder um der betroffenen Person oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahmen rechtmäßig durchgeführt worden sind. Sie sind bis zum Abschluss der Kontrolle nach § 48b Absatz 6 aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 1 genannten Zweck noch erforderlich sind.

§ 46g
Kennzeichnungspflichten

(1) Bei der Speicherung in automatisierten polizeilichen Verfahren nach § 42 sind personenbezogene Daten wie folgt zu kennzeichnen:

1. Angabe des Mittels der Erhebung der Daten einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden,
2. Angabe der Kategorie nach § 25a Absatz 2 bei Personen, zu denen Grunddaten nach § 3 Absatz 5 Nummer 2 angelegt wurden,
3. Angabe der
   a) Rechtsgüter, deren Schutz ihre Erhebung dient oder
   b) Straftaten oder Ordnungswidrigkeiten, deren Verfolgung oder Verhütung ihre Erhebung dient,
4. Angabe der Stelle, die sie erhoben hat,
5. falls zutreffend die Angabe, dass sie in oder aus Wohn- oder Geschäftsräumen oder befriedetem Besitztum erhoben wurden,
6. falls zutreffend die Angabe, dass es sich um kernbereichsrelevante Daten nach § 26a handelt, soweit diese nicht unverzüglich gelöscht werden konnten,
7. falls zutreffend die Angabe, dass es sich um Daten nach § 26b, die den Schutz zeugnisverweigerungsberechtigter Personen betreffen, handelt, soweit diese nicht unverzüglich gelöscht werden konnten,
8. falls zutreffend die Angaben, ob sie beim Diensteanbieter erhoben wurden und um welche konkrete Datenart es sich handelt; im Fall des § 33d auch die Angabe, auf welcher konkreten Rechtsgrundlage des Telekommunikationsgesetzes der Diensteanbieter die Daten gespeichert hat,
9. falls zutreffend die Angabe, dass es sich um besondere Kategorien personenbezogener Daten nach § 3 Absatz 5 Nummer 3 handelt,
10. falls zutreffend die Angaben, dass es sich bei ihnen um eine persönliche Einschätzung oder Beurteilung handelt und welche Stelle die Unterlagen führt, die der auf einer persönlichen Einschätzung beruhenden Beurteilung zugrunde liegen.

Die Kennzeichnung nach Satz 1 Nummer 1 kann auch durch die Angabe der Rechtsgrundlage der jeweiligen Mittel der Datenerhebung ergänzt werden. Sollen personenbezogene Daten zu einem anderen Zweck als dem, zu dem sie erhoben wurden, weiterverarbeitet werden, sind sie zu kennzeichnen.

(2) Personenbezogene Daten, die nicht entsprechend den Anforderungen des Absatzes 1 gekennzeichnet sind, dürfen so lange nicht weiterverarbeitet oder übermittelt werden, bis eine Kennzeichnung entsprechend den Anforderungen des Absatzes 1 erfolgt ist.

(3) Durch geeignete technische Maßnahmen ist sicherzustellen, dass die Kennzeichnung auch nach einer Übermittlung an eine andere Stelle erhalten bleibt. Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung nach Absatz 1 durch diese Stelle aufrechtzuerhalten.

(4) Abweichende Regelungen bestimmt § 115 Absatz 1 und 2.

§ 46h
Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Die verantwortliche Stelle hat sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst angemessene Vorkehrungen zu treffen, die geeignet sind, die Datenschutzgrundsätze wie etwa die Datensparsamkeit wirksam umzusetzen, und die sicherstellen, dass die gesetzlichen Anforderungen eingehalten und die Rechte der betroffenen Personen geschützt werden. Sie hat hierbei den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen zu berücksichtigen. Insbesondere sind die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. Personenbezogene Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verarbeitungszweck möglich ist.

(2) Die verantwortliche Stelle hat geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden können, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Dies betrifft die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Die Maßnahmen müssen insbesondere gewährleisten, dass die Daten durch Voreinstellungen nicht automatisiert einer unbestimmten Anzahl von Personen zugänglich gemacht werden können.

(3) Die Einhaltung eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 der Verordnung (EU) 2016/679 durch die verantwortliche Stelle kann als Umstand zum Nachweis für die Erfüllung der Anforderungen in den Absätzen 1 und 2 dienen.

§ 46i
Anforderungen an die Sicherheit der Datenverarbeitung

(1) Die verantwortliche Stelle und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Die verantwortliche Stelle hat hierbei die einschlägigen Standards, Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 der Verordnung (EU) 2016/679 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 der Verordnung (EU) 2016/679 kann als Umstand zum Nachweis der Erfüllung der Anforderungen nach den Absätzen 1 bis 3 dienen.

(2) Die in Absatz 1 genannten Maßnahmen sollen unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. Die Maßnahmen nach Absatz 1 sollen dazu führen, dass
1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und
2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

(3) Im Fall einer automatisierten Verarbeitung haben die verantwortliche Stelle und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

1. Verwehrung des Zugangs für Unbefugte zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird (Zugangskontrolle),
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle),
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle),
6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),
8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle),

9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit),
10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),
11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),
12. Gewährleistung, dass personenbezogene Daten, zu denen der verantwortlichen Stelle oder dem Auftragsverarbeiter unterstellte Personen Zugang haben, nur entsprechend den Weisungen der verantwortlichen Stelle verarbeitet werden können (Auftragskontrolle),
13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).

Ein Zweck nach Satz 1 Nummer 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

(4) Die Maßnahmen zur Datensicherheit sind regelmäßig auf ihre Wirksamkeit hin zu überprüfen und zu bewerten.

§ 46j
Vertrauliche Meldung von Verstößen

Die verantwortliche Stelle hat zu ermöglichen, dass ihr vertrauliche Meldungen über in ihrem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften zugeleitet werden können.

§ 46k
Auftragsverarbeitung

(1) Erfolgt die Verarbeitung personenbezogener Daten im Auftrag durch andere Personen oder Stellen, bleibt die beauftragende Stelle verantwortliche Stelle und hat für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz zu sorgen. Die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Schadensersatz sind in diesem Fall gegenüber der verantwortlichen Stelle geltend zu machen.

(2) Die verantwortliche Stelle hat den Auftragsverarbeiter insbesondere unter Berücksichtigung der Art der zu verarbeitenden Daten sorgfältig auszuwählen. Der Auftragsverarbeiter muss mit geeigneten technischen und organisatorischen Maßnahmen sicherstellen können, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 der Verordnung (EU) 2016/679 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 der Verordnung (EU) 2016/679 durch einen Auftragsverarbeiter kann als Umstand zur Begründung für dessen Geeignetheit im Sinne des Satzes 2 dienen.

(3) Auftragsverarbeiter dürfen ohne vorherige schriftliche Genehmigung der verantwortlichen Stelle keine weiteren Auftragsverarbeiter hinzuziehen. Hat die verantwortliche Stelle dem Auftragsverarbeiter eine allgemeine Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter erteilt, hat der Auftragsverarbeiter die verantwortliche Stelle über jede beabsichtigte Hinzuziehung oder Ersetzung zu informieren. Die verantwortliche Stelle kann in diesem Fall die Hinzuziehung oder Ersetzung untersagen.

(4) Zieht ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter hinzu, so hat er diesem dieselben Verpflichtungen aus seinem Vertrag mit der verantwortlichen Stelle nach Absatz 5 aufzuerlegen, die auch für ihn gelten, soweit diese Pflichten für den weiteren Auftragsverarbeiter nicht schon aufgrund anderer Vorschriften verbindlich sind. Absatz 2 gilt entsprechend. Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber der verantwortlichen Stelle für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.

(5) Die Auftragsverarbeitung ist in einem Vertrag oder einer anderen verbindlichen Regelung auszugestalten, der oder die den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten der verantwortlichen Stelle festlegt. Der Vertrag oder die andere Regelung haben insbesondere vorzusehen, dass der Auftragsverarbeiter

1. nur auf dokumentierte Weisung der verantwortlichen Stelle handelt; ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Auftraggebers gegen eine Vorschrift über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen;
2. gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden, soweit sie keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
3. die verantwortliche Stelle mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten;
4. alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl der verantwortlichen Stelle zurückgibt oder löscht und bestehende Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht;
5. der verantwortlichen Stelle alle erforderlichen Informationen, insbesondere die gemäß den §§ 46d bis 46f erstellten Dokumentationen und Protokolle, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt;
6. Überprüfungen durch die verantwortliche Stelle, eine von dieser beauftragten Prüferin oder einen von dieser beauftragten Prüfer oder die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz ermöglicht und diese unterstützt;
7. die in den Absätzen 3 und 4 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
8. alle gemäß § 46i erforderlichen Maßnahmen ergreift und
9. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen die verantwortliche Stelle bei der Einhaltung der in den §§ 45b, 46c, 46i, 48c und 48d genannten Pflichten unterstützt.

(6) Der Vertrag im Sinne des Absatzes 5 bedarf der Schriftform; § 3a des Landesverwaltungsverfahrensgesetzes gilt entsprechend. Die oder der Landesbeauftragte für den Datenschutz ist über die Beauftragung zu informieren.

(7) Ein Auftragsverarbeiter, der die Zwecke und Mittel der Verarbeitung unter Verstoß gegen diese Vorschrift bestimmt, gilt in Bezug auf diese Verarbeitung als verantwortliche Stelle.

Unterabschnitt 5
Rechte der betroffenen Person (§§ 47 - 48a)

§ 47
Recht auf Anrufung der oder des Landesbeauftragten für den Datenschutz

Jede betroffene Person kann sich unbeschadet anderweitiger Rechtsbehelfe mit einer Beschwerde an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz wenden, wenn sie der Auffassung ist, bei der Verarbeitung ihrer personenbezogenen Daten nach diesem Gesetz durch die Polizei oder Ordnungsbehörden in ihren Rechten verletzt worden zu sein.

§ 48
Recht auf Auskunft und Akteneinsicht

(1) Die verantwortliche Stelle teilt einer Person auf deren schriftlichen Antrag gebührenfrei mit, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, erhält die Person ihrem Antrag entsprechend Auskunft über sie betreffende personenbezogene Daten und über

1. die Rechtsgrundlage und die Zwecke der Verarbeitung,
2. verfügbare Informationen zur Herkunft der Daten oder, falls dies im Einzelfall nicht möglich ist, zu den Kategorien personenbezogener Daten, die verarbeitet werden,
3. die Empfänger, gegenüber denen die personenbezogenen Daten offengelegt wurden,
4. die für deren Speicherung vorgesehene Dauer oder, falls dies im Einzelfall nicht möglich ist, die Kriterien für deren Festlegung,
5. die bestehenden Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung gemäß § 48a und
6. die Kontaktdaten der oder des Landesbeauftragten für den Datenschutz und die Möglichkeit, bei ihr oder ihm Beschwerde nach § 47 einzulegen.

Bestehen begründete Zweifel an der Identität der antragstellenden Person, kann die Erteilung der Auskunft von der Erbringung geeigneter Nachweise abhängig gemacht werden.

(2) Wurden personenbezogene Daten von oder an andere Stellen übermittelt, gibt die verantwortliche Stelle diesen vor Erteilung der Auskunft Gelegenheit zur Stellungnahme. Ergibt sich aus der Stellungnahme, dass eine Auskunftserteilung die Aufgabenerfüllung dieser Stellen gefährden würde, unterbleibt die Auskunft. Die Auskunft zur Übermittlung personenbezogener Daten von oder an Verfassungsschutzbehörden des Bundes oder der Länder, den Bundesnachrichtendienst oder den Militärischen Abschirmdienst, wird nur mit Zustimmung dieser Stellen erteilt.

(3) Ein Auskunftsanspruch besteht nicht, wenn eine Auskunft bereits erteilt wurde und die gespeicherten personenbezogenen Daten sich nicht geändert haben oder die Auskunft offensichtlich missbräuchlich verlangt wird. Darüber hinaus gelten für das Zurückstellen, Einschränken oder Unterbleiben der Auskunft die §§ 46a bis 46c entsprechend. Die Regelungen zu den Benachrichtigungspflichten nach den §§ 46 a bis 46c bleiben unberührt.

(4) Sind personenbezogene Daten in Akten oder nicht automatisierten Dateisystemen gespeichert, ist der betroffenen Person auf schriftlichen Antrag bei der verantwortlichen Stelle unter den Voraussetzungen der Absätze 1 bis 3 gebührenfrei Einsicht in die jeweiligen ihn betreffenden Akten oder Dateien zu gewähren. Die Einsichtnahme darf nicht erfolgen, wenn die personenbezogenen Daten der betroffenen Person mit personenbezogenen Daten Dritter im Sinne von § 3 Absatz 4 Nummer 2 oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist der betroffenen Person jedoch über die zu ihr gespeicherten Daten Auskunft zu erteilen. Rechtsvorschriften über die Akteneinsicht im Verwaltungsverfahren bleiben unberührt.

(5) Die betroffene Person wird unverzüglich durch die verantwortliche Stelle darüber in Kenntnis gesetzt, wie mit dem Antrag nach Absatz 1 oder 4 verfahren wird, falls über ihn nicht unverzüglich entschieden wird. Soweit ein Antrag abgelehnt wird, ist die betroffene Person hierüber unter Mitteilung der Gründe schriftlich zu unterrichten und darauf hinzuweisen, dass sie Beschwerde bei der oder dem Landesbeauftragten für den Datenschutz einlegen oder ihre Rechte auch über diese oder diesen ausüben kann. Die Mitteilung der Gründe unterbleibt, soweit und solange hierdurch

1. die Erfüllung der Aufgaben nach diesem Gesetz erheblich erschwert oder gefährdet werden würde,
2. die öffentliche Sicherheit oder Ordnung gefährdet würde, oder
3. überwiegende Rechte anderer Personen gefährdet werden würden.

Die Begründung für das Unterbleiben der Mitteilung der Gründe ist von der verantwortlichen Stelle zu dokumentieren. Sie sind der oder dem Landesbeauftragten für deren oder dessen Kontrolle in auswertbarer Weise zur Verfügung zu stellen, soweit nicht das Ministerium für Inneres und Europa im Einzelfall feststellt, dass dadurch die Sicherheit des Landes, eines anderen Bundeslandes oder des Bundes gefährdet würde. Eine Mitteilung der oder des Landesbeauftragten für den Datenschutz an die betroffene Person im Beschwerdeverfahren darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(6) Wird ein Antrag nicht vollständig genehmigt oder über ihn nicht unverzüglich entschieden, ist die betroffene Person schriftlich darauf hinzuweisen, dass sie Beschwerde bei der oder dem Landesbeauftragten für den Datenschutz einlegen, ihre Rechte auch über diese oder diesen ausüben oder gerichtlichen Rechtsschutz in Anspruch nehmen kann.

(7) § 6 Absatz 5 des Landesdatenschutzgesetzes gilt entsprechend.

(8) Bei offensichtlich unbegründeten oder in ungebührlichem Umfang gestellten Anträgen können angemessene Kosten erhoben werden, soweit nicht ausnahmsweise schon von der Bearbeitung abgesehen werden kann.

§ 48a
Recht auf Berichtigung, Ergänzung, Löschung sowie Einschränkung der Verarbeitung

(1) Die betroffene Person kann bei der verantwortlichen Stelle gebührenfrei die unverzügliche Berichtigung, Ergänzung, Löschung oder Einschränkung der Verarbeitung ihrer personenbezogenen Daten schriftlich beantragen. Bestehen begründete Zweifel an der Identität der antragstellenden Person, kann die Bearbeitung ihres Anliegens von der Erbringung geeigneter Nachweise abhängig gemacht werden. Im Fall von Aussagen, Beurteilungen oder anderweitigen Wertungen betrifft die Frage der Richtigkeit der Daten nicht deren Inhalt, sondern die Tatsache, ob die Aussage, Beurteilung oder anderweitige Wertung so erfolgt ist. Kann die Richtigkeit der Daten nicht erwiesen werden, werden die Daten in der Verarbeitung eingeschränkt. In diesem Fall wird die betroffene Person unterrichtet, bevor die Verarbeitungseinschränkung aufgehoben wird.

(2) Die verantwortliche Stelle prüft nach Maßgabe des § 45 den Antrag. Sie hat die betroffene Person über die Genehmigung des Antrages beziehungsweise über ein Absehen von der Berichtigung, Ergänzung oder Löschung oder über die an deren Stelle tretende Einschränkung der Verarbeitung der personenbezogenen Daten schriftlich zu unterrichten; im Falle einer Ablehnung des Antrages sind der betroffenen Person auch die Gründe mitzuteilen. Die Mitteilung der Gründe unterbleibt, soweit und solange hierdurch

1. die Erfüllung polizeilicher Aufgaben nach diesem Gesetz erheblich erschwert oder gefährdet werden würde,
2. die öffentliche Sicherheit oder Ordnung gefährdet werden würde, oder
3. überwiegende Rechte anderer Personen gefährdet werden würden.

Falls über den Antrag nicht unverzüglich entschieden wird, wird die betroffene Person unverzüglich darüber in Kenntnis gesetzt, wie mit dem Antrag verfahren wird.

(3) § 48 Absatz 6 bis 8 gilt entsprechend.

Unterabschnitt 6
Datenschutzaufsichtliche und parlamentarische Kontrolle (§§ 48b - 48h)

§ 48b
Aufsicht durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz über die Datenverarbeitung

(1) Unbeschadet anderer Regelungen dieses Gesetzes nimmt die oder der Landesbeauftragte für den Datenschutz im Rahmen der Aufsicht über die Datenverarbeitung zu Zwecken der Richtlinie (EU) 2016/680 die Aufgaben entsprechend Artikel 57 Absatz 1 Buchstabe a bis i und t der Verordnung (EU) 2016/679 wahr und übt die Befugnisse entsprechend Artikel 58 Absatz 1, Absatz 2 Buchstabe a und b, Absatz 3 Buchstabe a und b dieser Verordnung aus.

(2) Weitergehende Maßnahmen darf die oder der Landesbeauftragte für den Datenschutz im Anwendungsbereich der Richtlinie (EU) 2016/680 nur anordnen, wenn dies zur Abwendung einer nach Ausübung der Befugnisse nach Absatz 1 fortbestehenden wesentlichen Verletzung datenschutzrechtlicher Vorschriften erforderlich ist und die Aufgabenwahrnehmung durch die verantwortliche Stelle dadurch nicht wesentlich beeinträchtigt wird. Eine Löschung von personenbezogenen Daten darf nicht angeordnet werden.

(3) Unbeschadet der Bestimmungen in Absatz 1 und 2 kann die oder der Landesbeauftragte für den Datenschutz festgestellte Verstöße gegen Vorschriften über den Datenschutz im Anwendungsbereich der Richtlinie (EU) 2016/680 beanstanden und ihre Behebung in angemessener Frist fordern. Sie oder er kann die Rechts- und Fachaufsichtsbehörde hierüber verständigen. Werden die beanstandeten Verstöße nicht behoben, kann sie oder er von den in Satz 2 genannten Stellen binnen angemessener Frist geeignete Maßnahmen fordern. Nach fruchtlosem Fristablauf kann die oder der Landesbeauftragte für den Datenschutz den Landtag und die Landesregierung verständigen.

(4) Übt die oder der Landesbeauftragte für den Datenschutz für die betroffene Person deren Rechte im Anwendungsbereich der Richtlinie (EU) 2016/680 aus, hat er die Rechtmäßigkeit der Verarbeitung zu überprüfen und die betroffene Person innerhalb einer angemessenen Frist über das Ergebnis dieser Überprüfung zu unterrichten oder ihr die Gründe mitzuteilen, aus denen die Überprüfung nicht vorgenommen werden kann. Hierbei ist die betroffene Person auf die Rechtsschutzmöglichkeiten gegen die oder den Landesbeauftragte für den Datenschutz hinzuweisen. Die Mitteilung an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern dieser nicht einer weitergehenden Auskunft zustimmt. Die oder der Landesbeauftragte für den Datenschutz hat eine bei ihr oder ihm eingelegte Beschwerde über eine Verarbeitung, die in die Zuständigkeit einer Aufsichtsbehörde des Bundes, eines anderen Landes oder in einem anderen Mitgliedstaat der Europäischen Union fällt, unverzüglich an die zuständige Aufsichtsbehörde weiterzuleiten. Sie oder er hat in diesem Fall die betroffene Person über die Weiterleitung zu unterrichten und ihr auf deren Ersuchen weitere Unterstützung zu leisten.

(5) Die Aufsicht durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz im Anwendungsbereich der Richtlinie (EU) 2016/680 erstreckt sich nicht auf eine Datenverarbeitung, die gerichtlich überprüft wurde.

(6) Die oder der Landesbeauftragte für den Datenschutz führt zu den in § 46f Absatz 2 genannten Maßnahmen und zu Datenübermittlungen an Drittstaaten und weitere zwischen- und überstaatliche Stellen nach den §§ 39d bis 39h im Abstand von längstens zwei Jahren zumindest stichprobenartig Kontrollen durch. Dies gilt auch für Datenübermittlungen an Drittstaaten und weitere zwischen- und überstaatliche Stellen nach der Verordnung (EU) 2016/679.

§ 48c
Zusammenarbeit mit der oder dem Landesbeauftragten für den Datenschutz und deren oder dessen Anhörung

(1) Die verantwortliche Stelle und der Auftragsverarbeiter haben mit der oder dem Landesbeauftragten für den Datenschutz bei der Erfüllung ihrer oder seiner Aufgaben zusammenzuarbeiten.

(2) Die verantwortliche Stelle hat vor der Inbetriebnahme von neu anzulegenden automatisierten Verfahren nach § 42 die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz anzuhören, wenn

1. aus einer Datenschutz-Folgenabschätzung nach § 45b hervorgeht, dass die Verarbeitung ein hohes Risiko für die Rechtsgüter betroffener Personen zur Folge hätte, wenn die verantwortliche Stelle keine Abhilfemaßnahmen treffen würde, oder

2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, ein hohes Risiko für die Rechtsgüter betroffener Personen zur Folge hat.

Die oder der Landesbeauftragte für den Datenschutz kann eine Liste der Verarbeitungsvorgänge erstellen, die der Pflicht zur Anhörung nach Satz 1 unterliegen.

(3) Der oder dem Landesbeauftragten für den Datenschutz sind im Fall des Absatzes 2 vorzulegen:

1. die nach § 45b durchgeführte Datenschutz-Folgenabschätzung,
2. gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten der verantwortlichen Stelle, der gemeinsam verantwortlichen Stellen und der an der Verarbeitung beteiligten Auftragsverarbeiter,
3. Angaben zu den Zwecken und Mitteln der beabsichtigten Verarbeitung,
4. Angaben zu den zum Schutz der Rechtsgüter der betroffenen Personen vorgesehenen Maßnahmen und Garantien und
5. Name und Kontaktdaten der oder des behördlichen Datenschutzbeauftragten.

Auf Anforderung sind ihr oder ihm zudem alle sonstigen Informationen zu übermitteln, die sie oder er benötigt, um die Rechtmäßigkeit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Personen bestehenden Gefahren und die diesbezüglichen Garantien bewerten zu können.

(4) Ist die oder der Landesbeauftragte für den Datenschutz der Auffassung, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstoßen würde, insbesondere weil die verantwortliche Stelle das Risiko nicht ausreichend ermittelt oder keine ausreichenden Abhilfemaßnahmen getroffen hat, kann sie oder er der verantwortlichen Stelle und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von sechs Wochen nach Einleitung der Anhörung schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergriffen werden sollten. Erfolgt die geplante Verarbeitung nicht zu Zwecken der Richtlinie (EU) 2016/680, beträgt die Frist acht Wochen. Die oder der Landesbeauftragte für den Datenschutz kann diese Frist im Anwendungsbereich der Richtlinie (EU) 2016/680 um einen Monat, in übrigen Fällen um sechs Wochen verlängern, wenn die geplante Verarbeitung besonders komplex ist. Sie oder er hat in diesem Fall innerhalb eines Monats nach Einleitung der Anhörung die verantwortliche Stelle und gegebenenfalls den Auftragsverarbeiter über die Fristverlängerung zu informieren. Die Fristen können durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz ausgesetzt werden, bis die verantwortliche Stelle ihr oder ihm die zur Anhörung angeforderten Informationen zur Verfügung gestellt hat. Die Ausübung ihrer oder seiner sonstigen Befugnisse nach § 48b bleibt davon unberührt.

(5) Hat die beabsichtigte Verarbeitung zu Zwecken der Richtlinie (EU) 2016/680 erhebliche Bedeutung für die Aufgabenerfüllung der verantwortlichen Stelle und ist sie daher besonders dringlich, kann er mit der Verarbeitung nach Beginn der Anhörung, aber vor Ablauf der in Absatz 4 Satz 1 genannten Frist beginnen. In diesem Fall sind die Empfehlungen der oder des Landesbeauftragten für den Datenschutz im Nachhinein zu berücksichtigen und die Art und Weise der Verarbeitung daraufhin gegebenenfalls anzupassen.

(6) Vor dem Erlass oder der Änderung von Rechts- oder Verwaltungsvorschriften, die das Recht auf informationelle Selbstbestimmung berühren, ist die oder der Landesbeauftragte für den Datenschutz frühestmöglich anzuhören.

§ 48d
Benachrichtigung der oder des Landesbeauftragten für den Datenschutz bei Verletzungen des Schutzes personenbezogener Daten

(1) Die verantwortliche Stelle hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch 72 Stunden nachdem sie ihr bekannt geworden ist, der oder dem Landesbeauftragten für den Datenschutz zu melden, es sei denn, dass die Verletzung voraussichtlich keine Gefahr für die Rechtsgüter natürlicher Personen mit sich gebracht hat. Erfolgt die Meldung an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz nicht innerhalb von 72 Stunden, so ist die Verzögerung ihr oder ihm gegenüber zu begründen.

(2) Ein Auftragsverarbeiter hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich der verantwortlichen Stelle entsprechend den Maßgaben der Absätze 3 und 4 zu melden.

(3) Die Meldung nach Absatz 1 hat zumindest folgende Informationen zu enthalten:

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, die, soweit möglich, Angaben zu den betroffenen Kategorien personenbezogener Daten und Erkenntnisse zur ungefähren Anzahl der betroffenen personenbezogenen Datensätze zu enthalten hat,
2. den Namen und die Kontaktdaten der oder des behördlichen Datenschutzbeauftragten oder einer sonstigen Person oder Stelle, die weitere Informationen erteilen kann,
3. eine Beschreibung der eingetretenen und eine Einschätzung der wahrscheinlichen Folgen der Verletzung und
4. eine Beschreibung der von der verantwortlichen Stelle durchgeführten oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung und der getroffenen Maßnahmen zur Vermeidung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn die Informationen nach Absatz 3 nicht zusammen mit der Meldung übermittelt werden können, hat die verantwortliche Stelle sie unverzüglich nachzureichen, sobald sie ihr vorliegen.

(5) Die verantwortliche Stelle hat Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen.

(6) Soweit von einer Verletzung personenbezogene Daten betroffen sind, die von einer verantwortlichen Stelle in einem anderen Mitgliedstaat der Europäischen Union übermittelt wurden, sind die in Absatz 3 genannten Informationen der dortigen verantwortlichen Stelle unverzüglich zu übermitteln.

(7) Weitere Pflichten der verantwortlichen Stelle zu Benachrichtigungen über Verletzungen des Schutzes personenbezogener Daten bleiben unberührt.

(8) § 46c Absatz 6 gilt entsprechend.

§ 48e
Bestellung behördlicher Datenschutzbeauftragter

(1) Die verantwortliche Stelle bestellt schriftlich eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten sowie eine Vertretung.

(2) Für mehrere Behörden nach Absatz 1 kann unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe eine gemeinsame Datenschutzbeauftragte oder ein gemeinsamer Datenschutzbeauftragter bestellt werden.

(3) Die oder der behördliche Datenschutzbeauftragte wird auf der Grundlage ihrer oder seiner beruflichen Qualifikation und insbesondere ihres oder seines Fachwissens, das sie oder er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage ihrer oder seiner Fähigkeit zur Erfüllung der in § 48g genannten Aufgaben bestellt.

(4) Die oder der behördliche Datenschutzbeauftragte kann Beschäftigte oder Beschäftigter der Stelle nach Absatz 1 oder einer der Stellen nach Absatz 2 sein oder ihre oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

(5) Die Kontaktdaten der oder des behördlichen Datenschutzbeauftragten sind von der Stelle nach Absatz 1 oder den Stellen nach Absatz 2 öffentlich bekannt zu geben und der oder dem Landesbeauftragten für den Datenschutz mitzuteilen.

§ 48f
Stellung der behördlichen Datenschutzbeauftragten

(1) Die verantwortliche Stelle hat
1. sicherzustellen, dass die oder der behördliche Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird,
2. die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben gemäß § 48g zu unterstützen, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung ihres oder seines Fachwissens erforderlichen Ressourcen zur Verfügung stellt und
3. sicherzustellen, dass die oder der behördliche Datenschutzbeauftragte bei der Erfüllung ihrer oder seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält.

Die oder der behördliche Datenschutzbeauftragte berichtet unmittelbar der Leitung der Behörde. Er oder sie darf von der Behörde wegen der Erfüllung ihrer oder seiner Aufgaben nicht abberufen oder benachteiligt werden.

(2) Die Abberufung der oder des behördlichen Datenschutzbeauftragten ist nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuches zulässig. Die Kündigung des Arbeitsverhältnisses ist unzulässig, es sei denn, dass Tatsachen vorliegen, die die Behörde zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach dem Ende der Tätigkeit als behördliche Datenschutzbeauftragte oder als behördlicher Datenschutzbeauftragter ist die Kündigung des Arbeitsverhältnisses innerhalb eines Jahres unzulässig, es sei denn, dass eine Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.

(3) Beschäftigte der verantwortlichen Stelle können sich ohne Einhaltung des Dienstweges in allen Angelegenheiten des Datenschutzes an die für sie zuständige behördliche Datenschutzbeauftragte oder den für sie zuständigen behördlichen Datenschutzbeauftragten wenden. Betroffene Personen können die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß der Verordnung (EU) 2016/679, diesem Gesetz sowie anderen Rechtsvorschriften über den Datenschutz im Zusammenhang stehenden Fragen zu Rate ziehen. Die oder der behördliche Datenschutzbeauftragte ist auch nach Beendigung ihrer oder seiner Tätigkeit zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf die betroffene Person zulassen, verpflichtet, soweit sie oder er nicht davon durch die betroffene Person befreit wird.

(4) Wenn die oder der behördliche Datenschutzbeauftragte bei ihrer oder seiner Tätigkeit Kenntnis von Daten erhält, für die der Leitung oder einer bei der in Absatz 1 genannten Behörden beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch der oder dem behördlichen Datenschutzbeauftragten und den ihr oder ihm unterstellten Beschäftigten zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht der oder des behördlichen Datenschutzbeauftragten reicht, unterliegen ihre oder seine Akten und andere Dokumente einem Beschlagnahmeverbot.

§ 48g
Aufgaben der behördlichen Datenschutzbeauftragten

(1) Der oder dem behördlichen Datenschutzbeauftragten obliegen neben den in der Verordnung (EU) 2016/679 genannten Aufgaben zumindest folgende Aufgaben:

1. Unterrichtung und Beratung der Behörde und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften;

2. Überwachung der Einhaltung der Vorschriften dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, sowie der Strategien der Behörde für den Schutz personenbezogener Daten, einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und der Schulung der an den Verarbeitungsvorgängen beteiligten Beschäftigten und der diesbezüglichen Überprüfungen;

3. Entscheidung nach § 26a Absatz 5 sowie Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung nach § 45b und Überwachung ihrer Durchführung;

4. Zusammenarbeit mit der oder dem Landesbeauftragten für den Datenschutz;

5. Tätigkeit als Anlaufstelle für die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation nach § 48c, und gegebenenfalls Beratung zu allen sonstigen Fragen.

(2) Die oder der behördliche Datenschutzbeauftragte hat ein Recht auf Einsichtnahme in das Verzeichnis aller Verarbeitungstätigkeiten. Vor erstmaliger Inbetriebnahme einer Verarbeitungstätigkeit ist der oder dem behördlichen Datenschutzbeauftragten das Verzeichnis mit der Gelegenheit zur Stellungnahme zu dem entsprechenden Eintrag vorzulegen.

(3) Die oder der behördliche Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Die Behörde hat dafür Sorge zu tragen, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen und der oder dem behördlichen Datenschutzbeauftragten für ihre oder seine Aufgaben nach Absatz 1 hinreichend Arbeitszeit verbleibt.

(4) Die oder der behördliche Datenschutzbeauftragte trägt bei der Erfüllung ihrer oder seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei sie oder er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

§ 48h
Parlamentarische Kontrolle, Unterrichtung der Öffentlichkeit

(1) Das Ministerium für Inneres und Europa berichtet einem Gremium des Landtages (SOG-Gremium) über folgende durchgeführte Maßnahmen:

1. Einsatz besonderer Mittel der Datenerhebung nach § 33 Absatz 1,
2. Einsatz technischer Mittel in Wohnungen nach § 33b; soweit die Maßnahme nach § 33b Absatz 9 als Personenschutzmaßnahme erfolgt ist nur, wenn die erhobenen Daten gemäß § 36 weiterverarbeitet wurden,
3. verdeckter Zugriff auf informationstechnische Systeme nach § 33c,
4. Eingriffen in den Telekommunikationsbereich nach den §§ 33d bis 33g,
5. Rasterfahndung nach § 44,
6. elektronische Aufenthaltsüberwachung nach § 67a und
7. Datenübermittlung an Drittstaaten und weitere zwischen- und überstaatliche Stellen nach den §§ 39d bis 39h und nach der Verordnung (EU) 2016/679.

Der Bericht bezieht sich auf ein Kalenderjahr und ist bis zum 31. Dezember des darauf folgenden Jahres abzugeben. Im Bericht ist darzustellen, in welchem Umfang von den Befugnissen aus Anlass welcher Art von Gefahrenlagen Gebrauch gemacht wurde und in welchem Umfang die Benachrichtigung der betroffenen Personen erfolgt ist.

Das Justizministerium berichtet unter Beachtung von Satz 2 dem SOG-Gremium entsprechend § 101b Absatz 4 der Strafprozessordnung über die durchgeführten Maßnahmen nach § 100c der Strafprozessordnung, die von einem Gericht in Mecklenburg-Vorpommern angeordnet worden sind.

(2) Das SOG-Gremium besteht aus fünf Mitgliedern und wird vom Landtag gewählt. Die Zusammensetzung regelt sich nach dem Stärkeverhältnis der Fraktionen. Das Gremium gibt sich eine Geschäftsordnung.

(3) Die Landesregierung unterrichtet auf der Grundlage des Berichts nach Absatz 1 den Landtag über die Anzahl der Maßnahmen nach Absatz 1 Satz 1 und Satz 3 und in welchem Umfang eine Benachrichtigung erfolgt ist.

(4) Das Ministerium für Inneres und Europa und das Justizministerium veröffentlichen nach Unterrichtung des Landtages zur Information der Öffentlichkeit die erfolgte Unterrichtung an den Landtag auf ihrer Internetseite.

(5) Das Ministerium für Inneres und Europa regelt das Nähere Verfahren zur Erfüllung der Berichtspflichten nach Absatz 1 Satz 1 durch Verwaltungsvorschrift.

Unterabschnitt 7
Straftaten von erheblicher Bedeutung (§ 49)

§ 49
Straftaten von erheblicher Bedeutung

Straftaten von erheblicher Bedeutung im Sinne dieses Gesetzes sind
1. Verbrechen,
2. Vergehen nach den §§ 86, 86a, 89a, 89b, 89c Absatz 1 bis 4, 91, 95, 129, 129a, 129b, 130, 184b Absatz 1 und 2, 184c Absatz 2, 303b Absatz 4, 310 Absatz 1 Nummer 2 des Strafgesetzbuches und
3. banden-, gewerbs-, serienmäßig oder sonst organisiert begangene Vergehen nach
   a) den §§ 125a, 180a, 181a, 224, 243, 244, 260, 261, 263 bis 264a, 265b, 266, 267, 283, 283a und 324 bis 330 des Strafgesetzbuches,
   b) § 52 Absatz 1 Nummer 2 Buchstabe c und d des Waffengesetzes,
   c) § 29 Absatz 3 Satz 2 Nummer 1 des Betäubungsmittelgesetzes,
   d) den §§ 95 Absatz 2 und 96 Absatz 2 des Aufenthaltsgesetzes.

Abschnitt 4
Besondere Maßnahmen (§§ 49a - 67d)

§ 49a
Grundsatz

Soweit personenbezogene Daten nach Abschnitt 4 verarbeitet werden und nichts Abweichendes geregelt ist, sind die Vorschriften des Abschnittes 3 anzuwenden.

Unterabschnitt 1
Besondere Maßnahmen der Polizei und der Ordnungsbehörden (§§ 50 - 67)

§ 50
Vorladung

(1) Eine Person kann schriftlich oder mündlich vorgeladen werden, wenn
1. Tatsachen die Annahme rechtfertigen, dass die Person sachdienliche Angaben machen kann, die für die Erfüllung einer bestimmten Aufgabe der Ordnungsbehörden oder der Polizei erforderlich sind, oder
2. dies zur Durchführung einer gesetzlich zugelassenen erkennungsdienstlichen Maßnahme erforderlich ist.

(2) Bei der Vorladung soll deren Grund angegeben werden. Bei der Festsetzung des Zeitpunktes soll auf den Beruf und die sonstigen Lebensverhältnisse der oder des Vorgeladenen Rücksicht genommen werden.

(3) Wird der Vorladung ohne hinreichenden Grund keine Folge geleistet, so kann sie zwangsweise durchgesetzt werden,
1. wenn die Angaben zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich sind oder
2. wenn erkennungsdienstliche Maßnahmen durchgeführt werden sollen.

(4) § 136a der Strafprozessordnung gilt mit Ausnahme seines Absatzes 1 Satz 2 entsprechend.

(5) Maßnahmen nach Absatz 3 im Wege des unmittelbaren Zwanges dürfen nur Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte vornehmen.

(6) Für die Entschädigung von Personen, die auf Vorladung als Zeuginnen und Zeugen erscheinen oder die als Sachverständige oder Dolmetscherinnen und Dolmetscher herangezogen werden, gilt das Justizvergütungs- und -entschädigungsgesetz entsprechend.

§ 51
Verfahren bei der Vorführung

(1) Kommt eine Person der gesetzlichen Verpflichtung, vor einer Behörde zu erscheinen, auf Vorladung nicht nach, so kann sie vorgeführt werden, wenn hierauf in der Vorladung hingewiesen worden ist. Unter der gleichen Voraussetzung kann eine Person vorgeführt werden, wenn sie aufgrund gesetzlicher Vorschrift einer Behörde vorzustellen ist, die Vorstellung aber unterblieben ist.

(2) Die vorgeführte Person darf nicht länger als bis zum Ende der Amtshandlung, zu der sie vorgeladen war, festgehalten werden. Spätestens am Ende des Tages nach der Vorführung ist sie zu entlassen.

(3) § 56 gilt entsprechend.

§ 52
Platzverweisung und Wegweisung

(1) Zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr ist es zulässig, eine Person vorübergehend von einem Ort zu verweisen oder ihr vorübergehend das Betreten eines Ortes zu verbieten. Die Platzverweisung kann auch gegen Personen angeordnet werden, die den Einsatz der Feuerwehr oder von Hilfs- oder Rettungsdiensten behindern.

(2) Die Polizei kann eine Person ihrer Wohnung und des unmittelbar angrenzenden Bereichs verweisen, wenn dies erforderlich ist, um eine gegenwärtige Gefahr für Leib, Leben oder Freiheit von Bewohnerinnen oder Bewohnern derselben Wohnung (gefährdete Personen) abzuwenden. Unter den gleichen Voraussetzungen kann die Einsatzleitung ein Betretungsverbot anordnen. Sie informiert unverzüglich die Leitung der zuständigen Polizeibehörde über die Anordnung; § 52a Absatz 3 gilt entsprechend und Widerspruch und Anfechtungsklage gegen die Anordnung haben keine aufschiebende Wirkung. Die Maßnahme darf die Dauer von 14 Tagen nicht überschreiten. Ergänzend können Maßnahmen zur Durchsetzung der Wegweisung oder des Betretungsverbotes verfügt werden. Im Falle eines Antrags auf zivilrechtlichen Schutz nach dem Gewaltschutzgesetz mit dem Ziel des Erlasses einer einstweiligen Anordnung endet die nach Satz 1 oder 2 verfügte polizeiliche Maßnahme bereits mit dem Tag der Wirksamkeit der gerichtlichen Entscheidung. Das Gericht informiert unverzüglich die örtlich zuständige Polizeidienststelle über seine Entscheidung.

(3) Im Falle einer Wegweisung oder eines angeordneten Betretungsverbots nach Absatz 2 darf die Polizei die für eine Kontaktaufnahme erforderlichen personenbezogenen Daten der gefährdeten Personen an die zuständige vom Ministerium für Soziales, Integration und Gleichstellung anerkannte Interventionsstelle übermitteln. Dies gilt nicht, wenn ausschließlich gefährdete Personen betroffen sind, die das 18. Lebensjahr noch nicht vollendet haben. Die Interventionsstelle darf die übermittelten personenbezogenen Daten ausschließlich dazu verwenden, den gefährdeten Personen unverzüglich Beratung zum Schutz ihrer Rechtsgüter anzubieten. Lehnt eine gefährdete Person die Beratung ab, hat die Interventionsstelle die übermittelten Daten unverzüglich zu löschen. Im Übrigen sind die übermittelten Daten nach Abschluss der Beratungstätigkeit zu löschen.

§ 52a
Aufenthalts- und Betretungsverbot

(1) Rechtfertigen Tatsachen die Annahme, dass eine Person in einem bestimmten örtlichen Bereich eine Straftat, die keine terroristische Straftat nach § 67c ist, begehen wird, können Ordnungsbehörden und Polizei ihr untersagen, diesen Bereich zu betreten oder sich dort aufzuhalten. Örtlicher Bereich im Sinne des Satzes 1 ist ein Ort oder ein Gebiet innerhalb einer Gemeinde oder auch ein gesamtes Gemeindegebiet.

(2) Maßnahmen nach Absatz 1 dürfen nur durch die Leitung der zuständigen Ordnungs- oder Polizeibehörde oder bei polizeilicher Anordnung auch durch die von ihr besonders beauftragte Beamtin oder den von ihr besonders beauftragten Beamten angeordnet werden. Widerspruch und Anfechtungsklage gegen die Anordnung haben keine aufschiebende Wirkung.

(3) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, mit Namen und Anschrift,
2. Art, Umfang und Dauer der Maßnahme, einschließlich einer Bezeichnung der örtlichen Bereiche, die die Person nicht betreten oder in denen sich die Person nicht aufhalten darf, sowie
3. die Gründe.

(4) Das Verbot ist zeitlich und örtlich auf den zur Verhütung der Straftat erforderlichen Umfang zu beschränken und darf räumlich nicht den Zugang zur Wohnung der betroffenen Person umfassen. Die Vorschriften des Versammlungsrechts bleiben unberührt.

(5) Das Verbot ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist möglich, soweit die Voraussetzungen fortbestehen. Eine Verlängerung bedarf der gerichtlichen Anordnung nach Maßgabe des Absatzes 3 auf Antrag der Leitung der zuständigen Ordnungs- oder Polizeibehörde; der Antrag muss die Angaben nach Absatz 3 Satz 2 Nummer 1 und 2 sowie den Sachverhalt und eine Begründung enthalten.

(6) Die jeweils örtlich zuständigen Ordnungs- und Polizeibehörden unterrichten sich gegenseitig unverzüglich über ein nach dieser Vorschrift angeordnetes Aufenthalts- und Betretungsverbot.

§ 52b
Meldeauflage

(1) Rechtfertigen Tatsachen die Annahme, dass eine Person eine Straftat begehen wird, kann sie durch die Polizei verpflichtet werden, an bestimmten Tagen zu bestimmten Zeiten in einer bestimmten Polizeidienststelle zu erscheinen (Meldeauflage). Gleiches gilt, wenn die Voraussetzungen des § 67a Absatz 1 vorliegen. Soweit der Zweck der Meldeauflage oder anderer im Zusammenhang mit der Anordnung stehenden Maßnahmen nicht gefährdet wird, kann mit Zustimmung der betroffenen Person auch eine inländische Polizeidienststelle außerhalb ihres Wohnsitzes oder ständigen Aufenthaltsortes bestimmt werden.

(2) Maßnahmen nach Absatz 1 Satz 1 dürfen nur durch die Leitung der zuständigen Polizeibehörde oder durch eine von ihr besonders beauftragte Beamtin oder einen von ihr besonders beauftragten Beamten angeordnet werden. Maßnahmen nach Absatz 1 Satz 2 darf nur die Leitung der zuständigen Polizeibehörde anordnen. Widerspruch und Anfechtungsklage gegen die Anordnung haben keine aufschiebende Wirkung.

(3) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, mit Namen und Anschrift,
2. Art, Umfang und Dauer der Maßnahme, einschließlich der Polizeidienststelle, bei der sich die Person zu melden hat, sowie
3. die Gründe.

(4) Die Meldeauflage ist zeitlich und örtlich auf den zur Verhütung der Straftat erforderlichen Umfang zu beschränken und darf unter Berücksichtigung der Art und Schwere der zu verhütenden Straftat keine unzumutbaren Auswirkungen auf die Lebensführung der betroffenen Person haben. Die Vorschriften des Versammlungsrechts bleiben unberührt.

(5) Das Gebot ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist möglich, soweit die Voraussetzungen fortbestehen. Eine Verlängerung bedarf der gerichtlichen Anordnung nach Maßgabe des Absatzes 3 auf Antrag der Leitung der zuständigen Polizeibehörde; der Antrag muss die Angaben nach Absatz 3 Satz 2 Nummer 1 und 2 sowie den Sachverhalt und eine Begründung enthalten.

(6) Eine nach Absatz 1 Satz 2 angeordnete Meldeauflage geht der nach Absatz 1 Satz 1 angeordneten Meldeauflage vor, soweit sie sich entgegenstehen. Gleiches gilt in Bezug auf ein nach § 52a angeordnetes Aufenthalts- und Betretungsverbots.

§ 53
Durchsuchung von Personen und Verfahren

(1) Eine Person kann außer in den Fällen des § 29 Absatz 3 Satz 2 nur durchsucht werden, wenn
1. tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person Sachen bei sich führt, die sichergestellt werden können,
2. sie nach diesem Gesetz oder anderen Rechtsvorschriften angehalten oder festgehalten werden kann und die Durchsuchung
   a) zum Schutz der Person oder
   b) zur Eigensicherung des Amtsträgers
   erforderlich ist oder
3. eine Identitätsfeststellung aufgrund des § 29 Absatz 1 Satz 2 Nummer 1, 2 oder 3 zulässig ist.

(2) Die Person kann zum Zwecke der Durchsuchung zur Dienststelle verbracht werden, wenn es sonst nicht möglich ist, die Durchsuchung ordnungsgemäß durchzuführen.

(3) Maßnahmen nach Absatz 1 und 2 dürfen nur Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte anordnen.

(4) Bei der Durchsuchung einer Person können der Körper, die Kleidung, der Inhalt der Kleidung und die sonstigen am Körper getragenen Sachen durchsucht werden.

(5) Personen dürfen nur von Personen gleichen Geschlechts oder von Ärztinnen oder Ärzten durchsucht werden. Bei berechtigtem Interesse soll dem Wunsch der zu durchsuchenden Person, die Durchsuchung einer Person oder einer Ärztin oder einem Arzt bestimmten Geschlechts zu übertragen, entsprochen werden; hierauf ist sie hinzuweisen. Satz 1 und 2 gelten nicht, wenn die sofortige Durchsuchung zum Schutz gegen eine im einzelnen Falle bevorstehende Gefahr für Leib oder Leben erforderlich ist.

§ 54
Untersuchung von Personen und Verfahren

(1) Bei einer lebenden oder verstorbenen Person, von der sich ergibt oder anzunehmen ist, dass sie krank, krankheitsverdächtig, ansteckungsverdächtig ist oder war, können körperliche Untersuchungen, Entnahmen von Blutproben und andere körperliche Eingriffe zur Feststellung des Infektionsstatus angeordnet werden, wenn Tatsachen die Annahme rechtfertigen, dass es zu einer Übertragung von Krankheitserregern, wie insbesondere Hepatitis B, Hepatitis C oder Humanes Immundefizienzvirus (HIV) auf eine andere Person gekommen ist und bei dieser Person dadurch eine Gefahr für das Leben oder eine schwerwiegende Gesundheitsgefährdung besteht und die Kenntnis des Infektionsstatus zur Abwehr der Gefahr erforderlich ist. Körperliche Untersuchungen und Eingriffe dürfen nur von einer Ärztin oder einem Arzt nach den Regeln der ärztlichen Kunst durchgeführt werden; § 53 Absatz 5 Satz 2 und 3 gelten insoweit entsprechend. Vor einer Blutentnahme soll eine ärztliche Konsultation erfolgen. Körperliche Untersuchungen und Eingriffe sind ohne Einwilligung der betroffenen Person zulässig, wenn kein Nachteil für ihre Gesundheit zu befürchten ist.

(2) Die Maßnahme bedarf, außer in Fällen von Gefahr im Verzug, der richterlichen Anordnung auf Antrag der Leitung der zuständigen Polizeibehörde oder einer von ihr besonders beauftragten Beamtin oder eines von ihr besonders beauftragten Beamten. Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. Art und Umfang der Maßnahme,
3. der Sachverhalt sowie
4. eine Begründung.

Im Falle einer Anordnung durch die Polizei bei Gefahr im Verzug gilt § 25b entsprechend. Die richterliche Entscheidung ist unverzüglich nachzuholen.

(3) Die Anordnung ergeht schriftlich, in Fällen von Gefahr im Verzug ist sie unverzüglich nachträglich zu dokumentieren. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. Art und Umfang der Maßnahme sowie
3. die Gründe.

(4) Die bei der Untersuchung erhobenen personenbezogenen Daten dürfen über den Zweck dieses Gesetzes hinaus nur zum Schutz vor oder zur Abwehr von schwerwiegenden Gesundheitsgefährdungen verarbeitet werden.

§ 55
Gewahrsam von Personen

(1) Eine Person kann nur in Gewahrsam genommen werden, wenn dies

1. zu ihrem Schutz gegen eine im einzelnen Falle bevorstehende Gefahr für Leib oder Leben erforderlich ist, insbesondere, weil sie sich erkennbar in einem die freie Willensbestimmung ausschließenden Zustand oder sonst in hilfloser Lage befindet,
2. unerlässlich ist, um die unmittelbar bevorstehende Begehung oder Fortsetzung einer Straftat zu verhindern; die Annahme, dass eine Person eine solche Tat begehen oder zu ihrer Begehung beitragen wird, kann sich insbesondere darauf stützen, dass
   a) sie die Begehung der Tat angekündigt oder dazu aufgefordert hat oder Transparente oder sonstige Gegenstände mit einer solchen Aufforderung mit sich führt; dies gilt auch für Flugblätter solchen Inhalts, soweit sie in einer Menge mitgeführt werden, die zur Verteilung geeignet ist,
   b) bei ihr Waffen, Werkzeuge oder sonstige Gegenstände aufgefunden werden, die ersichtlich zur Tatbegehung bestimmt sind oder erfahrungsgemäß bei derartigen Taten verwendet werden oder ihre Begleitperson solche Gegenstände mit sich führt und sie den Umständen nach hiervon Kenntnis haben musste, oder
   c) sie bereits in der Vergangenheit aus vergleichbarem Anlass bei der Begehung von Straftaten als Störer angetroffen worden ist und Tatsachen die Annahme rechtfertigen, dass eine Wiederholung dieser Verhaltensweise zu erwarten ist,
3. unerlässlich ist, um eine gegenwärtige Gefahr für die öffentliche Sicherheit oder Ordnung abzuwehren,
4. unerlässlich ist, um private Rechte zu schützen und eine Festnahme und Vorführung der Person nach den §§ 229 und 230 Absatz 3 des Bürgerlichen Gesetzbuches zulässig ist, oder
5. unerlässlich ist, um eine Maßnahme nach den §§ 52, 52a, 52b, 67a oder 67b durchzusetzen.

(2) Minderjährige, die sich der Obhut der Sorgeberechtigten entzogen haben, können in Gewahrsam genommen werden, um sie den Sorgeberechtigten oder dem Jugendamt zuzuführen. Satz 1 gilt sinngemäß für unter Betreuung stehende Personen.

(3) Eine Person, die aus dem Vollzug von Untersuchungshaft, Freiheitsstrafen, Jugendstrafen oder freiheitsentziehenden Maßregeln der Besserung und Sicherung entwichen ist oder sich sonst ohne Erlaubnis außerhalb der Justizvollzugsanstalt, Jugendanstalt, Jugendarrestanstalt oder einer Anstalt nach den §§ 63, 64 oder 66 des Strafgesetzbuches aufhält, kann in Gewahrsam genommen und in die Anstalt zurückgebracht werden.

(4) Maßnahmen nach den Absätzen 1 bis 3 dürfen nur Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte vornehmen.

(5) Der Gewahrsam ist unverzüglich aufzuheben, sobald der Grund weggefallen oder der Zweck erreicht ist. Der Gewahrsam ist spätestens am Ende des Tages nach der Übernahme in den Gewahrsam aufzuheben, sofern nicht vorher die Fortdauer der Freiheitsentziehung gerichtlich angeordnet worden ist.

§ 56
Verfahren bei amtlichem Gewahrsam

(1) Wird eine Person in Gewahrsam, Verwahrung oder Haft genommen oder untergebracht (amtlicher Gewahrsam), so sind ihr unverzüglich der Grund der Maßnahme und die zulässigen Rechtsbehelfe bekanntzugeben, es sei denn, die Bekanntgabe wirkt sich für die Person nachteilig aus.

(2) Einer in Gewahrsam genommenen Person ist unverzüglich Gelegenheit zu geben, eine oder einen Angehörigen oder eine Person ihres Vertrauens zu benachrichtigen. Ist die betroffene Person nicht in der Lage, von diesem Recht Gebrauch zu machen, so soll die Behörde selbst die Benachrichtigung einer oder eines Angehörigen übernehmen. Ist die betroffene Person minderjährig, so ist in jedem Falle diejenige Person unverzüglich zu benachrichtigen, der die Sorge für die betroffene Person obliegt; ist für die betroffene Person eine Betreuerin oder ein Betreuer bestellt, so ist diese oder dieser zu benachrichtigen. Satz 1 und 2 gelten nicht, soweit der Zweck des Gewahrsams dadurch gefährdet wird.

(3) Die Person soll nicht in einem Raum mit Strafgefangenen, Untersuchungsgefangenen oder Suchtkranken verwahrt werden. Die Unterbringung soll getrennt nach Geschlechtern erfolgen; findet der Gewahrsam in Gewahrsamsräumen statt, hat sie getrennt zu erfolgen.

(4) Der Person dürfen nur solche Beschränkungen auferlegt werden, die zur Sicherung des Zwecks oder zur Aufrechterhaltung der Ordnung des amtlichen Gewahrsams notwendig sind.

(5) Nimmt die Polizei eine Person in Gewahrsam, so hat sie unter Angabe der betroffenen Person, mit deren Namen und deren Anschrift, der beabsichtigten Gewahrsamsdauer, des Sachverhalts und der Begründung unverzüglich eine richterliche Entscheidung über die Zulässigkeit und Fortdauer des Gewahrsams herbeizuführen. Der Herbeiführung der Entscheidung bedarf es nicht, wenn anzunehmen ist, dass die Entscheidung erst nach Wegfall des Grundes des Gewahrsams ergehen würde. Die richterliche Entscheidung ergeht schriftlich und in ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. Art und höchstzulässige Dauer des Gewahrsams; der Gewahrsam darf im Falle des § 55 Absatz 1 Nummer 2 zehn Tage und in den übrigen Fällen drei Tage nicht überschreiten, soweit gesetzlich nichts anderes bestimmt ist, sowie
3. die Gründe.

Für die Entscheidung ist das Amtsgericht zuständig, in dessen Bezirk der Gewahrsam vollzogen wird. Für das Verfahren gelten die Vorschriften über das Verfahren in Freiheitsentziehungssachen nach dem Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Die richterliche Entscheidung kann ohne persönliche Anhörung der in Gewahrsam genommenen Person ergehen, wenn diese rauschbedingt nicht in der Lage ist, den Gegenstand der persönlichen Anhörung durch das Gericht ausreichend zu erfassen und in der Anhörung zur Feststellung der entscheidungserheblichen Tatsachen beizutragen. In diesen Fällen wird die richterliche Entscheidung mit Erlass wirksam und bedarf hierzu nicht der Bekanntgabe an die in Gewahrsam genommene Person.

Dauert die Freiheitsentziehung länger als bis zum Ende des Tages nach dem Ergreifen, ist in den Fällen des Satzes 6 unverzüglich eine erneute richterliche Entscheidung herbeizuführen. Ist eine Anhörung hierbei nicht möglich, hat sich das Gericht einen persönlichen Eindruck von der in Gewahrsam genommenen Person zu verschaffen. Für die Gerichtskosten gelten, soweit nichts anderes bestimmt ist, die Vorschriften über die Kostenerhebung in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.

(6) Wird der Gewahrsam nach § 55 Absatz 1 im Wege der Amtshilfe in der nach dem Vollstreckungsplan für das Land Mecklenburg-Vorpommern zuständigen Justizvollzugsanstalt vollzogen, gelten die §§ 171, 173 bis 175 und 178 Absatz 3 des Strafvollzugsgesetzes entsprechend.

§ 57
Durchsuchung von Sachen

(1) Sachen können außer in den Fällen des § 29 Absatz 3 Satz 2, § 33c Absatz 5, § 33d Absatz 3 Satz 3 und des § 35 Absatz 2 Satz 2 Nummer 2 nur durchsucht werden, wenn
1. eine Person sie mitführt, die nach § 53 durchsucht werden darf,
2. tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass sich darin eine andere Sache befindet, die sichergestellt werden kann,
3. tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass sich darin eine Person befindet, die
   a) in Gewahrsam genommen werden darf,
   b) widerrechtlich festgehalten wird oder
   c) hilflos ist,
4. sie sich an einem der in § 29 Absatz 1 Satz 2 Nummer 1 genannten Orte befinden,
5. sie sich in einem Objekt im Sinne des § 29 Absatz 1 Satz 2 Nummer 2 oder 3 oder in dessen unmittelbarer Nähe befinden und tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Straftaten in oder an diesem Objekt begangen werden sollen, oder
6. es sich um ein Land-, Wasser- oder Luftfahrzeug handelt, in dem sich eine Person befindet, deren Identität nach § 29 festgestellt werden darf; die Durchsuchung kann sich auch auf die in dem Fahrzeug enthaltenen Sachen erstrecken.

(2) Betrifft die Durchsuchung ein elektronisches Speichermedium, können auch vom Durchsuchungsobjekt räumlich getrennte Speichermedien durchsucht werden, soweit von diesem aus auf sie zugegriffen werden kann und wenn die Erfüllung der Aufgabe nach diesem Gesetz auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Maßnahme darf auch durchgeführt werden, wenn Dritte (§ 3 Absatz 4 Nummer 2) unvermeidbar betroffen sind. Personenbezogene Daten dürfen darüberhinausgehend nur dann weiterverarbeitet werden, wenn dies gesetzlich zugelassen ist.

§ 58
Verfahren bei der Durchsuchung von Sachen

(1) Bei der Durchsuchung von Sachen vor Ort hat die Gewahrsamsinhaberin oder der Gewahrsamsinhaber das Recht, anwesend zu sein. Ist sie oder er abwesend und eine Vertreterin oder ein Vertreter oder eine Zeugin oder ein Zeuge anwesend, so sollen diese hinzugezogen werden.

(2) Der Gewahrsamsinhaberin oder dem Gewahrsamsinhaber ist eine Bescheinigung über die Durchsuchung und ihren Grund zu erteilen; dies im Falle ihrer oder seiner Anwesenheit jedoch nur auf Verlangen.

§ 59
Betreten und Durchsuchung von Räumen

(1) Das Betreten von Wohn- und Geschäftsräumen oder eines befriedeten Besitztums ist gegen den Willen der Inhaberin oder des Inhabers nur zulässig, wenn dies zur Verhütung einer erheblichen Gefahr für die öffentliche Sicherheit oder Ordnung erforderlich ist.

(2) Arbeits-, Betriebs- und Geschäftsräume sowie andere Räume und Grundstücke, die der Öffentlichkeit zugänglich sind, dürfen zum Zwecke der Gefahrenabwehr während der Arbeits-, Geschäfts- oder Aufenthaltszeit betreten werden.

(3) Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte dürfen Wohn- und Geschäftsräume oder ein befriedetes Besitztum nur durchsuchen, wenn
1. tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass sich darin eine Person befindet, die nach § 51 vorgeführt oder nach einer Rechtsvorschrift in Gewahrsam genommen werden darf,
2. tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass sich darin Sachen befinden, die nach § 61 Absatz 1 Satz 1 Nummer 1 sichergestellt werden dürfen, oder
3. dies zur Abwehr einer gegenwärtigen erheblichen Gefahr erforderlich ist.

(4) Während der Nachtzeit, welche die Stunden von 21 bis 6 Uhr umfasst, sind das Betreten und die Durchsuchung durch Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte nur zur Abwehr einer gegenwärtigen erheblichen Gefahr zulässig. Dies gilt nicht für das Betreten von Räumen,
1. die zur Nachtzeit jeder Person zugänglich sind,
2. wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass
   a) dort Personen Straftaten verabreden, vorbereiten oder verüben,
   b) sich dort Personen treffen, die gegen aufenthaltsrechtliche Vorschriften verstoßen,
   c) sich dort gesuchte Straftäter verbergen oder
   d) dort Personen dem unerlaubten Glücksspiel nachgehen, oder
3. die der Prostitution dienen.

(5) Durchsuchungen von Wohn- und Geschäftsräumen bedürfen, außer in den Fällen von Gefahr im Verzug, der richterlichen Anordnung auf Antrag der Leitung der zuständigen Polizeibehörde oder der von ihr besonders beauftragten Beamtin oder des von ihr besonders beauftragten Beamten. Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. die zu durchsuchenden Räume und deren Anschrift,
3. der Sachverhalt sowie
4. eine Begründung.

Im Falle einer Anordnung durch die Polizei bei Gefahr im Verzug gilt § 25b entsprechend. Die richterliche Entscheidung ist unverzüglich nachzuholen.

(6) Die Anordnung ergeht schriftlich; in Fällen von Gefahr im Verzug ist sie unverzüglich nachträglich zu dokumentieren. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. die zu durchsuchenden Räume und deren Anschrift sowie
3. die Gründe.

Für die Anordnung ist das Amtsgericht, in dessen Bezirk die zu durchsuchenden Räume liegen, zuständig.

§ 60
Verfahren bei der Durchsuchung von Räumen

(1) Bei der Durchsuchung der Wohnung, der Geschäftsräume oder des befriedeten Besitztums hat die Inhaberin oder der Inhaber das Recht, anwesend zu sein. Ist sie oder er nicht anwesend, so soll eine Vertreterin oder ein Vertreter oder eine Zeugin oder ein Zeuge hinzugezogen werden.

(2) Der Inhaberin oder dem Inhaber oder ihrem oder seinem Vertreter ist vor Beginn der Durchsuchung der Grund der Maßnahme bekanntzugeben. Auf die zulässigen Rechtsbehelfe ist hinzuweisen.

(3) Über die Durchsuchung ist eine Niederschrift zu fertigen, in der die für die Durchführung verantwortliche Behörde, Anlass, Zeit und Ort der Durchsuchung und die anwesenden Personen namentlich aufzuführen sind. Die Niederschrift ist von den durchsuchenden Vollzugsbeamtinnen oder Vollzugsbeamten und der Inhaberin oder dem Inhaber des durchsuchten Raumes, ihrer oder seiner Vertreterin oder ihrem oder seinem Vertreter oder den hinzugezogenen Zeuginnen oder Zeugen zu unterschreiben. Wird die Unterschrift verweigert, so ist hierüber ein Vermerk aufzunehmen. Der Inhaberin oder dem Inhaber und ihrer oder seiner Vertreterin oder ihrem oder seinem Vertreter ist auf Verlangen eine Abschrift der Niederschrift auszuhändigen.

(4) Ist die Anfertigung der Niederschrift oder die Aushändigung ihrer Abschrift unter den vorherrschenden Umständen nicht möglich oder würde sie den Zweck der Durchsuchung gefährden, so sind der Inhaberin oder dem Inhaber oder ihrer oder seiner Vertreterin oder ihrem oder seinem Vertreter lediglich die Vornahme der Durchsuchung unter Angabe der für die Durchsuchung verantwortlichen Behörde sowie Zeit und Ort der Durchsuchung schriftlich zu bestätigen.

(5) Die nach § 291 der Abgabenordnung für die Vornahme einer Vollstreckungshandlung zur Beitreibung einer Geldforderung erforderliche Niederschrift ersetzt die Niederschrift nach dieser Bestimmung.

§ 61
Sicherstellung von Sachen

(1) Eine Sache kann nur sichergestellt werden,
1. um eine gegenwärtige Gefahr für die öffentliche Sicherheit oder Ordnung abzuwehren,
2. wenn sie von einer Person mitgeführt wird, die nach diesem Gesetz oder anderen Rechtsvorschriften festgehalten wird, und die Sache verwendet werden kann, um
   a) sich zu töten oder zu verletzen,
   b) Leben oder Gesundheit anderer zu schädigen,
   c) fremde Sachen zu beschädigen oder
   d) die Flucht zu ermöglichen oder zu erleichtern,
3. um die Eigentümerin oder den Eigentümer oder die rechtmäßige Inhaberin oder den rechtmäßigen Inhaber der tatsächlichen Gewalt vor Verlust oder Beschädigung einer Sache zu schützen oder
4. wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass sie zur Begehung einer Straftat oder Ordnungswidrigkeit verwendet werden soll.

Satz 1 gilt auch für Daten auf einem elektronischen Speichermedium und für Daten, auf von diesem räumlich getrennten Speichermedien, soweit auf sie vom elektronischen Speichermedium aus zugegriffen werden kann. Der weitere Zugriff auf diese Daten kann ausgeschlossen werden, wenn andernfalls die Abwehr der Gefahr, der Schutz vor Verlust oder die Verhinderung der Verwendung aussichtslos oder wesentlich erschwert wäre. Die sicherstellende Behörde hat die richterliche Bestätigung der Rechtmäßigkeit der Maßnahmen nach Satz 2 und 3 unverzüglich zu beantragen; im Übrigen gilt § 25b entsprechend. Daten, die nach den §§ 26a und 26b nicht weiter verarbeitet werden dürfen oder für die Aufgabenerfüllung nicht mehr erforderlich sind, sind zu löschen; dies gilt nicht für Daten, die zusammen mit dem Datenträger sichergestellt wurden, auf dem sie gespeichert sind. Die Regelungen in Absatz 3 sowie in den §§ 62, 63, 64 Absatz 4 hinsichtlich der Herausgabe, des Verfahrens, der Verwahrung und der Vernichtung gelten unter Berücksichtigung der unkörperlichen Natur von Daten entsprechend.

(2) Die Polizei kann Forderungen oder andere Vermögensrechte bis zu einer Dauer von sechs Monaten sicherstellen, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass diese zur Begehung einer Straftat von erheblicher Bedeutung nach § 49 oder einer terroristischen Straftat nach § 67c verwendet werden sollen. Die Sicherstellung wird auf Antrag der Leitung der Polizeibehörde durch Pfändung durch das Amtsgericht, in dessen Bezirk die Inhaberin oder der Inhaber der Forderung oder Vermögensrechte ihren oder seinen Wohnsitz oder ständigen Aufenthalt hat, bewirkt. Die Vorschriften der Zivilprozessordnung über die Zwangsvollstreckung in Forderungen und andere Vermögensrechte sind entsprechend anzuwenden.

(3) Sobald die Voraussetzungen für die Sicherstellung weggefallen sind, sind die Sachen derjenigen oder demjenigen herauszugeben, bei der oder dem sie sichergestellt worden sind; Forderungen oder andere Vermögensrechte sind entsprechend freizugeben. Ist die Herausgabe an sie oder ihn nicht möglich, können sie an eine andere Person herausgegeben werden, die ihre Berechtigung glaubhaft macht. Die Herausgabe ist ausgeschlossen, wenn dadurch erneut die Voraussetzungen für eine Sicherstellung eintreten würden; soweit es sich um sichergestellte Forderungen oder anderen Vermögensrechte handelt, kann die Sicherstellung um jeweils weitere sechs Monate verlängert werden. Über die Verlängerung entscheidet auf Antrag der Leitung der Polizeibehörde das Amtsgericht, in dessen Bezirk die Inhaberin oder der Inhaber der Forderung oder Vermögensrechte ihren oder seinen Wohnsitz oder ständigen Aufenthalt hat. Der Antrag muss neben den Angaben aus der nach Absatz 2 erfolgten Sicherstellung insbesondere die Gründe für die Verlängerung enthalten.

(4) Die Herausgabe der Sachen kann von der Zahlung der Kosten, die durch die Sicherstellung entstanden sind, abhängig gemacht werden.

§ 62
Verfahren bei der Sicherstellung von Sachen

(1) Hat eine Person eine bewegliche Sache herauszugeben oder vorzulegen, so kann die Vollzugsbeamtin oder der Vollzugsbeamte (§ 103) sie ihr wegnehmen.

(2) Der herausgabepflichtigen Person ist eine Bescheinigung zu erteilen, die die weggenommene Sache bezeichnet, den Grund der Maßnahme erkennen lässt und eine Belehrung über die zulässigen Rechtsbehelfe enthalten soll.

(3) Wird die Sache nicht vorgefunden, so hat die herausgabepflichtige Person auf Verlangen der Vollzugsbehörde vor dem Amtsgericht an Eides Statt zu versichern, dass sie nicht wisse, wo die Sache sich befinde.

(4) Dem Antrag an das Amtsgericht, der herausgabepflichtigen Person die eidesstattliche Versicherung abzunehmen, sind beglaubigte Abschriften des Verwaltungsaktes sowie eine etwaige Niederschrift über den erfolglosen Wegnahmeversuch beizufügen. Für das Verfahren vor dem Amtsgericht gelten die §§ 478 bis 480, 483, 802e, 802f Absatz 4, 802g bis 802i, 883 Absatz 2 Satz 2 und Absatz 3 der Zivilprozessordnung entsprechend.

(5) Sichergestellte Sachen sind amtlich zu verwahren. Falls die Beschaffenheit der Sache dies nicht zulässt oder die amtliche Verwahrung unzweckmäßig ist, kann der Zweck der Sicherstellung auf andere Weise gewährleistet werden.

§ 63
Amtliche Verwahrung

(1) Wird eine Sache amtlich oder durch einen Anderen in amtlichem Auftrag verwahrt, so ist das Erforderliche zu veranlassen, um einem Verderb oder einer wesentlichen Minderung ihres Wertes vorzubeugen. Dies gilt nicht, wenn der Andere auf Verlangen der früheren Gewahrsamsinhaberinnen oder Gewahrsamsinhaber mit der Verwahrung beauftragt worden sind. Abweichende Rechtsvorschriften bleiben unberührt.

(2) Die verwahrten Sachen sind zu verzeichnen und so zu kennzeichnen, dass Verwechselungen vermieden werden.

§ 64
Verwertung, Vernichtung

(1) Die Verwertung verwahrter Sachen ist zulässig, wenn
1. ihr Verderb oder eine wesentliche Minderung ihres Wertes droht oder ihre Aufbewahrung oder Unterhaltung mit unverhältnismäßig hohen Kosten, erheblichen Schwierigkeiten oder Gefahren für die öffentliche Sicherheit oder Ordnung verbunden ist,
2. die empfangsberechtigte Person die Sache innerhalb einer Frist von sechs Wochen nach schriftlich ergangener Aufforderung nicht in Empfang nimmt oder
3. die Sache nach einer Frist von sechs Monaten nicht an die empfangsberechtigte Person herausgegeben werden kann, ohne dass die Gründe, die zu ihrer Sicherstellung berechtigten, fortbestehen oder Sicherstellungsgründe erneut entstehen würden.

(2) Die Verwertung soll nach den §§ 296, 298, 302 bis 305 und 308 der Abgabenordnung durchgeführt werden. Die Eigentümerin oder der Eigentümer und andere Personen, denen Rechte an der Sache zustehen, sollen vor der Androhung der Verwertung gehört werden; ihnen sollen Ort und Zeit der Verwertung mitgeteilt werden. Bei der Verwertung von Datenträgern ist sicherzustellen, dass zuvor personenbezogene Daten dem Stand der Technik entsprechend gelöscht wurden.

(3) Der Erlös tritt an die Stelle der Sache und ist an die berechtigte Person herauszugeben. Ist eine berechtigte Person nicht vorhanden oder nicht zu ermitteln, so ist der Erlös nach den Vorschriften des Bürgerlichen Gesetzbuchs zu hinterlegen. Der Anspruch auf Herausgabe des Erlöses erlischt drei Jahre nach Ablauf des Jahres, in dem die Sache verwertet worden ist. Ist eine Sache verwertet worden, können die Kosten aus dem Erlös gedeckt werden.

(4) Verwahrte Sachen können unbrauchbar gemacht, vernichtet oder eingezogen werden, wenn
1. im Falle einer Verwertung die Gründe, die zu ihrer Sicherstellung berechtigten, fortbestehen oder Sicherstellungsgründe erneut entstehen würden oder
2. eine Verwertung aus anderen Gründen nicht möglich ist oder der zu erwartende Erlös aus einer Verwertung die entstehenden Kosten nicht deckt.

Absatz 2 Satz 2 gilt entsprechend.

§ 65
Verfahren bei der Wegnahme einer Person

(1) Hat jemand eine Person herauszugeben, so kann die Vollzugsbeamtin oder der Vollzugsbeamte (§ 103) sie jeder Person wegnehmen, bei der sie angetroffen wird.

(2) Der herausgabepflichtigen Person ist eine Bescheinigung zu erteilen, die die weggenommene Person bezeichnet, den Grund der Maßnahme erkennen lässt und eine Belehrung über die zulässigen Rechtsbehelfe enthalten soll.

(3) Wird die Person nicht vorgefunden, so hat die herausgabepflichtige Person auf Verlangen der Vollzugsbehörde vor dem Amtsgericht an Eides Statt zu versichern, dass sie nicht wisse, wo die Person sich befinde.

(4) § 62 Absatz 4 gilt entsprechend.

§ 66
Verfahren bei der Zwangsräumung

(1) Hat eine Person eine unbewegliche Sache, einen Raum oder ein Schiff zu räumen oder herauszugeben, so können sie und die ihrem Haushalt oder Geschäftsbetrieb angehörenden Personen aus dem Besitz gesetzt werden. Der Zeitpunkt der Zwangsräumung soll der betroffenen Person in angemessener Zeit vorher angekündigt werden.

(2) Werden bei einer Zwangsräumung bewegliche Sachen vorgefunden, die nicht herauszugeben oder vorzulegen sind, so werden sie der betroffenen Person oder, wenn diese abwesend ist, der Vertreterin oder dem Vertreter oder einer dem Haushalt oder Geschäftsbetrieb der betroffenen Person angehörenden erwachsenen Person übergeben.

(3) Ist keine empfangsberechtigte Person nach Absatz 2 anwesend, so sind die beweglichen Sachen in amtliche Verwahrung zu nehmen. Dies gilt auch, wenn sich die empfangsberechtigte Person weigert, die Sachen anzunehmen.

§ 67
Übertragung des Eigentums

(1) Ist eine Person zur Übertragung des Eigentums an einer Sache verpflichtet, so ist für die nach bürgerlichem Recht erforderlichen Willenserklärungen und für die Eintragung in öffentliche Bücher und Register § 93 anzuwenden.

(2) Die Übergabe der Sache wird dadurch bewirkt, dass die Vollzugsbeamtin oder der Vollzugsbeamte die Sache in Besitz nimmt. § 62 Absatz 3 und 4 gilt entsprechend. Befindet sich die Sache im Gewahrsam Anderer, so ist der Behörde, die den Verwaltungsakt erlassen hat, der Anspruch der betroffenen Person auf Herausgabe der Sache zu überweisen. Die §§ 309 bis 313 und 315 bis 317 der Abgabenordnung sind entsprechend anzuwenden.

Unterabschnitt 2
Besondere Maßnahmen der Polizei im Zusammenhang mit drohenden terroristischen Straftaten (§§ 67a - 67d)

§ 67a
Elektronische Aufenthaltsüberwachung

(1) Die Polizei kann eine Person dazu verpflichten, ein technisches Mittel, mit dem der Aufenthaltsort dieser Person elektronisch überwacht werden kann, ständig in betriebsbereitem Zustand am Körper bei sich zu führen und dessen Funktionsfähigkeit nicht zu beeinträchtigen, wenn

1. Tatsachen die Annahme rechtfertigen, dass diese Person innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat nach § 67c begehen oder an dieser teilnehmen wird, oder
2. das individuelle Verhalten dieser Person die konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb eines überschaubaren Zeitraums eine terroristische Straftat nach § 67c begehen oder an dieser teilnehmen wird,

um diese Person durch die Überwachung und die Datenverwendung von der Begehung einer solchen Straftat abzuhalten.

(2) Eine Maßnahme nach Absatz 1 soll mit einer Maßnahme nach § 67b verbunden werden.

(3) Die Polizei kann mit Hilfe der von der verantwortlichen Person mitgeführten technischen Mittel automatisiert Daten über deren Aufenthaltsort sowie über etwaige Beeinträchtigungen der Datenerhebung erheben und speichern. Soweit es technisch möglich ist, ist sicherzustellen, dass innerhalb der Wohnung der betroffenen Person keine über den Umstand ihrer Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden. Die Daten dürfen ohne Einwilligung der betroffenen Person nur verarbeitet werden, soweit dies erforderlich ist für die folgenden Zwecke:

1. zur Verhütung oder zur Verfolgung einer terroristischen Straftat nach § 67c,
2. zur Feststellung von Verstößen gegen eine Aufenthaltsanordnung nach § 67b,
3. zur Verfolgung einer Straftat nach § 67d,
4. zur Abwehr einer gegenwärtigen erheblichen Gefahr oder
5. zur Aufrechterhaltung der Funktionsfähigkeit der technischen Mittel.

Zur Einhaltung der Zweckbindung nach Satz 3 hat die Verarbeitung der Daten automatisiert zu erfolgen. Zudem sind die Daten gegen unbefugte Kenntnisnahme und Verarbeitung besonders zu sichern.

(4) Die in Absatz 3 Satz 1 genannten Daten sind spätestens zwei Monate nach ihrer Erhebung zu löschen, soweit sie nicht für die in Absatz 3 Satz 3 genannten Zwecke verwendet werden. Für die Protokollierung gelten die §§ 46e und 46f. Werden innerhalb der Wohnung der betroffenen Person über den Umstand ihrer Anwesenheit hinausgehende Aufenthaltsdaten erhoben, dürfen diese nicht verarbeitet werden und sind unverzüglich nach Kenntnisnahme zu löschen. Die Tatsache ihrer Kenntnisnahme ist zu dokumentieren und die Löschung zu protokollieren; für die Dokumentation gilt § 46d und für die Protokollierung Satz 2.

(5) Eine Maßnahme nach Absatz 1, auch in Verbindung mit Absatz 2, bedarf der richterlichen Anordnung auf Antrag der Leitung der zuständigen Polizeibehörde. Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, mit Namen und Anschrift,
2. Art, Umfang und Dauer der Maßnahme, die Angabe, ob gegenüber der Person, gegen die sich die Maßnahme richtet, eine Aufenthaltsanordnung nach § 67b besteht,
3. der Sachverhalt sowie
4. eine Begründung.

Bei Gefahr im Verzug kann die Leitung der zuständigen Polizeibehörde die Maßnahme anordnen; § 25b gilt entsprechend. Eine richterliche Entscheidung ist unverzüglich nachzuholen. Soweit die Anordnung nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(6) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, mit Namen und Anschrift,
2. Art, Umfang und Dauer der Maßnahme,
3. im Fall des Absatzes 2 die Angaben aus § 67b Absatz 3 Satz 2 Nummer 2 sowie
4. die Gründe.

(7) Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist möglich, soweit die Anordnungsvoraussetzungen fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, ist die Maßnahme unverzüglich zu beenden.

§ 67b
Aufenthaltsanordnung

(1) Die Polizei kann zur Abwehr einer Gefahr oder zur Verhütung einer terroristischen Straftat nach § 67c einer Person untersagen, sich ohne Erlaubnis der zuständigen Polizeibehörde von ihrem Wohn- oder Aufenthaltsort oder aus einem bestimmten Bereich zu entfernen (Aufenthaltsgebot) oder sich an bestimmten Orten aufzuhalten (Aufenthaltsverbot), wenn

1. Tatsachen die Annahme rechtfertigen, dass die betroffene Person innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat nach § 67c begehen oder an dieser teilnehmen wird, oder
2. das individuelle Verhalten der betroffenen Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines überschaubaren Zeitraums eine terroristische Straftat nach § 67c begehen oder an dieser teilnehmen wird.

(2) Maßnahmen nach Absatz 1 dürfen nur von der Leitung der zuständigen Polizeibehörde angeordnet werden. Widerspruch und Anfechtungsklage gegen die Anordnung haben keine aufschiebende Wirkung.

(3) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, mit Namen und Anschrift,
2. Art, Umfang und Dauer der Maßnahme, einschließlich einer Bezeichnung der Orte, von denen sich die Person ohne Erlaubnis der zuständigen Polizeibehörde nicht entfernen oder an denen sich die Person ohne Erlaubnis der zuständigen Polizeibehörde nicht aufhalten darf, sowie
3. die Gründe.

(4) Aufenthaltsgebote und Aufenthaltsverbote sind auf den zur Abwehr der Gefahr oder zur Verhütung einer terroristischen Straftat nach § 67c erforderlichen Umfang zu beschränken und dürfen räumlich den Zugang zur Wohnung der betroffenen Person nicht umfassen. Sie sind auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist möglich, soweit ihre Voraussetzungen fortbestehen. Eine Verlängerung bedarf der gerichtlichen Anordnung nach Maßgabe des Absatzes 3 auf Antrag der Leitung der zuständigen Polizeibehörde; der Antrag muss die Angaben nach Absatz 3 Satz 2 Nummer 1 und 2 sowie den Sachverhalt und eine Begründung enthalten.

(5) Die Vorschriften des Versammlungsrechts bleiben unberührt. Eine Aufenthaltsanordnung nach Absatz 1 geht einem Aufenthalts- und Betretungsverbot nach § 52a vor, soweit sie sich entgegenstehen. Gleiches gilt in Bezug auf eine nach § 52b Absatz 1 Satz 1 angeordnete Meldeauflage.

§ 67c
Terroristische Straftat

Eine terroristische Straftat im Sinne dieses Gesetzes ist eine Straftat
1. nach den §§ 89a bis 89c, 129a und 129b des Strafgesetzbuches,
2. nach den §§ 211, 212, 224, 226 und 227 des Strafgesetzbuches,
3. nach den §§ 239a und 239b des Strafgesetzbuches,
4. nach den §§ 303b, 305, 305a, 306 bis 306c, 307 Absatz 1 bis 3, 308 Absatz 1 bis 4, 309 Absatz 1 bis 5, 310 Absatz 1 oder 2, 313, 314, 315 Absatz 1, 3 oder 4, 315b Absatz 1 oder 3, 316b Absatz 1 oder 3, 316c Absatz 1 bis 3 und 317 Absatz 1 des Strafgesetzbuches,
5. nach den §§ 328 Absatz 1 oder 2, 330 Absatz 1 oder 2 und 330a Absatz 1 bis 3 des Strafgesetzbuches,
6. nach den §§ 19 Absatz 1 bis 3, 20 Absatz 1 oder 2, 20a Absatz 1 bis 3 oder nach § 22a Absatz 1 bis 3 des Gesetzes über die Kontrolle von Kriegswaffen,
7. nach den §§ 19 Absatz 2 Nummer 2 oder Absatz 3 Nummer 2, 20 Absatz 1 oder 2 oder 20a Absatz 1 bis 3 jeweils auch in Verbindung mit § 21 des Gesetzes über die Kontrolle von Kriegswaffen,
8. nach § 51 Absatz 1 bis 3 des Waffengesetzes,
9. nach den §§ 6 bis 12 des Völkerstrafgesetzbuches

bei Begehung im In- und Ausland, wenn diese Straftat dazu bestimmt ist,

1. die Bevölkerung auf erhebliche Weise einzuschüchtern,
2. eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder
3. die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates, eines Landes oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen

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

§ 67d
Strafvorschrift

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer gegen eine gerichtliche Anordnung nach § 67a Absatz 1 verstößt und dadurch den Zweck der Maßnahme gefährdet.

(2) Ebenso wird bestraft, wer gegen eine gerichtliche Anordnung nach § 67b, die mit der Anordnung einer Maßnahme nach § 67a Absatz 1 verbunden wurde, verstößt und dadurch den Zweck der Aufenthaltsanordnung gefährdet.

(3) Absatz 1 und 2 gelten auch in den Fällen einer behördlichen Anordnung bei Gefahr im Verzug nach § 67a Absatz 5 Satz 3; die Strafbarkeit entfällt, wenn die Anordnung nicht innerhalb der Frist des § 67a Absatz 5 Satz 4 durch das zuständige Gericht bestätigt wird.

(4) Die Tat wird nur auf Antrag der zuständigen Polizeibehörde verfolgt.

Abschnitt 5
In Anspruch zu nehmende Personen (§§ 68 - 71)

§ 68
Grundsatz

Maßnahmen zur Gefahrenabwehr dürfen nur gegen die nach den §§ 69 oder 70 verantwortlichen Personen gerichtet werden, es sei denn, dass gesetzlich etwas anderes bestimmt ist.

§ 69
Verantwortlichkeit für das Verhalten von Personen

(1) Wird die öffentliche Sicherheit oder Ordnung durch das Verhalten von Personen gestört oder im einzelnen Fall gefährdet, so ist die Person verantwortlich, die die Störung oder Gefahr verursacht hat.

(2) Verursachen Personen, die das 14. Lebensjahr noch nicht vollendet haben, die Störung oder Gefahr, so ist auch diejenige Person verantwortlich, der die Sorge für die minderjährige Person obliegt. Ist für die Person eine Betreuerin oder ein Betreuer bestellt, so können die Maßnahmen im Rahmen ihres oder seines Aufgabenkreises auch gegen sie oder ihn gerichtet werden.

(3) Verursacht eine Person, die zu einer Verrichtung bestellt ist, die Störung oder Gefahr, so ist auch die Person verantwortlich, die die andere Person zu der Verrichtung bestellt hat.

§ 70
Verantwortlichkeit für Sachen

(1) Wird die öffentliche Sicherheit oder Ordnung durch den Zustand einer Sache gestört oder im einzelnen Fall gefährdet, so ist deren Eigentümerin oder Eigentümer verantwortlich.

(2) Eine Person, die die tatsächliche Gewalt über eine Sache ausübt, ist neben der Eigentümerin oder dem Eigentümer verantwortlich. Sie ist an Stelle der Eigentümerin oder des Eigentümers verantwortlich, wenn sie die tatsächliche Gewalt gegen den Willen der Eigentümerin oder des Eigentümers ausübt.

(3) Geht die Störung oder Gefahr von einer herrenlosen Sache aus, so können die Maßnahmen gegen die Person gerichtet werden, die das Eigentum an der Sache aufgegeben hat.

(4) Gesetze, die eine andere Regelung enthalten, bleiben unberührt.

§ 70a
Unmittelbare Ausführung einer Maßnahme

Die Ordnungsbehörden und die Polizei können eine Maßnahme selbst oder durch eine Beauftragte oder einen Beauftragten (unmittelbar) ausführen, wenn die oder der nach den §§ 69 oder 70 Verantwortliche nicht oder nicht rechtzeitig erreicht werden kann und die Maßnahme dem tatsächlichen oder mutmaßlichen Willen der oder des Verantwortlichen entspricht. Die von der Maßnahme Betroffenen sind unverzüglich zu unterrichten.

§ 71
Inanspruchnahme des Nichtstörers

(1) Zur Beseitigung einer Störung oder zur Abwehr einer gegenwärtigen Gefahr können Maßnahmen auch gegen andere Personen als die Verantwortlichen (§§ 68 bis 70) getroffen werden, soweit und solange

1. die Verantwortlichen nicht oder nicht rechtzeitig in Anspruch genommen werden können oder Maßnahmen gegen sie keinen Erfolg versprechen und
2. die Störung oder Gefahr nicht durch die Behörde selbst oder durch eine Beauftragte oder einen Beauftragten beseitigt werden kann und
3. die andere Person ohne erhebliche eigene Gefährdung oder Verletzung anderer überwiegender Pflichten in Anspruch genommen werden kann.

(2) Wird eine andere Person in Anspruch genommen, so hat die Behörde die verantwortliche Person unverzüglich zu benachrichtigen.

Abschnitt 6
Entschädigungsansprüche (§§ 72 - 77)

§ 72
Entschädigungsanspruch des Nichtstörers

(1) Wer nach § 71 in Anspruch genommen wird, kann Entschädigung für den ihm hierdurch entstandenen Schaden verlangen.

(2) Ein Entschädigungsanspruch besteht jedoch nicht, soweit
1. die oder der Geschädigte auf andere Weise Ersatz erlangt hat oder
2. die oder der Geschädigte oder ihr oder sein Vermögen durch die Maßnahme geschützt worden ist.

(3) Die Absätze 1 und 2 finden keine Anwendung, soweit die Entschädigungspflicht wegen rechtmäßiger Maßnahmen in anderen gesetzlichen Vorschriften geregelt oder ausgeschlossen ist.

§ 73
Entschädigungsanspruch Unbeteiligter

§ 72 findet entsprechende Anwendung, wenn Unbeteiligte, die weder nach den §§ 68 bis 70 verantwortlich noch nach § 71 in Anspruch genommen worden sind, durch Maßnahmen zur Gefahrenabwehr getötet oder verletzt werden oder einen billigerweise nicht zumutbaren Schaden erleiden.

§ 74
Art, Inhalt und Umfang der Entschädigungsleistung

(1) Die Entschädigung wird nur für Vermögensschäden gewährt. Für entgangenen Gewinn, der über den Ausfall des gewöhnlichen Verdienstes oder Nutzungsentgeltes hinausgeht, und für Vermögensnachteile, die nicht in unmittelbarem Zusammenhang mit der zu entschädigenden Maßnahme stehen, ist jedoch eine Entschädigung nur zu leisten, wenn und soweit diese zur Abwendung unbilliger Härten geboten erscheint.

(2) Die Entschädigung ist in Geld zu gewähren. Besteht der Schaden in der Aufhebung oder Verminderung der Erwerbsfähigkeit oder in einer Vermehrung der Bedürfnisse oder in dem Verlust oder der Minderung eines Rechts auf Unterhalt, so ist die Entschädigung durch Entrichtung einer Geldrente zu gewähren. Statt der Rente kann eine Abfindung in Kapital verlangt werden, wenn ein wichtiger Grund vorliegt.

(3) Die Entschädigung ist nur gegen Abtretung der Ansprüche zu gewähren, die der oder dem Entschädigungsberechtigten aufgrund der Maßnahme, auf der die Entschädigung beruht, gegen Andere zustehen.

(4) Hat bei der Entstehung des Schadens ein Verschulden der betroffenen Person mitgewirkt, so ist das Mitverschulden zu berücksichtigen.

(5) Der Entschädigungsanspruch kann nur innerhalb eines Jahres geltend gemacht werden; die Frist beginnt, sobald die oder der Geschädigte von dem Schaden und dem entschädigungspflichtigen Träger der öffentlichen Verwaltung Kenntnis erlangt. Ohne Rücksicht auf diese Kenntnis kann der Anspruch nur innerhalb von dreißig Jahren seit der Entstehung des Anspruchs geltend gemacht werden.

(6) Gesetze, die weitergehende Ersatzansprüche gewähren, bleiben unberührt.

§ 75
Entschädigungspflichtiger Rückgriff

(1) Entschädigungspflichtig ist der Träger der öffentlichen Verwaltung, in dessen Dienst diejenige oder derjenige steht, die oder der die Maßnahme getroffen hat.

(2) Hat die oder der Bedienstete für die Behörde eines anderen Trägers gehandelt, so ist letztgenannter entschädigungspflichtig. Ist in den Fällen des Satzes 1 eine Entschädigung nur wegen der Art und Weise der Durchführung der Maßnahme zu gewähren, so kann der entschädigungspflichtige Träger von dem Träger, in dessen Dienst die oder der Bedienstete steht, Ersatz seiner Aufwendungen verlangen, es sei denn, dass er selbst die Verantwortung für die Art und Weise der Durchführung trägt.

(3) In den Fällen des § 72 kann die oder der Entschädigungspflichtige in entsprechender Anwendung der Vorschriften des Bürgerlichen Gesetzbuches über die Geschäftsführung ohne Auftrag von den nach den §§ 68 bis 70 Verantwortlichen durch Verwaltungsakt Ersatz seiner Aufwendungen verlangen.

§ 76
Schadensersatzansprüche und Entschädigung aus der Verarbeitung von Daten

(1) Hat eine verantwortliche Stelle einer betroffenen Person durch eine Verarbeitung zu Zwecken der Richtlinie (EU) 2016/680 personenbezogener Daten, die nach diesem Gesetz oder nach anderen auf ihre Verarbeitung anwendbaren Vorschriften rechtswidrig war, einen Schaden zugefügt, ist sie oder ihr Rechtsträger der betroffenen Person zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit bei einer nicht automatisierten Verarbeitung der Schaden nicht auf ein Verschulden der verantwortlichen Stelle zurückzuführen ist.

(2) Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

(3) Lässt sich bei einer automatisierten Verarbeitung personenbezogener Daten nicht ermitteln, welche von mehreren beteiligten verantwortlichen Stellen den Schaden verursacht hat, so haftet jede verantwortliche Stelle beziehungsweise ihr Rechtsträger.

(4) Mehrere Ersatzpflichtige haften als Gesamtschuldner.

(5) Hat bei der Entstehung des Schadens ein Verschulden der betroffenen Person mitgewirkt, ist § 254 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(6) Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

(7) Vorschriften, nach denen Ersatzpflichtige in weiterem Umfang als nach dieser Vorschrift haften oder nach denen andere für den Schaden verantwortlich sind, bleiben unberührt.

§ 77
Rechtsweg

Für Streitigkeiten über die in §§ 72 bis 74 und 76 bezeichneten Ansprüche ist der ordentliche Rechtsweg gegeben.

Abschnitt 7
Einschränkung von Grundrechten (§ 78)

§ 78
Einschränkung von Grundrechten

Für Maßnahmen, die nach den Vorschriften der Abschnitte 1 bis 6 getroffen werden können, werden das Recht auf körperliche Unversehrtheit (Artikel 2 Absatz 2 Satz 1 des Grundgesetzes), das Recht der Freiheit der Person (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes), das Recht auf Versammlungsfreiheit (Artikel 8 Absatz 1 des Grundgesetzes), das Recht auf Wahrung des Fernmeldegeheimnisses (Artikel 10 Absatz 1 des Grundgesetzes), das Recht der Freizügigkeit (Artikel 11 des Grundgesetzes) und das Recht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) eingeschränkt.

Abschnitt 8
Erzwingung von Handlungen, Duldungen oder Unterlassungen (§§ 79 - 113)

Unterabschnitt 1
Allgemeines Vollzugsverfahren (§§ 79 - 92)

§ 79
Grundsatz

(1) Verwaltungsakte, die auf Herausgabe einer Sache oder auf Vornahme einer Handlung oder auf Duldung oder Unterlassung gerichtet sind, werden im Wege des Verwaltungszwangs durchgesetzt (Vollzug).

(2) Für den Vollzug gelten die §§ 80 bis 99.

(3) Die §§ 80 bis 99 gelten auch für den Vollzug von Verwaltungsakten, die nicht der Gefahrenabwehr dienen und die von Behörden der in § 1 genannten Verwaltungsträger sowie der sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts erlassen werden.

§ 80
Zulässigkeit des Vollzugs von Verwaltungsakten

(1) Der Vollzug von Verwaltungsakten ist zulässig, wenn
1. der Verwaltungsakt unanfechtbar ist oder
2. ein Rechtsbehelf keine aufschiebende Wirkung hat.

(2) Beim Vollzug eines Verwaltungsaktes im Wege der Ersatzvornahme (§ 89) oder der Anwendung unmittelbaren Zwangs (§ 90) kann von Absatz 1 abgewichen werden, wenn
1. auf andere Weise eine gegenwärtige Gefahr für die öffentliche Sicherheit oder Ordnung nicht abgewehrt werden kann oder
2. eine rechtswidrige Tat oder mit Geldbuße bedrohte Handlung anders nicht verhindert werden kann.

§ 81
Sofortiger Vollzug

(1) Der Verwaltungszwang ohne vorausgegangenen Verwaltungsakt (sofortiger Vollzug) ist im Wege der Ersatzvornahme oder des unmittelbaren Zwangs zulässig, wenn eine gegenwärtige Gefahr auf andere Weise nicht abgewehrt werden kann und die Behörde hierbei innerhalb ihrer gesetzlichen Befugnisse handelt. Dies gilt insbesondere, wenn Maßnahmen gegen pflichtige Personen nicht oder nicht rechtzeitig möglich sind. Rechtsvorschriften, die die Voraussetzungen des sofortigen Vollzugs abweichend regeln, bleiben unberührt.

(2) Bei einer Ersatzvornahme sind die Verantwortlichen unverzüglich zu benachrichtigen.

(3) Für den sofortigen Vollzug gelten die nachfolgenden Vorschriften über den Vollzug von Verwaltungsakten entsprechend, soweit in ihnen nichts anderes bestimmt ist.

§ 82
Vollzugsbehörden

Der Verwaltungsakt wird von der Behörde vollzogen, die ihn erlassen hat; sie vollzieht auch die Widerspruchsentscheidungen.

§ 82a
Vollzugshilfe

(1) Die Polizei leistet anderen Behörden im Einzelfall auf Ersuchen Vollzugshilfe, wenn unmittelbarer Zwang anzuwenden ist und die anderen Behörden nicht über die hierzu erforderlichen Dienstkräfte verfügen oder ihre Maßnahmen nicht auf andere Weise selbst durchsetzen können.

(2) Die Polizei ist nur für die Art und Weise der Durchführung verantwortlich. Im Übrigen gelten die Grundsätze der Amtshilfe entsprechend.

(3) Die Verpflichtung zur Amtshilfe bleibt unberührt.

§ 82b
Verfahren

(1) Vollzugshilfeersuchen sind grundsätzlich schriftlich zu stellen; sie haben den Grund und die Rechtsgrundlage der Maßnahme anzugeben.

(2) In Eilfällen kann das Ersuchen formlos gestellt werden. Es ist jedoch auf Verlangen unverzüglich schriftlich zu bestätigen.

(3) Die ersuchende Behörde ist von der Ausführung des Ersuchens zu verständigen.

§ 82c
Vollzugshilfe bei Freiheitsentziehung

(1) Hat das Vollzugshilfeersuchen eine Freiheitsentziehung zum Inhalt, ist auch die richterliche Entscheidung über die Zulässigkeit der Freiheitsentziehung vorzulegen oder in dem Ersuchen zu bezeichnen.

(2) Ist eine vorherige richterliche Entscheidung nicht ergangen, hat die Polizei die festgehaltene Person zu entlassen, wenn die ersuchende Behörde diese nicht übernimmt oder die richterliche Entscheidung nicht unverzüglich nachträglich beantragt.

(3) § 56 gilt entsprechend.

§ 83
Pflichtige Person

(1) Als pflichtige Person kann in Anspruch genommen werden
1. diejenige, gegen die sich der Verwaltungsakt richtet,
2. ihr Rechtsnachfolger, soweit der Verwaltungsakt auch gegen ihn wirkt.

(2) Ist jemand nach diesem Gesetz oder nach anderen Rechtsvorschriften verpflichtet, den Vollzug zu dulden, so ist er pflichtige Person, soweit seine Duldungspflicht reicht.

§ 84
Vollzug gegen den Rechtsnachfolger

(1) Der Vollzug gegen den Rechtsnachfolger darf erst beginnen, nachdem er von dem Verwaltungsakt Kenntnis erhalten hat und darauf hingewiesen worden ist, dass der Vollzug gegen ihn durchgeführt werden kann. Von diesen Voraussetzungen kann in den Fällen des § 80 Absatz 2 abgesehen werden.

(2) Der Vollzug, der im Zeitpunkt des Eintritts der Rechtsnachfolge bereits begonnen hat, darf gegen den Rechtsnachfolger fortgesetzt werden. Dabei ist Absatz 1 zu beachten.

§ 85
Vollzug gegen Träger der öffentlichen Verwaltung

Gegen Träger der öffentlichen Verwaltung ist der Vollzug nur zulässig, soweit er durch Rechtsvorschrift ausdrücklich zugelassen ist.

§ 86
Zwangsmittel

(1) Zwangsmittel sind
1. das Zwangsgeld (§ 88),
2. die Ersatzvornahme (§ 89),
3. der unmittelbare Zwang (§ 90).

(2) Die Zwangsmittel können auch neben einer Strafe oder Geldbuße angewandt und solange wiederholt und gewechselt werden, bis der Verwaltungsakt befolgt worden oder auf andere Weise erledigt ist.

§ 87
Androhung von Zwangsmitteln

(1) Die Zwangsmittel müssen schriftlich angedroht werden. Beim Vorliegen der Voraussetzungen des § 80 Absatz 2 sowie des § 81 kann das Zwangsmittel mündlich angedroht werden oder die Androhung unterbleiben.

(2) In der Androhung ist eine Frist zu bestimmen, innerhalb der die Erfüllung der Verpflichtung der pflichtigen Person billigerweise zugemutet werden kann. Eine Frist braucht nicht bestimmt zu werden, wenn eine Duldung oder Unterlassung erzwungen werden soll.

(3) Die Androhung kann mit dem Verwaltungsakt, der vollzogen werden soll, verbunden werden. Sie soll mit ihm verbunden werden, wenn die sofortige Vollziehung angeordnet oder dem Rechtsbehelf keine aufschiebende Wirkung beigelegt ist (§ 80 Absatz 1 Nummer 2).

(4) Die Androhung muss sich auf bestimmte Zwangsmittel beziehen. Werden mehrere Zwangsmittel angedroht, ist anzugeben, in welcher Reihenfolge sie angewandt werden sollen. Unzulässig ist die Androhung, mit der sich die Vollzugsbehörde die Wahl zwischen den Zwangsmitteln vorbehält.

(5) Das Zwangsgeld ist in bestimmter Höhe anzudrohen.

(6) Im Falle der Ersatzvornahme (§ 89) ist in der Androhung der Kostenbetrag vorläufig zu veranschlagen. Das Recht auf Nachforderung bleibt unberührt.

§ 88
Zwangsgeld

(1) Das Zwangsgeld ist zulässig, wenn
1. die pflichtige Person angehalten werden soll, eine Handlung vorzunehmen, oder
2. die pflichtige Person ihrer Verpflichtung zuwiderhandelt, eine Handlung zu dulden oder zu unterlassen.

(2) Das Zwangsgeld ist schriftlich festzusetzen.

(3) Das Zwangsgeld beträgt mindestens 10 Euro, höchstens 50 000 Euro.

§ 89
Ersatzvornahme

(1) Wird eine Verpflichtung, eine Handlung vorzunehmen, deren Vornahme durch einen anderen möglich ist, nicht erfüllt, so kann die Vollzugsbehörde die Handlung auf Kosten der pflichtigen Person ausführen oder durch eine oder einen Beauftragten ausführen lassen (Ersatzvornahme).

(2) Die Vollzugsbehörde kann der pflichtigen Person auferlegen, die Kosten in der vorläufig veranschlagten Höhe vorauszuzahlen.

§ 90
Unmittelbarer Zwang

Führen die Ersatzvornahme oder das Zwangsgeld nicht zum Erfolg oder sind sie unzweckmäßig, so kann die Vollzugsbehörde mit unmittelbarem Zwang die Handlung selbst vornehmen oder die pflichtige Person zur Handlung, Duldung oder Unterlassung zwingen.

§ 91
Ersatzzwangshaft

(1) Ist das Zwangsgeld uneinbringlich, so kann das Verwaltungsgericht auf Antrag der Vollzugsbehörde die Ersatzzwangshaft anordnen, wenn bei Androhung des Zwangsgeldes hierauf hingewiesen worden ist. Die Ersatzzwangshaft beträgt mindestens einen Tag, höchstens zwei Wochen.

(2) Die Ersatzzwangshaft ist auf Antrag der Vollzugsbehörde von der Justizverwaltung nach den Bestimmungen der §§ 802g Absatz 1 Satz 2 und 3 sowie Absatz 2, 802h und 802i der Zivilprozessordnung zu vollstrecken.

§ 92
Einstellung des Vollzugs

(1) Der Vollzug ist einzustellen, wenn
1. der Verwaltungsakt aufgehoben worden ist,
2. die Vollziehung des Verwaltungsaktes ausgesetzt worden ist,
3. die aufschiebende Wirkung eines Rechtsbehelfs angeordnet oder wiederhergestellt worden ist,
4. der Zweck des Vollzuges erreicht ist oder
5. weitere Verstöße gegen eine Duldungs- oder Unterlassungspflicht nicht zu erwarten sind.

(2) Die Vollzugsbeamtinnen und Vollzugsbeamten (§ 103) sind nur dann verpflichtet, von weiteren Vollzugsmaßnahmen abzusehen, wenn ihnen Tatsachen nachgewiesen werden, aus denen sich die Pflicht zur Einstellung eindeutig ergibt.

Unterabschnitt 2
Vollzug von Verwaltungsakten, die auf Abgabe einer Erklärung gerichtet sind (§ 93)

§ 93
Abgabe einer Erklärung

(1) Ist jemand verpflichtet, eine bestimmte Erklärung abzugeben, so gilt diese Erklärung als abgegeben, sobald der Verwaltungsakt, der die Verpflichtung begründet hat, unanfechtbar geworden ist. Voraussetzung ist, dass
1. der Inhalt der Erklärung in dem Verwaltungsakt festgelegt worden ist,
2. die pflichtige Person auf diese Rechtsfolge hingewiesen worden ist und
3. sie in dem Zeitpunkt des Eintritts der Unanfechtbarkeit des Verwaltungsaktes diese Erklärung rechtswirksam abgeben kann.

(2) Die Behörde, die den Verwaltungsakt erlassen hat, teilt den Beteiligten mit, in welchem Zeitpunkt der Verwaltungsakt unanfechtbar geworden ist. Sie ist berechtigt, die zur Wirksamkeit der Erklärung erforderlichen Genehmigungen und Zustimmungen einzuholen und Anträge auf Eintragungen in öffentliche Bücher und Register zu stellen. § 792 der Zivilprozessordnung ist anzuwenden.

Unterabschnitt 3
Erweiterte Anwendung der Vollzugsvorschriften (§§ 94 - 97)

§ 94
Anwendung der Vollzugsvorschriften aufgrund bundesrechtlicher Ermächtigungen

Die Vorschriften über die Erzwingung von Handlungen, Duldungen oder Unterlassungen gelten auch, soweit in Bundesgesetzen die Länder ermächtigt worden sind zu bestimmen, dass die landesrechtlichen Vorschriften über das Verwaltungszwangsverfahren anzuwenden sind oder an die Stelle von bundesrechtlichen Vorschriften treten können.

§ 95
Anwendung der Vollzugsvorschriften auf öffentlich-rechtliche Verträge

Auf öffentlich-rechtliche Verträge im Sinne des § 61 Absatz 1 des Landesverwaltungsverfahrensgesetzes sind die Vorschriften über die Erzwingung von Handlungen, Duldungen oder Unterlassungen entsprechend anzuwenden. Richtet sich die Vollstreckung wegen der Erzwingung einer Handlung, Duldung oder Unterlassung gegen einen Träger der öffentlichen Verwaltung, so ist § 172 der Verwaltungsgerichtsordnung entsprechend anzuwenden.

§ 96
Sonstige Anwendung der Vollzugsvorschriften

(1) Die Vorschriften über die Erzwingung von Handlungen, Duldungen oder Unterlassungen gelten entsprechend
1. für die Vollstreckung aus gerichtlichen Entscheidungen, die nach gesetzlicher Vorschrift von einer Verwaltungsbehörde zu vollziehen sind, und
2. wenn ein Gericht eine Vollstreckungsbehörde zur Ausführung einer Vollstreckung in Anspruch nimmt und die Vollstreckung nach landesrechtlichen Bestimmungen durchzuführen ist.

(2) In den Fällen des Absatzes 1 bedarf es einer Androhung der Zwangsmittel (§ 87) nicht.

§ 97
Maßnahmen gegen Tiere

Bei Maßnahmen gegen Tiere aufgrund der Vorschriften dieses Gesetzes sind die für Sachen geltenden Vorschriften entsprechend anzuwenden. Hierbei haben die Behörden die Verantwortung des Menschen für das Tier zu berücksichtigen.

Unterabschnitt 4
Einschränkung von Grundrechten und Rechtsbehelfe (§§ 98 - 100)

§ 98
Einschränkung von Grundrechten

Für Maßnahmen, die nach den Vorschriften der Unterabschnitte 1 bis 3 getroffen werden können, werden das Recht auf körperliche Unversehrtheit (Artikel 2 Absatz 2 Satz 1 des Grundgesetzes), das Recht der Freiheit der Person (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes) und das Recht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) eingeschränkt.

§ 99
Rechtsbehelfe

(1) Die Rechtsmittel und sonstigen Rechtsbehelfe gegen Vollzugsmaßnahmen richten sich, soweit durch Gesetz nicht ausdrücklich etwas anderes bestimmt ist, nach den Vorschriften über die allgemeine Verwaltungsgerichtsbarkeit. Sie haben keine aufschiebende Wirkung.

(2) Einwendungen gegen den dem Vollzug zugrundeliegenden Verwaltungsakt sind außerhalb des Vollzugsverfahrens mit den dafür zugelassenen Rechtsbehelfen zu verfolgen.

§ 100
(aufgehoben)

Unterabschnitt 5
Ausübung unmittelbaren Zwangs (§§ 101 - 113)

§ 101
Rechtliche Grundlagen

(1) Lassen Rechtsvorschriften die Anwendung unmittelbaren Zwangs zu, so gelten für die Art und Weise der Ausübung des unmittelbaren Zwangs die §§ 102 bis 112 und, soweit sich aus ihnen nichts Abweichendes ergibt, die übrigen Vorschriften dieses Gesetzes.

(2) Das Recht zur Verteidigung in den Fällen der Notwehr und des Notstandes bleibt unberührt.

§ 102
Begriffsbestimmung

(1) Unmittelbarer Zwang ist die Einwirkung auf Personen oder Sachen durch
1. körperliche Gewalt,
2. Hilfsmittel der körperlichen Gewalt,
3. Waffen.

(2) Körperliche Gewalt ist jede unmittelbare körperliche Einwirkung auf Personen oder Sachen.

(3) Hilfsmittel der körperlichen Gewalt sind insbesondere Fesseln, Wasserwerfer, technische Sperren, Diensthunde, Dienstpferde, Dienstfahrzeuge, Reizstoffe und Sprengmittel; Sprengmittel dürfen nicht gegen Personen angewandt werden.

(4) Als Waffen sind nur Schlagstöcke, Distanz-Elektroimpulsgeräte, Pistolen, Revolver, Gewehre und Maschinenpistolen zugelassen.

§ 103
Vollzugsbeamtinnen und Vollzugsbeamte

(1) Unmittelbarer Zwang darf nur durch Vollzugsbeamtinnen und Vollzugsbeamte ausgeübt werden.

(2) Vollzugsbeamtinnen und Vollzugsbeamte sind
1. Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte und
2. andere Beamtinnen und Beamte und sonstige Bedienstete, die durch Rechtsverordnung der Landesregierung ermächtigt sind, unmittelbaren Zwang auszuüben.

(3) Vollzugsbeamtinnen und Vollzugsbeamte der Ämter und amtsfreien Gemeinden bedürfen der Bestätigung der Kreisordnungsbehörde.

§ 104
Handeln auf Anordnung

(1) Vollzugsbeamtinnen und Vollzugsbeamte sind verpflichtet, unmittelbaren Zwang anzuwenden, der im Vollzugsdienst von ihrer oder ihrem Vorgesetzten oder einer sonst dazu befugten Person angeordnet wird. Dies gilt nicht, wenn die Anordnung die Menschenwürde verletzt oder nicht zu dienstlichen Zwecken erteilt worden ist.

(2) Eine Anordnung darf nicht befolgt werden, wenn dadurch eine Straftat begangen würde. Befolgen Vollzugsbeamtinnen und Vollzugsbeamte die Anordnung trotzdem, so trifft sie eine Schuld nur, wenn sie erkennen oder wenn es nach den ihnen bekannten Umständen offensichtlich ist, dass dadurch eine Straftat begangen wird.

(3) Bedenken gegen die Rechtmäßigkeit der Anordnung haben Vollzugsbeamtinnen und Vollzugsbeamte der oder dem Anordnenden gegenüber vorzubringen, soweit das nach den Umständen möglich ist.

(4) § 36 Absatz 2 und 3 des Beamtenstatusgesetzes ist nicht anzuwenden.

§ 105
Hilfeleistung für Verletzte

Wird unmittelbarer Zwang angewendet, ist Verletzten, soweit es nötig ist und die Lage es zulässt, Beistand zu leisten und ärztliche Hilfe zu verschaffen.

§ 106
Fesselung von Personen

Eine Person, die nach diesem Gesetz oder anderen Gesetzen festgehalten wird, darf gefesselt werden,
1. wenn Tatsachen die Annahme rechtfertigen, dass sie
   a) andere Personen angreifen oder Sachen von nicht geringem Wert beschädigen wird,
   b) fliehen wird oder befreit werden soll oder
   c) sich töten oder erheblich verletzen wird, oder
2. wenn sie Widerstand leistet.

§ 107
Zum Gebrauch von Schusswaffen Berechtigte

Die Befugnis zum Gebrauch von Schusswaffen steht ausschließlich zu
1. den Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten,
2. den Beamtinnen und Beamten sowie anderen Bediensteten der Landesforstverwaltung, die im Forst- und Jagdschutz verwendet werden, sowie bestätigten Jagdaufsehern (§ 25 Landesjagdgesetz), sofern sie Berufsjäger oder forstlich ausgebildet sind,
3. den Beamtinnen und Beamten sowie anderen Bediensteten der Gerichte und Behörden der Justizverwaltung, die mit Sicherungs- und Vollzugsaufgaben betraut sind, jedoch nicht den Gerichtsvollzieherinnen und Gerichtsvollziehern.

§ 108
Allgemeine Vorschriften für den Schusswaffengebrauch

(1) Schusswaffen dürfen nur gebraucht werden, wenn andere Maßnahmen des unmittelbaren Zwangs erfolglos angewendet worden sind oder offensichtlich keinen Erfolg versprechen.

(2) Der Schusswaffengebrauch ist unzulässig, wenn Unbeteiligte gefährdet werden. Dies gilt nicht, wenn der Schusswaffengebrauch das einzige Mittel zur Abwehr einer gegenwärtigen Lebensgefahr ist.

(3) Gegen Personen, die tatsächlich oder dem äußeren Eindruck nach noch nicht 14 Jahre alt sind, dürfen Schusswaffen nicht gebraucht werden. Das gilt nicht, wenn der Schusswaffengebrauch das einzige Mittel zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben ist.

§ 109
Schusswaffengebrauch gegen Personen

(1) Gegen Personen ist der Gebrauch von Schusswaffen nur zulässig, um diese angriffs- oder fluchtunfähig zu machen und soweit der Zweck nicht durch Schusswaffengebrauch gegen Sachen erreicht werden kann. Ein Schuss, der mit an Sicherheit grenzender Wahrscheinlichkeit tödlich wirken wird, ist durch Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte nur zulässig, wenn er das einzige Mittel zur Abwehr einer gegenwärtigen Lebensgefahr oder der gegenwärtigen Gefahr einer schwerwiegenden Verletzung der körperlichen Unversehrtheit ist.

(2) Schusswaffen dürfen gegen Personen nur gebraucht werden,
1. um eine gegenwärtige Gefahr für Leib oder Leben abzuwehren,
2. um die unmittelbar bevorstehende Begehung oder Fortsetzung eines Verbrechens oder eines Vergehens unter Anwendung oder Mitführung von Schusswaffen oder Explosivmitteln zu verhindern,
3. um eine Person anzuhalten, die sich der Festnahme oder Identitätsfeststellung durch Flucht zu entziehen versucht, wenn sie
   a) eines Verbrechens dringend verdächtig ist oder
   b) eines Vergehens dringend verdächtig ist und tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass sie von einer Schusswaffe oder einem Explosivmittel Gebrauch machen werde,

4. zur Vereitelung der Flucht oder zur Ergreifung einer Person, die in amtlichem Gewahrsam zu halten oder ihm zuzuführen ist
   a) aufgrund richterlicher Entscheidung wegen eines Verbrechens oder aufgrund des dringenden Verdachts eines Verbrechens oder
   b) aufgrund richterlicher Entscheidung wegen eines Vergehens oder aufgrund des dringenden Verdachts eines Vergehens, sofern tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass sie von einer Schusswaffe oder einem Explosivmittel Gebrauch machen wird, oder
5. um die gewaltsame Befreiung einer Person aus amtlichem Gewahrsam zu verhindern.

(3) Schusswaffen dürfen nach Absatz 2 Nummer 4 nicht gebraucht werden, wenn es sich um den Vollzug eines Jugendarrestes oder eines Strafarrestes handelt oder wenn die Flucht aus einer offenen Anstalt verhindert werden soll.

§ 110
Schusswaffengebrauch gegen Personen in einer Menschenmenge

(1) Schusswaffen dürfen gegen Personen in einer Menschenmenge nur gebraucht werden, wenn von ihr oder aus ihr heraus schwerwiegende Gewalttaten begangen werden oder unmittelbar bevorstehen und andere Maßnahmen keinen Erfolg versprechen.

(2) Wer sich aus einer solchen Menschenmenge nach wiederholter Androhung des Schusswaffengebrauches nicht entfernt, obwohl ihm das möglich ist, ist nicht unbeteiligte Person im Sinne des § 108 Absatz 2.

§ 111
Warnung

(1) Bevor unmittelbarer Zwang gegen Personen angewendet wird, ist zu warnen. Von der Warnung kann abgesehen werden, wenn die Umstände sie nicht zulassen, insbesondere wenn die sofortige Anwendung des Zwangsmittels zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr notwendig ist. Als Warnung vor dem Schusswaffengebrauch gilt auch die Abgabe eines Warnschusses.

(2) Schusswaffen dürfen nur dann ohne Warnung gebraucht werden, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben erforderlich ist.

(3) Gegenüber einer Menschenmenge ist vor Anwendung unmittelbaren Zwangs möglichst so rechtzeitig zu warnen, dass sich Unbeteiligte noch entfernen können. Vor Gebrauch von Schusswaffen gegen Personen in einer Menschenmenge ist stets zu warnen; die Warnung ist vor dem Gebrauch zu wiederholen. Bei Gebrauch von technischen Sperren und Einsatz von Dienstpferden kann von der Warnung abgesehen werden.

§ 112
Verwaltungsvorschriften über die Anwendung unmittelbaren Zwangs

Die allgemeinen Verwaltungsvorschriften über die Anwendung unmittelbaren Zwangs erlässt das Ministerium für Inneres und Europa für seinen Geschäftsbereich; die anderen Ministerien erlassen sie für ihren Geschäftsbereich im Einvernehmen mit dem Ministerium für Inneres und Europa.

§ 113
Einschränkung von Grundrechten

Für Maßnahmen, die nach Vorschriften dieses Unterabschnitts getroffen werden, werden das Recht auf Leben und körperliche Unversehrtheit (Artikel 2 Absatz 2 Satz 1 des Grundgesetzes), das Recht der Freiheit der Person (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes) und das Recht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) eingeschränkt.

Abschnitt 9
Kosten (§ 114)

§ 114
Kosten, Ermächtigung zum Erlass von Rechtsverordnungen

(1) Für Amtshandlungen nach diesem Gesetz und den zur Durchführung dieses Gesetzes erlassenen Rechtsverordnungen werden Kosten (Gebühren und Auslagen) erhoben.

(2) Die obersten Landesbehörden werden ermächtigt, jeweils für ihren Zuständigkeitsbereich durch Rechtsverordnung nach § 2 des Landesverwaltungskostengesetzes die einzelnen Amtshandlungen, für die die Verwaltungsgebühren erhoben werden, die Gebührensätze, die Entstehung der Gebührenschuld sowie Art und Umfang der zu erstattenden Auslagen zu bestimmen. Das Landesverwaltungskostengesetz findet Anwendung, soweit dieses Gesetz keine abweichenden Vorschriften enthält. Durch Rechtsverordnung kann von den §§ 10, 11 Absatz 1, 13 Absatz 1, 15 Absatz 1 und 2 sowie § 16 des Landesverwaltungskostengesetzes abgewichen werden.

(3) Die Kosten trägt die pflichtige Person, im Fall der unmittelbaren Ausführung einer Maßnahme (§ 70a) die oder der nach den §§ 69 oder 70 Verantwortliche.

Abschnitt 10
Schlussbestimmungen (§§ 115, 116)

§ 115
Ausnahme- und Übergangsvorschriften

(1) § 46g Absatz 1 und 2 gelten nicht, soweit eine Kennzeichnung tatsächlich nicht möglich ist oder solange eine Kennzeichnung nach dem Stand der Technik nicht möglich ist.

(2) Abweichend von § 46g Absatz 2 ist eine Weiterverarbeitung oder Übermittlung personenbezogener Daten auch zulässig nach den Bestimmungen der für die Daten am … [*Tag vor dem Inkrafttreten des Gesetzes*] jeweils geltenden Verfahrensbeschreibung in der bis zum … [*Tag vor dem Inkrafttreten des Gesetzes*] geltenden Fassung. Satz 1 gilt für personenbezogene Daten,

a) die mit Ablauf des … [*Tag vor dem Inkrafttreten des Gesetzes*] keine Kennzeichnung nach § 46g Absatz 1 aufweisen,
b) die ab dem … [*Tag des Inkrafttretens des Gesetzes*] gespeichert werden, soweit eine Kennzeichnung tatsächlich nicht möglich ist oder solange eine Kennzeichnung nach dem Stand der Technik nicht möglich ist.

(3) Protokollierungen nach § 46e müssen bei vor dem 6. Mai 2016 eingerichteten, automatisierten Verfahren erst bis zum 6. Mai 2023 erfolgen, wenn andernfalls ein unverhältnismäßiger Aufwand entstünde. Satz 1 gilt nicht für die Protokollierungen bei verdeckten und eingriffsintensiven Maßnahmen nach § 46f und bei der Übermittlung personenbezogener Daten an Drittstaaten und weitere zwischen- und überstaatliche Stellen nach den §§ 39d bis 39h sowie nach der Verordnung (EU) 2016/679. Die Anwendung von Satz 1 ist zu begründen, zu dokumentieren und dem Ministerium für Inneres und Europa mitzuteilen. Die oder der Landesbeauftragte für den Datenschutz ist über das betroffene automatisierte Verfahren und die Gründe für die Anwendung von Satz 1 zu unterrichten.

(4) Die Frist für Prüfungen der oder des Landesbeauftragten für den Datenschutz nach § 48b Absatz 6 beginnt erstmalig mit dem 1. Januar 2020.

(5) Das erste berichtspflichtige Kalenderjahr gemäß § 48h Absatz 1 Satz 2 ist das Jahr 2020. Bis zum 31. Dezember 2019 finden § 34 Absatz 7, auch in Verbindung mit § 34a Absatz 9 und § 34b Absatz 9 des Sicherheits- und Ordnungsgesetzes in der am … [*Tag vor dem Inkrafttreten des Gesetzes*] geltenden Fassung Anwendung.

§ 116
Evaluierungspflicht

Die Landesregierung berichtet dem Landtag bis zum 31. Dezember 2024 über die erzielten Wirkungen der mit dem Inkrafttreten dieses Gesetzes am … [*Tag des Inkrafttretens des Gesetzes*] vorgenommenen Änderungen.

Artikel 2
Änderung des Brandschutz- und Hilfeleistungsgesetzes M-V

Das Brandschutz- und Hilfeleistungsgesetz M-V in der Fassung der Bekanntmachung vom 21. Dezember 2015 (GVOBl. M-V S. 612; 2016 S. 20) wird wie folgt geändert:

1. § 28 Absatz 1 wird wie folgt gefasst:

   „(1) Für die Verarbeitung personenbezogener Daten gelten die Bestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, L 314 vom 22.11.2016, S. 72, L 127 vom 23.5.2018, S. 2) und des Landesdatenschutzgesetzes nach Maßgabe der folgenden Vorschriften.“

2. In den §§ 14 Absatz 2 Satz 3, 17 Absatz 2 Satz 1 und in § 32 Absatz 1 und 2 wird jeweils das Wort „Sport“ durch das Wort „Europa“ ersetzt.

Artikel 3
Änderung des Landeskatastrophenschutzgesetzes

Das Landeskatastrophenschutzgesetz in der Fassung der Bekanntmachung vom 15. Juli 2016 (GVOBl. M-V S. 611, 793) wird wie folgt geändert:

1. In den §§ 3 Absatz 1 Nummer 1, 5 Absatz 4, 6 Absatz 1, 15 Absatz 5 Satz 7, 24a Satz 2, 25 Absatz 5 Satz 2 und in § 33 wird jeweils das Wort „Sport“ durch das Wort „Europa“ ersetzt.

2. § 35 wird wie folgt geändert:

   a) Absatz 1 wird wie folgt gefasst:

      „(1) Für die Verarbeitung personenbezogener Daten gelten die Bestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, L 314 vom 22.11.2016, S. 72, L 127 vom 23.5.2018, S. 2) und des Landesdatenschutzgesetzes nach Maßgabe der folgenden Vorschriften.“

   b) Die bisherigen Absätze 1 bis 3 werden die Absätze 2 bis 4.

3. § 38 wird wie folgt gefasst:

„Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Datenübermittlung durch automatisierten Abruf, tragen die Empfänger die Verantwortung für die Rechtmäßigkeit des Abrufs. Die Empfänger dürfen die übermittelten personenbezogenen Daten nur zu dem Zweck verarbeiten, zu dessen Erfüllung sie ihnen übermittelt worden sind. Die Verarbeitung zu einem anderen Zweck ist neben den in § 4 Absatz 2 des Landesdatenschutzgesetzes genannten Gründen zulässig, soweit die erneute Erhebung der personenbezogenen Daten zu diesem Zweck mit vergleichbaren Mitteln zulässig wäre.“

Artikel 4
Einschränkung von Grundrechten

Durch Artikel 1 werden das Recht auf körperliche Unversehrtheit (Artikel 2 Absatz 2 Satz 1 des Grundgesetzes), das Recht der Freiheit der Person (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes), das Recht auf Versammlungsfreiheit (Artikel 8 Absatz 1 des Grundgesetzes), das Recht auf Wahrung des Fernmeldegeheimnisses (Artikel 10 Absatz 1 des Grundgesetzes), das Recht der Freizügigkeit (Artikel 11 des Grundgesetzes) und das Recht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) eingeschränkt.

Artikel 5
Inkrafttreten, Außerkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft. Gleichzeitig tritt das Sicherheits- und Ordnungsgesetz in der Fassung der Bekanntmachung vom 9. Mai 2011 (GVOBl. M-V S. 246), das zuletzt durch Artikel 1 des Gesetzes vom 22. März 2018 (GVOBl. M-V S. 114) geändert worden ist, außer Kraft.

Begründung:

I. Allgemeine Begründung

Zur Umsetzung des sogenannten EU-Datenschutzpakets und in Anbetracht der hierzu getroffenen Festlegungen in den Nummern 434 und 379 in der bestehenden Koalitionsvereinbarung 2016 - 2021 sowie zur Schaffung eines effektiven und zeitgemäßen Gefahrenabwehrrechts werden mit dem Gesetz folgende Änderungen vorgenommen:

Umsetzung des EU-Datenschutzpakets:

Seit dem 25. Mai 2016 gilt die „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ (Datenschutz-Grundverordnung, im Folgenden Verordnung (EU) 2016/679 genannt) als unmittelbar anzuwendendes Recht. Ziel dieser Verordnung ist ein unionsweites gleichwertiges Schutzniveau für die Rechte und die Freiheiten von natürlichen Personen bei der Verarbeitung von Daten (Erwägungsgründe 10 und 13 der Verordnung). Die Verordnung (EU) 2016/679 regelt das allgemeine und bereichsspezifische Datenschutzrecht jedoch nicht abschließend. So enthält sie sowohl an die Mitgliedstaaten adressierte Regelungsaufträge als auch Öffnungsklauseln und die Möglichkeit zur Normierung spezifischer Bestimmungen und zur Beschränkung ihrer Vorschriften. Insoweit haben der Bund und auch die Länder ihre allgemeinen und fachspezifischen Datenschutzvorschriften anzupassen.

Vor diesem Hintergrund wurde im Land Mecklenburg-Vorpommern bereits das Landesdatenschutzgesetz angepasst (siehe GVOBl. M-V 2018, Seite 193). Die Verordnung (EU) 2016/679 führte aufgrund ihrer grundsätzlich unmittelbaren Geltung (siehe Artikel 288 des Vertrages über die Arbeitsweise der Europäischen Union) zu grundlegenden strukturellen Änderungen beim Landesdatenschutzrecht. Mit der Neufassung des Landesdatenschutzgesetzes wird der Systemwechsel deutlich gemacht. Es trifft künftig nur noch ergänzende Regelungen zur Verordnung (EU) 2016/679.

Unter Berücksichtigung der unmittelbar geltenden Vorschriften der Verordnung (EU) 2016/679 und der diese ergänzenden Regelungen im neu gefassten Landesdatenschutzgesetz erfolgt mit diesem Gesetz die - bereichsspezifische - Anpassung der datenschutzrechtlichen Bestimmungen in folgenden Gesetzen:

- „Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern“ (Sicherheits- und Ordnungsgesetz - SOG M-V),
- „Gesetz über den Brandschutz und die Technischen Hilfeleistungen durch die Feuerwehren für Mecklenburg-Vorpommern“ (Brandschutz- und Hilfeleistungsgesetz M-V)
- „Gesetz über den Katastrophenschutz in Mecklenburg-Vorpommern“ (Landeskatastrophenschutzgesetz).

Zum anderen ist am 5. Mai 2016 die „Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates“ (zukünftig bezeichnet als Richtlinie (EU) 2016/680) in Kraft getreten. Sie war nach deren Artikel 63 bis zum 6. Mai 2018 in den Mitgliedstaaten verpflichtend umzusetzen. Mit Blick auf den Anwendungsbereich und Regelungsinhalt der Richtlinie besteht in den Bundesländern insbesondere ein zwingender Umsetzungsbedarf in den Polizei- beziehungsweise Sicherheits- und Ordnungsgesetzen der Länder.

Die notwendigen Anpassungen aufgrund der Verordnung (EU) 2016/679 und die zwingend gebotene Umsetzung der Richtlinie (EU) 2016/680 im Gefahrenabwehrrecht führen zu umfangreichen Änderungen im SOG M-V, sodass eine Neufassung des Gesetzes erforderlich erscheint. Mit der Neufassung wird im Gesetz unter anderem eine Anpassung an den Sprachgebrauch in den genannten EU-Vorschriften vorgenommen (§ 3) und ausdrücklich bestimmt, dass auch die Verhütung von Ordnungswidrigkeiten von der Gefahrenabwehr umfasst ist (§ 4). Darüber hinaus erfolgt eine umfangreiche datenschutzrechtliche Anpassung und Ergänzung der Regelungen unter Abschnitt 3 „Verarbeitung personenbezogener Daten“ (§§ 25 bis 49). Es werden in diesem Abschnitt zusätzliche Unterabschnitte eingeführt, die insbesondere zur Anpassung an das europäische Datenschutzrecht detaillierte Vorschriften zur Einwilligung (§ 26), Datenübermittlung (§§ 39ff), zu den Pflichten der im Sinne des Datenschutzrechts verantwortlichen Stelle sowie des Auftragsverarbeiters (§§ 45 bis 46k), zu den Rechten der betroffenen Person (§§ 47 bis 48a) und zum Bereich der datenschutzaufsichtlichen Kontrolle (§§ 48b bis 48h) enthalten. Zudem wird der § 76 zur Regelung der Schadensersatzansprüche und der Entschädigung aus der Verarbeitung von personenbezogenen Daten überarbeitet.

Es wird - soweit wie rechtlich zulässig und möglich - eine direkte Regelung der im Bereich des Gefahrenabwehrrechtes zu beachtenden datenschutzrechtlichen Bestimmungen im SOG M-V selbst vorgenommen. Dabei wird insbesondere von der Klausel in Artikel 6 Absatz 2 der Verordnung (EU) 2016/679 zur Schaffung spezifischer Bestimmungen Gebrauch gemacht. Diese Regelung sieht vor, dass die Mitgliedstaaten spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften der Verordnung (EU) 2016/679 in Bezug auf die Verarbeitung für die Wahrnehmung einer Aufgabe in Ausübung öffentlicher Gewalt oder zur Erfüllung einer rechtlichen Verpflichtung beibehalten oder einführen können. Dies bedeutet zwar einerseits einen größeren gesetzgeberischen Aufwand, anderseits wird den Gesetzesanwendern damit aber weitestgehend ein ständiges „Hineinspringen“ in verschiedene datenschutzrechtliche Regelungswerke erspart und so die bessere praktische Handhabung gewährleistet. Auch stellt dieses Vorgehen eine möglichst einheitliche Verfahrensweise bei Polizei und Ordnungsbehörden im Land Mecklenburg-Vorpommern mit Blick auf die notwendige Zusammenarbeit im Bereich der Gefahrenabwehr sicher.

Soweit Regelungen aus der Verordnung (EU) 2016/679 in das Gesetz übernommen werden, so erfolgte dies in Ansehung des Erwägungsgrundes 8 dieser Verordnung. Danach sind Wiederholungen von Regelungen der Verordnung (EU) 2016/679 im nationalen Recht insoweit möglich, als im Falle von Präzisierungen oder Einschränkungen von Regelungen der Verordnung (EU) 2016/679 durch das nationale Recht diese erforderlich sind, um die Kohärenz zu wahren und die Vorschriften des nationalen Rechts für die Personen, für die sie gelten, verständlicher zu machen. Das Wiederholungsverbot soll verhindern, dass die unmittelbare Geltung einer Verordnung verschleiert wird, weil die Normadressaten über den wahren Urheber des Rechtsaktes oder die Jurisdiktion des Europäischen Gerichtshofes im Unklaren gelassen werden (EuGH, Rs. C-34/73, Variola, Randnummern 9 ff; EuGH, Rs. C-94/77, Zerbone, Randnummern 22, 27).

Im Übrigen wird der Gesetzesanwender mit § 25 Absatz 5 im SOG M-V ausdrücklich darauf hingewiesen, dass das Landesdatenschutzgesetz ergänzend Anwendung findet, soweit das SOG M-V nichts Besonderes bestimmt.

Zur Umsetzung des EU-Datenschutzpakets im SOG M-V wird im Weiteren auf die ausführliche Begründung zu Artikel 1, dort insbesondere zu § 25, verwiesen.

Hinsichtlich des Brandschutz- und Hilfeleistungsgesetzes M-V und des Landeskatastrophenschutzgesetzes bedarf es Anpassungen aufgrund der unmittelbaren Geltung der Verordnung (EU) 2016/679 und der ergänzenden Bestimmungen im Landesdatenschutzgesetz. Diesbezüglich wird auf die Begründung zu Artikel 2 und 3 verwiesen.

Änderungen im SOG M-V aufgrund des Urteils des Bundesverfassungsgerichtes vom 20. April 2016

Das Bundesverfassungsgericht hat in seinem Urteil vom 20. April 2016 (Aktenzeichen 1 BvR 966/09) entschieden, dass die Ermächtigung des Bundeskriminalamtes zum Einsatz von heimlichen Überwachungsmaßnahmen zur Abwehr von Gefahren des internationalen Terrorismus zwar im Grundsatz mit den Grundrechten vereinbar ist, die derzeitige Ausgestaltung von Befugnissen aber in verschiedener Hinsicht dem Verhältnismäßigkeitsgrundsatz nicht genügt. Die Entscheidung betrifft, eine lange Rechtsprechung zusammenführend, sowohl die Voraussetzungen für die Durchführung solcher Maßnahmen als auch die Frage der Übermittlung der Daten zu anderen Zwecken an dritte Behörden. Die Verhältnismäßigkeitsanforderungen für eine zweckändernde Datenverwendung orientieren sich gemäß den Ausführungen des Gerichtes am Grundsatz der hypothetischen Datenneuerhebung. Danach muss die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Ferner hat sich das Bundesverfassungsgericht in der Entscheidung erstmals auch mit den Anforderungen an eine Weiterleitung von Daten an ausländische Sicherheitsbehörden befasst.

Das Gericht stellte zudem fest, dass es zum Teil an flankierenden rechtsstaatlichen Absicherungen, insbesondere zum Schutz des Kernbereichs privater Lebensgestaltung, oder zur Gewährleistung von Transparenz, individuellem Rechtsschutz und aufsichtlicher Kontrolle fehlt. Auch die Vorschriften zur Übermittlung von Daten sind - sowohl hinsichtlich inländischer als auch hinsichtlich ausländischer Behörden - an etlichen Stellen als nicht hinreichend begrenzt beurteilt worden. Unter Berufung auf den Verhältnismäßigkeitsgrundsatz fordert das Bundesverfassungsgericht zudem eine Ausweitung des Richtervorbehaltes. So bedürfen etwa auch die Anordnung einer längerfristigen Observation, die Aufzeichnung nicht öffentlicher Gespräche und der Einsatz von Vertrauenspersonen einer richterlichen Entscheidung.

Die Entscheidung des Bundesverfassungsgerichtes bezieht sich zwar auf das BKAG. Seine grundsätzlichen Ausführungen treffen jedoch ebenso auf Ermächtigungsnormen in den Gefahrenabwehrgesetzen der Länder zu, die eingriffsintensive beziehungsweise verdeckte Maßnahmen enthalten. Insofern sind die bundesverfassungsgerichtlichen Vorgaben aus der Entscheidung vom 20. April 2016 auch im SOG M-V nachzuvollziehen.

Deswegen wird im SOG M-V im Wesentlichen der Abschnitt 3 (§§ 25 bis 49) angepasst. Insbesondere wird dort eine explizite und umfassende Regelungslage zum Kernbereichsschutz (§ 26a) und zum Schutz von Amts- und Berufsgeheimnisträgern (§ 26b) geschaffen. Die Eingriffsvoraussetzungen verdeckter Maßnahmen werden insgesamt überarbeitet und teilweise ergänzt. Die hierzu bestehenden Anordnungsvorbehalte haben Änderungen erfahren. Vorgegeben wird hinsichtlich gesetzlich normierter Anordnungen nunmehr, welche Inhalte behördliche Anträge an das Gericht aufweisen müssen und welche Inhalte gerichtliche oder behördliche Anordnungen mindestens zu enthalten haben. Insbesondere werden zu den bestehenden verdeckten Maßnahmen nach § 33 und zur Rasterfahndung nach § 44 weitere Richtervorbehalte eingefügt.

Zugleich werden mit Blick auf den Grundsatz der hypothetischen Datenneuerhebung in Bezug auf die Datenerhebungsbefugnisse nach dem SOG M-V verstärkte Anforderungen unter anderem an die Zweckbindung und die weitere Verarbeitung von Daten, die durch eingriffsintensive Maßnahmen gewonnen wurden, geregelt. Insbesondere sind in diesem Zuge auch die Bestimmungen zur Datenübermittlung (§§ 39 bis 39h) neu ausgestaltet worden. Zudem werden weitere Vorschriften zur Information und Benachrichtigung der Personen, die von den Maßnahmen betroffen sind oder waren (§§ 46 bis 46c), zur Dokumentation (§ 46d) und Protokollierung (§§ 46e und 46f) behördlichen Handelns sowie zur Kennzeichnung (§ 46g) von Daten geschaffen.

Ferner werden die Vorschriften zu den Berichts- und Unterrichtungspflichten gegenüber dem Landtag und seinem SOG-Gremium sowie der Öffentlichkeit bei eingriffsintensiven und verdeckten Maßnahmen angepasst.

Mit § 115 wird hierzu und auch zur Kennzeichnung von Daten und zur Protokollierung eine Übergangsregelung geschaffen, um nach Inkrafttreten des Gesetzes der Praxis die notwendige Umsetzungszeit einzuräumen.

Ergänzung des SOG M-V um neue Befugnisnormen und klarstellende Regelungen

In Anbetracht der aktuellen Sicherheitslage müssen die Länder effiziente Wege finden, um der ihnen obliegende Aufgabe der Gefahrenabwehr nachkommen zu können. Der Handlungsspielraum der Ordnungsbehörden und Polizei wird dabei von den Gefahrenabwehrgesetzen der Länder bestimmt. Die darin enthaltenen Befugnisse sind das wesentliche Instrumentarium, Gefahren abzuwehren und Rechtsgüter zu schützen und so die öffentliche Sicherheit und Ordnung im Land Mecklenburg-Vorpommern zu gewährleisten.

Eine Sichtung der geltenden präventiv-polizeilichen Länderbefugnisse lässt deutlich werden, wie unterschiedlich die Landesgesetzgeber technische, gesellschaftliche und sicherheitspolitische Entwicklungen in Bezug auf die Schaffung gefahrenabwehrrechtlicher Befugnisse aufgegriffen haben. Da Gefahren nicht an Ländergrenzen halt machen, muss es in der heutigen Zeit, die von Mobilität, grenzenloser Kommunikation und Netzwerken geprägt ist, mehr denn je das Ziel sein, mit harmonisierten gefahrenabwehrrechtlichen Regelungen in allen Bundesländern in vergleichbarem und hohen Maße Sicherheit und Ordnung gewährleisten zu können. In Anbetracht dessen beschloss die Innenministerkonferenz bereits im Juni 2017, dass durch gemeinsame gesetzliche Standards im Gefahrenabwehrrecht der Länder eine effektive Erhöhung der öffentlichen Sicherheit erreicht werden soll. Vor diesem Hintergrund wurde auch eine länderübergreifende Arbeitsgruppe zur Erarbeitung eines Musterpolizeigesetzentwurfs eingerichtet. Die Erarbeitung des Musterentwurfs benötigt jedoch Zeit, sodass er nicht kurzfristig zur Verfügung stehen wird.

Die Länder sind aber jetzt - im Zuge der notwendigen Harmonisierung mit dem EU-Datenschutzpaket (Anpassung an die Verordnung (EU) 2016/679 sowie Umsetzung der Richtlinie (EU) 2016/680) und der Anpassungen aufgrund des vorgenannten Urteils des Bundesverfassungsgerichtes vom 20. April 2016 zum Bundeskriminalamtgesetz - gehalten, mit Blick auf die aktuelle Sicherheitslage und auf den Stand der technischen Entwicklung auch gesetzliche Befugnisse anzupassen oder neu im Gefahrenabwehrrecht zu verankern. Nur so ist eine effektive Gefahrenabwehr möglich.

In diesem Zuge ist auch zu berücksichtigen, dass alle Polizei- beziehungsweise Sicherheits- und Ordnungsgesetze bisher ganz wesentlich darauf ausgerichtet waren, Eingriffstatbestände zu formulieren, die dem tradierten Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprachen. Sie beschränken sich demnach zum Beispiel bei den Maßnahmen in Bezug auf die Überwachung der Telekommunikation oder die Abfrage bestimmter Telekommunikationsdaten darauf, Eingriffe (erst) im Stadium einer konkreten Gefahr zuzulassen. Ein Land, das sich terroristischen Bedrohungen ausgesetzt sieht, handelt in diesem Stadium allerdings zu spät. So hat auch das Bundesverfassungsgericht in der oben angeführten Entscheidung zum Bundeskriminalamtgesetz unter den Randnummern 96 bis 100 unter anderem ausgeführt:

„[…] Straftaten mit dem Gepräge des Terrorismus […] zielen auf eine Destabilisierung des Gemeinwesens und umfassen hierbei in rücksichtsloser Instrumentalisierung anderer Menschen Angriffe auf Leib und Leben beliebiger Dritter. Sie richten sich gegen die Grundpfeiler der verfassungsrechtlichen Ordnung und das Gemeinwesen als Ganzes. Die Bereitstellung von wirksamen Aufklärungsmitteln zu ihrer Abwehr ist ein legitimes Ziel und für die demokratische und freiheitliche Ordnung von großem Gewicht. […] Danach müssen die Überwachungs- und Ermittlungsbefugnisse mit Blick auf das Eingriffsgewicht angemessen ausgestaltet sein. Es ist Aufgabe des Gesetzgebers, einen Ausgleich zwischen der Schwere der mit den hier zur Prüfung stehenden Eingriffen in die Grundrechte potenziell Betroffener auf der einen Seite und der Pflicht des Staates zum Schutz der Grundrechte auf der anderen Seite zu schaffen.

1. *Der Gesetzgeber hat dabei auf der einen Seite das Eingriffsgewicht der durch die angegriffenen Vorschriften erlaubten Maßnahmen in Rechnung zu stellen. […]*
2. *Auf der anderen Seite hat der Gesetzgeber einen wirksamen Schutz der Grundrechte und Rechtsgüter der Bürgerinnen und Bürger zu sichern. Für die verfassungsrechtliche Prüfung der Angemessenheit ist zu berücksichtigen, dass die verfassungsmäßige Ordnung, der Bestand und die Sicherheit des Bundes und der Länder sowie Leib, Leben und Freiheit der Person Schutzgüter von hohem verfassungsrechtlichem Gewicht sind. Dementsprechend hat das Bundesverfassungsgericht hervorgehoben, dass die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die von ihm - unter Achtung von Würde und Eigenwert des Einzelnen - zu gewährleistende Sicherheit der Bevölkerung Verfassungswerte sind, die mit anderen hochwertigen Verfassungsgütern im gleichen Rang stehen. Es hat den Staat deshalb für verpflichtet erachtet, das Leben, die körperliche Unversehrtheit und die Freiheit des Einzelnen zu schützen, das heißt vor allem, auch vor rechtswidrigen Eingriffen von Seiten anderer zu bewahren […] .*“

Zusätzlich führt das Gericht unter der Randnummer 112 aus:

„[…] Der Gesetzgeber ist von Verfassungs wegen aber nicht von vornherein für jede Art der Aufgabenwahrnehmung auf die Schaffung von Eingriffstatbeständen beschränkt, die dem tradierten sicherheitsrechtlichen Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprechen. Vielmehr kann er die Grenzen für bestimmte Bereiche mit dem Ziel, schon der Straftatenverhütung auch weiterziehen, indem er die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert. […] In Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, können Überwachungsmaßnahmen auch dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird. Denkbar ist das etwa, wenn eine Person aus einem Ausbildungslager für Terroristen im Ausland in die Bundesrepublik Deutschland einreist.“

Damit können gerade im Vorfeld terroristischer Straftaten Überwachungsmaßnahmen auch dann erlaubt werden, wenn keine konkrete Gefahr vorliegt, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie terroristische Straftaten in überschaubarer Zukunft begehen wird.

Dies führt zur maßgeblichen Schlussfolgerung für den gesetzgeberischen Handlungsbedarf, dass auch bestimmte bestehende Befugnisse der Polizeien der Länder dahingehend überprüft werden müssen, inwieweit in diese neben dem Eingriffsanlass der konkreten Gefahr auch die drohende Begehung terroristischer Straftaten Eingang finden muss. Die diesbezügliche Anpassung der Gefahrenabwehrgesetze der Länder und auch des SOG M-V ist die Reaktion auf die zur Verfügung stehenden gesetzgeberischen Möglichkeiten unter Berücksichtigung der aktuellen Sicherheitslage.

Im SOG M-V wird daher in bestimmten Befugnissen - wie zum Beispiel zur Telekommunikationsüberwachung oder zur Wohnraumüberwachung - bei den Überwachungsanlässen zusätzlich auch die Gefahr der Begehung oder Teilnahme einer in § 67c definierten terroristischen Straftat aufgenommen. Insoweit wird sich der Anwendungsbereich einiger Befugnisse erweitern.

Zudem werden folgende Befugnisse neu beziehungsweise aus Gründen der Rechtssicherheit nun ausdrücklich im SOG M-V verankert:

- Eilkompetenz für Zollbedienstete in den Vollzugsbereichen der Zollverwaltung (§ 9),
- ausdrückliche Regelung zum Einsatz technischer Mittel zur Fertigung von Übersichtsaufnahmen/-aufzeichnungen im öffentlichen Raum zur Herstellung von Rechtssicherheit (§ 32 Absatz 1),
- polizeiliche Befugnis zur offenen Bildbeobachtung und Anfertigung von Bild- und Tonaufzeichnungen in den für die Durchführung der Gewahrsamnahme genutzten polizeilichen Räumen (§ 32 Absatz 9) sowie klarstellende Regelung zur Anfertigung von Bild- und Tonaufzeichnungen zur Suche nach Personen, deren Leben oder Gesundheit gefährdet ist (§ 32 Absatz 10),
- polizeiliche Befugnis mit Richtervorbehalt zum verdeckten Zugriff auf fremde informationstechnische Systeme über Kommunikationsnetze mittels einer Überwachungssoftware (sogenannte Online-Durchsuchungsbefugnis; § 33c),
- polizeiliche Befugnis mit Richtervorbehalt zur Ausleitung von Telekommunikationsinhalten vor der Verschlüsselung mittels spezieller Software, die auf dem Endgerät der betroffenen Person verdeckt installiert wird (sogenannte Quellen-TKÜ-Befugnis; § 33d Absatz 3),
- polizeiliche Befugnis mit Richtervorbehalt zur Beauskunftung von Nutzungsdaten nach dem Telemediengesetz (§ 33e) sowie eine polizeiliche Befugnis zur Beauskunftung von Bestandsdaten nach dem Telemediengesetz (§ 33h) zur Schaffung von Rechtssicherheit und -klarheit,
- klarstellende Auflistung der Anlässe für den offenen und verdeckten Einsatz von unbemannten Luftfahrtsystemen (sogenannter Drohneneinsatz; § 34),
- polizeiliche Befugnis zur Ausschreibung zur gezielten Kontrolle (§ 35),
- polizeiliche Befugnis zur Datenübermittlungen zum Zwecke einer Zuverlässigkeitsüberprüfung (§ 40),

- Erweiterung des Katalogs der Straftaten von erheblicher Bedeutung in § 49 wie folgt:

  - in § 49 Nummer 2 Erweiterung um die Vergehenstatbestände der §§ 89c Absatz 1 bis 4 (Terrorismusfinanzierung), 129a (Bildung terroristischer Vereinigungen), 129b (Kriminelle und terroristische Vereinigungen im Ausland), 184b Absatz 1 und 2 sowie 184c Absatz 2 (Verbreitung, Erwerb und Besitz kinderpornographischer und jugendpornographischer Schriften), 303b Absatz 4 (besonders schwerer Fall der Computersabotage) des Strafgesetzbuches,
  - in § 49 Nummer 3 Erweiterung um banden-, gewerbs-, serienmäßig oder sonst organisierte Vergehen nach § 261 des Strafgesetzbuches (Geldwäsche) sowie nach § 96 Absatz 2 des Aufenthaltsgesetzes (Einschleusen von Ausländern).

- ausdrückliche polizeiliche Befugnis zur Erteilung von Meldeauflagen (§ 52b),
- Aufnahme von Forderungen und anderen Vermögensrechten in die Sicherstellungsbefugnis (§ 61),
- klarstellende Regelung zum finalen Rettungsschuss (§ 109 Absatz 1).

Zudem werden die Regelungen aus § 52 Absatz 3 (regelt Betretungs- und Aufenthaltsgebote bis maximal zehn Wochen) herausgelöst und in eine gesonderte Norm (§ 52a) - unter Anpassung der Höchstfrist auf drei Monate und Ergänzung notwendiger Regelungen zur Anordnung - überführt. Die Regelungen bedurften zudem einer Anpassung aufgrund des am 5. April 2018 in Kraft getretenen § 67b (vergleiche GVOBl. M-V 2018, Seite 114).

Weitere Änderungen

Ferner werden mit der in Artikel 1 vorgesehenen Neufassung des SOG M-V weitere notwendige rechtliche Anpassungen und redaktionelle Korrekturen vollzogen. Es erfolgt die Aufnahme der großen kreisangehörigen Städte in das Gesetz. Die sprachliche Gleichstellung sowie die Aktualisierung von Behördenbezeichnungen und Verweisungen werden vorgenommen.

Im Zuge der in Artikel 2 und 3 vorgesehenen Änderungen des Brandschutz- und Hilfeleistungsgesetzes M-V und des Landeskatastrophenschutzgesetzes erfolgt eine Aktualisierung der Behördenbezeichnungen.

II. Zu den einzelnen Bestimmungen:

Zu Artikel 1
Neufassung des SOG M-V

Zum Inhaltsverzeichnis

Das Inhaltsverzeichnis zum SOG M-V ist aufgrund der Aufnahme von Neuregelungen zur Umsetzung des EU-Datenschutzpakets und von neuen Befugnissen oder klarstellenden Regelungen anzupassen.

Insbesondere wird der Abschnitt 3, der die Regelungen zur Verarbeitung personenbezogener Daten enthält (§§ 25 bis 49), aufgrund der Anpassungen und Änderungen zur Umsetzung des EU-Datenschutzpakets in die Unterabschnitte 1 bis 7 unterteilt. Es erfolgt unter anderem die Aufnahme von neuen Vorschriften zur Einwilligung, zum Schutz des Kernbereichs privater Lebensgestaltung und auch von Zeugnisverweigerungsberechtigten, zur Weiterverarbeitung personenbezogener Daten (hier insbesondere auch zur Datenübermittlung), zu Pflichten der verantwortlichen Stelle und des Auftragsverarbeiters, zu den Rechten der betroffenen Personen und zur datenschutzaufsichtlichen Kontrolle.

In den Abschnitten 3 und 4 werden die oben angeführten neuen oder auch klarstellenden Datenerhebungsbefugnisse im SOG M-V verankert. Hierbei ist zu beachten, dass bereits bestehende Befugnisse zum Teil unter einer anderen Paragraphenbezeichnung verortet sind.

Zudem werden redaktionelle Anpassungen und die sprachliche Gleichstellung im Inhaltsverzeichnis vollzogen.

§ 1 (Aufgaben)

Der bisher geltende § 1 wird mit folgenden Änderungen übernommen:

Aufgrund der Aufhebung der Kreisfreiheit für die Universitäts- und Hansestadt Greifswald, die Hansestadt Stralsund, die Hansestadt Wismar und die Stadt Neubrandenburg durch § 1 Absatz 2 des Artikels 1 des Kreisstrukturgesetzes vom 12. Juli 2010 (GVOBl. M-V Seite 366) wurde in § 7 der Kommunalverfassung die Gemeindeart der großen kreisangehörigen Städte eingeführt. Es sind daher in Absatz 1 und auch in Absatz 4 die großen kreisangehörigen Städte aufzunehmen.

§ 2 (Ordnungsbehörden und Polizei)

Keine Änderung.

§ 3 (Begriffsbestimmungen)

Der bisher geltende Absatz 1 wird mit folgender Änderung übernommen:

Unter Verweis auf die Ausführungen zu § 1 wird der bisher geltende Satz 1 Nummer 3 (Benennung der örtlichen Ordnungsbehörden) um die großen kreisangehörigen Städte ergänzt. Gemäß § 38 der Kommunalverfassung haben kreisfreie und große kreisangehörige Städte einen hauptamtlichen Bürgermeister, der die Bezeichnung Oberbürgermeister trägt, sofern die Hauptsatzung nicht die Bezeichnung Bürgermeister vorsieht. Vor diesem Hintergrund wird neben der Bezeichnung „Oberbürgermeister“ zusätzlich die Bezeichnung „Bürgermeister“ eingefügt.

Der bisher geltende Absatz 2 wird übernommen und die sprachliche Gleichstellung vollzogen.

Der bisher geltende Absatz 3 wird unverändert übernommen.

Absatz 4 wird neu aufgenommen. Aufgrund der mit der Verordnung (EU) 2016/679 und Richtlinie (EU) 2016/680 eingeführten Definition des „Dritten“ bedarf es einer Abgrenzung des Begriffs im datenschutzrechtlichen Sinne zu dem im SOG M-V bisher verwendeten Begriff des „Dritten“. Diese Abgrenzung wird mit dem neuen Absatz 4 eingeführt. Unter Nummer 1 fällt damit beispielsweise eine Stelle, die weder verantwortliche Stelle noch Auftragsverarbeiter ist und die personenbezogenen Daten im Wege einer Übermittlung erhält. Gleichzeitig wird mit dem Klammerzusatz in Nummer 1 eine Definition der betroffenen Person eingefügt, um missverständliche Überschneidungen mit einer durch die Maßnahme mitbetroffenen Person, die jedoch nicht Ziel der Maßnahme war (unbeteiligter Dritter), zu vermeiden. Unter Nummer 2 fallen im Ergebnis die unvermeidbar betroffenen, unbeteiligten Dritten (beispielsweise im Rahmen einer Bodycam-Aufnahme miterfasste Spaziergänger).

Die im bisherigen Absatz 4 vorgesehene Trennung der Prozesse der Datenerhebung, -verarbeitung und -nutzung ist mit Blick auf die Umsetzung der Verordnung (EU) 2016/279 sowie der Richtlinie (EU) 2016/280 zukünftig nicht mehr möglich. Der Sprachgebrauch des Gesetzes wird daher angepasst und die verwendeten neuen Begrifflichkeiten werden entsprechend den EU-Vorschriften - siehe Artikel 3 der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/670 - in Absatz 5 in den Nummern 1 bis 17 verankert.

Insbesondere wird der Forderung der seinerzeitigen Bundesdatenschutzbeauftragten nachgekommen und hierzu in Nummer 2 der Begriff der „Grunddaten“ definiert. Die Definition orientiert sich an der Formulierung in § 20 des Hessischen Sicherheits- und Ordnungsgesetzes. Die Auflistung der aufgeführten Grunddaten ist als nicht abschließend zu betrachten.

Auch die besonderen Kategorien personenbezogener Daten werden weitgehend entsprechend Artikel 9 der Verordnung (EU) 2016/279 beziehungsweise Artikel 10 der Richtlinie (EU) 2016/680 mit Nummer 3 in das SOG M-V übernommen, da das neugefasste Landesdatenschutzgesetz keine Regelung mehr zu diesen Datenarten enthält (vergleiche § 7 Absatz 2 des Landesdatenschutzgesetzes in der vor dem 25. Mai 2018 geltenden Fassung mit dem neugefassten Landesdatenschutzgesetz - GVOBl. M-V 2018, Seite 193 ff.). Hinsichtlich der Nummer 3 Buchstabe c ist auf den Erwägungsgrund 51 der Verordnung (EU) 2016/679 hinzuweisen.

Danach ist die Verarbeitung von Lichtbildern nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten anzusehen, da Lichtbilder nur dann von der Definition des Begriffs „biometrische Daten“ erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen.

Nummer 4 macht deutlich, dass unter den Begriff der Datenverarbeitung anders als bisher nicht „nur“ das Speichern, Verändern, Übermitteln, Sperren, Löschen, Anonymisieren, Pseudonymisieren und Verschlüsseln von Daten (vergleiche die bisher geltende Fassung in § 3 Absatz 4 Nummer 2) fallen, sondern der Begriff nun umfassend zu verstehen ist. „Verarbeitung“ ist gemäß Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 und Artikel 3 Nummer 2 der Richtlinie (EU) 2016/680 nun jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten.

In Nummer 5 wird die „Einschränkung der Verarbeitung“ definiert, die im bisherigen Sprachgebrauch des Gesetzes als „Sperrung“ bekannt war.

Mit Nummer 9 wird durch die Definition der „verantwortlichen Stelle“ von der Öffnungsklausel aus Artikel 4 Nummer 7 der Verordnung (EU) 2016/679 Gebrauch gemacht und gleichzeitig Artikel 3 Nummer 8 der Richtlinie umgesetzt. Zudem wird der Begriff des „Verantwortlichen“ durch die „verantwortliche Stelle“ ersetzt, um Irritationen im Zusammenhang mit dem im Gefahrenabwehrrecht beziehungsweise Polizei- und Ordnungsrecht feststehenden Begriff des „Verantwortlichen“, zum Beispiel im Sinne von § 27 Absatz 2 Satz 1 Nummer 2 bis 4 oder §§ 68ff, zu vermeiden.

Im Übrigen ist zur Notwendigkeit der Einführungen der Definitionen auf die nachfolgende neue gesetzliche Regelungslage zu verweisen.

§ 4 (Sachliche Zuständigkeit der Ordnungsbehörden, Ermächtigung zum Erlass von Rechtsverordnungen)

Der bisher geltende § 4 wird mit folgenden Änderungen übernommen:

Es erfolgt eine Ergänzung der Bezeichnung des § 4, um auf die bisher im § 4 enthaltene und übernommene Ermächtigung zum Erlass von Rechtsverordnungen deutlicher hinzuweisen.

Im Absatz 1 wird durch die Aufnahme von Satz 2 ausdrücklich klargestellt, dass sich die sachliche Zuständigkeit der Ordnungsbehörden zur Gefahrenabwehr - wie bisher auch schon - ebenfalls auf die Verhütung von Ordnungswidrigkeiten erstreckt (im Weiteren siehe hierzu die Begründung zu § 25).

Die Bezeichnung des Innenressorts wird im Absatz 2 aktualisiert. Zudem wird zur Präzisierung das Wort „Verordnung“ durch das Wort „Rechtsverordnung“ ersetzt.

§ 5 (Örtliche Zuständigkeit der Ordnungsbehörden, Ermächtigung zum Erlass von Rechtsverordnungen)

Der bisher geltende § 5 wird mit folgenden Änderungen übernommen:

Es erfolgt eine Ergänzung der Bezeichnung des § 5, um auf die bisher im § 5 enthaltene und übernommene Ermächtigung zum Erlass von Rechtsverordnungen deutlicher hinzuweisen.

Im Absatz 4 wird die Bezeichnung des Innenressorts aktualisiert und es wird zur Präzisierung das Wort „Verordnung“ durch das Wort „Rechtsverordnung“ ersetzt.

§ 6 (aufgehoben)

Die Beibehaltung des bereits aufgehobenen und damit inhaltsleeren § 6 erfolgt zur Vermeidung einer kompletten Regelungsverschiebung.

§ 7 (Sachliche Zuständigkeit der Polizei)

Keine Änderung

§ 8 (Örtliche Zuständigkeit der Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten

Der bisher geltende § 8 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 9 (Amtshandlungen von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten eines anderen Landes oder des Bundes oder anderer Staaten sowie von Zollbediensteten in den Vollzugsbereichen der Zollverwaltung)

Die Bezeichnung des § 9 wird aufgrund der sprachlichen Gleichstellung und der Aufnahme einer polizeilichen Eilkompetenz für Zollbedienstete in den Vollzugsbereichen der Zollverwaltung angepasst.

Der bisher geltende § 9 wird unter Vollzug der sprachlichen Gleichstellung und darüber hinaus mit folgenden Ergänzungen und Änderungen übernommen:

In Absatz 2 wird unter Berücksichtigung anderer vergleichbarer Länderreglungen (wie etwa in § 77 des Brandenburgischen Polizeigesetzes, § 77 des Sächsischen Polizeigesetzes, § 78 des Polizeigesetzes Baden-Württemberg oder § 11 des Polizeiorganisationsgesetzes in Bayern) ausdrücklich klargestellt, dass die nach § 9 Absatz 1 tätig werdenden Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten den Weisungen derjenigen Polizeibehörde, in deren örtlichem und sachlichem Zuständigkeitsbereich sie tätig geworden sind, unterliegen. Diese Klarstellung wird insbesondere mit Blick auf den neu aufgenommen Absatz 4 (Eilkompetenz für Zollbedienstete in den Vollzugsbereichen der Zollverwaltung) für notwendig erachtet, da Absatz 2 dort entsprechend zur Anwendung gelangt.

Mit dem neuen Absatz 4 werden Absatz 1 und 2 des § 9 für Zollbedienstete in den Vollzugsbereichen der Zollverwaltung, denen der Gebrauch von Schusswaffen bei Anwendung des unmittelbaren Zwangs bei Ausübung öffentlicher Gewalt gestattet ist, für entsprechend anwendbar erklärt. Damit dürfen diese Bediensteten der Zollverwaltung zukünftig ebenfalls die Amtshandlungen vornehmen, die auch Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten, die nicht in einem Dienstverhältnis zum Land Mecklenburg-Vorpommern stehen, unter bestimmten Voraussetzungen ausführen dürfen.

Mit dieser Regelung wird einer langjährigen Forderung des Bundesministeriums der Finanzen und der BDZ Deutsche Zoll- und Finanzgewerkschaft nach einer polizeilichen Eilkompetenz für Zollbedienstete in den Vollzugsbereichen der Zollverwaltung nachgekommen. So hat der Bundesgesetzgeber mit der zum 16. März 2017 in Kraft gesetzten Öffnungsklausel in § 12d des Zollverwaltungsgesetzes nunmehr bestimmt, dass Zollbedienstete in den Vollzugsbereichen der Zollverwaltung nach Maßgabe des jeweiligen Landesrechts im Zuständigkeitsbereich des Landes polizeiliche Amtshandlungen vornehmen dürfen, wenn die zuständige Polizeibehörde die erforderlichen Maßnahmen nicht rechtzeitig treffen kann. Aufgrund dieser geschaffenen bundesrechtlichen Regelung ist nun auch eine landesrechtliche Regelung zur Vornahme von Amtshandlungen im Bereich der Gefahrenabwehr durch Zollbedienstete in den Vollzugsbereichen der Zollverwaltung, denen der Gebrauch von Schusswaffen bei Anwendung des unmittelbaren Zwangs bei Ausübung öffentlicher Gewalt gestattet ist, rechtlich zulässig. Entsprechende ausdrückliche landesrechtliche Regelungen bestehen unter anderem bereits in anderen Ländern (Beispiele siehe Ausführungen zum vorstehenden Absatz 2).

Durch die geregelte entsprechende Anwendung von Absatz 2 und wegen der dort vorgenommenen Ergänzung unterliegen auch Zollbedienstete in den Vollzugsbereichen der Zollverwaltung den Weisungen derjenigen Polizeibehörde, in deren örtlichem und sachlichem Zuständigkeitsbereich sie tätig geworden sind. Ihre getroffenen Maßnahmen gelten als Maßnahmen dieser Polizeibehörde.

Die bisherige Regelung des Absatzes 4 gilt als Absatz 5 mit der sprachlich vollzogenen Gleichstellung grundsätzlich fort. Es wird jedoch in Anlehnung an entsprechende Formulierungen anderer Bundesländer (zum Beispiel § 9 Absatz 4 Satz 2 des Gesetzes über die Organisation und die Zuständigkeit der Polizei im Lande Nordrhein-Westfalen, § 8 Absatz 3 des Allgemeinen Gesetzes zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin) der Verweis auf den „Beschluss des Rates 2008/615/JI vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität“ durch die allgemeinere Formulierung „nach Maßgabe von Rechtsakten der Europäischen Union“ ersetzt, um auf neue Vereinbarungen flexibel reagieren zu können.

§ 10 (Amtshandlungen von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten außerhalb Mecklenburg-Vorpommerns)

Der bisher geltende § 10 wird unter Vollzug der sprachlichen Gleichstellung übernommen. Zudem wird in Anlehnung an entsprechende Formulierungen anderer Bundesländer (zum Beispiel § 8 Absatz 3 des Gesetzes über die Organisation und die Zuständigkeit der Polizei im Lande Nordrhein-Westfalen, § 7 Absatz 1 Satz 2 des Allgemeinen Gesetzes zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin) der Verweis auf den „Beschluss des Rates 2008/615/JI vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität“ durch die allgemeinere Formulierung „nach Maßgabe von Rechtsakten der Europäischen Union“ ersetzt, um auf neue Vereinbarungen flexibel reagieren zu können.

§ 11 (Zusammenarbeit von Ordnungsbehörden und Polizei)

Der bisher geltende § 11 wird unter der Aktualisierung der Bezeichnung des Innenressorts übernommen.

§ 12 (Grundsatz)

§ 12 wird mit einer Präzisierung in den Absätzen 1 und 2 übernommen. Es wird jeweils das Wort „Verordnungen“ durch das Wort „Rechtsverordnungen“ ersetzt.

§ 13 (Allgemeine Befugnisse)

Keine Änderung.

§ 14 (Ermessen)

Der bisher geltende § 14 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 15 (Grundsatz der Verhältnismäßigkeit)

Keine Änderung.

§ 16 (Verfügungen)

Der bisher geltende § 16 wird unter Aktualisierung der in Absatz 2 enthaltenen Gesetzesbezeichnung („Landesverwaltungsverfahrensgesetz“) übernommen.

§ 17 (Verordnungen über die öffentliche Sicherheit oder Ordnung)

Der bisher geltende § 17 wird mit der Änderung übernommen, dass jeweils in den Absätzen 2 bis 4 zur Präzisierung nach dem Wort „Verordnungen“ die Wörter „über die öffentliche Sicherheit oder Ordnung“ hinzugefügt werden. Im Absatz 3 erfolgt zudem eine Ergänzung um die großen kreisangehörigen Städte (siehe hierzu Begründung zu § 1).

§ 18 (Inhalt der Verordnungen über die öffentliche Sicherheit oder Ordnung)

Die Bezeichnung des § 18 und dessen Absatz 1 werden zur Präzisierung jeweils nach dem Wort „Verordnungen“ um die Wörter „über die öffentliche Sicherheit oder Ordnung“ ergänzt. Im Absatz 2 wird das Wort „Verordnungen“ durch das Wort „Rechtsverordnungen“ ersetzt. Im Übrigen wird der Regelungsinhalt des § 18 unverändert übernommen.

§ 19 (Ordnungswidrigkeiten)

Der bisher geltende § 19 wird mit der Änderung übernommen, dass in Absatz 3 Satz 1 die Oberbürgermeister beziehungsweise Bürgermeister der großen kreisangehörigen Städte ergänzt werden (vergleiche hierzu auch Begründung zu § 3 Absatz 1). Zudem wird in Absatz 3 Satz 1 ein Bezug zu § 17 hergestellt, um den verwendeten Begriff der „Verordnung“ zu präzisieren.

§ 20 (Verhältnis zu anderen Rechtsvorschriften; Genehmigungspflicht)

Der bisher geltende § 20 wird mit folgender Änderungen übernommen:

In Absatz 1 Satz 1 wird das Wort „Verordnungen“ durch den Zusatz „über die öffentliche Sicherheit oder Ordnung“ präzisiert. Zudem werden nach dem Wort „Gesetzen“ die Wörter „und Rechtsverordnungen“ eingefügt.

In Absatz 2 Satz 1 und Absatz 3 Satz 1 wird jeweils das Wort „Verordnungen“ durch den Zusatz „über die öffentliche Sicherheit oder Ordnung“ präzisiert. Zudem erfolgt in Absatz 3 Satz 1 eine Aktualisierung der Bezeichnung des Innenressorts und die großen kreisangehörigen Städte werden in die Regelung aufgenommen. Es wird klargestellt, dass ihre Verordnungen - wie auch die Verordnungen der Landkreise und der kreisfreien Städte - der Genehmigung des Ministeriums für Inneres und Europa bedürfen. Die Regelung erfolgt vor dem Hintergrund des § 86 Absatz 3 der Kommunalverfassung (Fachaufsichtsbehörde für die großen kreisangehörigen Städte ist die fachlich zuständige oberste Landesbehörde).

§ 21 (Form der Verordnungen über die öffentliche Sicherheit oder Ordnung)

Die Bezeichnung des § 21 und dessen Absätze 1 und 2 werden mit Präzisierungen übernommen. Es werden dem Wort „Verordnungen“ jeweils die Wörter „über die öffentliche Sicherheit oder Ordnung“ hinzugefügt.

§ 22 (Geltungsdauer)

Der bisher geltende § 22 wird mit der Präzisierung übernommen, dass in den Absätzen 1 und 2 jeweils nach dem Wort „Verordnungen“ die Wörter „über die öffentliche Sicherheit oder Ordnung“ hinzugefügt werden.

§ 23 (Amtliche Bekanntmachung)

Der bisher geltende § 23 wird mit folgenden Änderungen übernommen:

Im Absatz 1 und im Absatz 3 Satz 2 werden zur Präzisierung jeweils nach dem Wort „Verordnung“ beziehungsweise „Verordnungen“ die Wörter „über die öffentliche Sicherheit oder Ordnung“ ergänzt.

Im Absatz 3 Satz 1 wird in die Aufzählung zur Ersatzverkündung bei Gefahr im Verzug auch das Internet aufgenommen.

§ 24 (Inkrafttreten der Verordnungen über die öffentliche Sicherheit oder Ordnung)

Die Bezeichnung des § 24 und dessen Inhalt werden jeweils mit einer Präzisierung übernommen. Es werden dem Wort „Verordnungen“ jeweils die Wörter „über die öffentliche Sicherheit oder Ordnung“ hinzugefügt.

§ 25 (Bestimmungen zur Anwendbarkeit der Vorschriften dieses Gesetzes im Anwendungsbereich der Verordnung (EU) 2016/679 und des Landesdatenschutzgesetzes)

§ 25 enthält grundlegende Bestimmungen zur Anwendbarkeit der Vorschriften der Datenverarbeitung nach diesem Gesetz im Anwendungsbereich der Verordnung (EU) 2016/679. Die Norm soll insbesondere auch deutlich machen, mit welchem rechtlichen Grundverständnis die Vorschriften zur Datenverarbeitung geschaffen werden. Die in den Absätzen 2 und 3 enthaltenen Regelungen dienen der Herstellung von Transparenz. Durch sie wird hinreichend bestimmbar, auf Basis welcher grundlegenden Vorgaben der Verordnung (EU) 2016/679 spezifische Bestimmungen in das zukünftige SOG M-V aufgenommen werden oder sogar beibehalten werden konnten. Sie lassen zudem erkennbar werden, dass die Regelungen ihren Ursprung im Recht der Europäischen Union haben.

Die Umsetzung der Richtlinie (EU) 2016/680 etwa allein durch die entsprechende Geltung der Verordnung (EU) 2016/679 vorzunehmen, würde den Zielen des EU-Gesetzgebers nicht gerecht werden. Denn dieser hat gerade durch die Schaffung von zwei unterschiedlichen Regelungswerken gewürdigt, dass im Anwendungsbereich der Richtlinie und demzufolge unter anderem zur Verhütung von Straftaten andere Datenschutzvorschriften gelten müssen, damit die Sicherheitsbehörden ihre Aufgaben erfüllen können. Vor diesem Hintergrund haben sowohl der Bund als auch andere Länder spezielle Vorschriften zur Umsetzung der Richtlinie (EU) 2016/680 in ihren Datenschutzgesetzen geschaffen. Dies mit der Folge, dass im jeweiligen Fachgesetz und damit auch in den Polizei- und Ordnungsgesetzen weniger Umsetzungsvorschriften verankert werden mussten.

Da - abgesehen von dem als Auffangnorm fungierenden § 3 - bewusst keine Vorschriften im Landesdatenschutzgesetz zur Umsetzung der Richtlinie (EU) 2016/680 geschaffen wurden, ist deren konkrete Umsetzung im Land Mecklenburg-Vorpommern im jeweiligen (Landes-) Fachrecht mit einem entsprechend größeren Regelungsaufwand vorzunehmen. Demzufolge sind im Gefahrenabwehrrecht des Landes und damit im SOG M-V spezielle Regelungen aufzunehmen, die die Datenverarbeitung im Anwendungsbereich der Richtlinie (EU) 2016/680 erfassen und damit den Willen des EU-Richtliniengebers in nationales Recht umsetzen. Da der EU-Richtliniengeber den Gefahrenabwehrbereich aber nicht vollständig in den Anwendungsbereich der Richtlinie einbezogen hat, verbleiben Fallgestaltungen, die dem Anwendungsbereich der Verordnung (EU) 2016/679 zuzuordnen sind und die bei der Gesetzesneufassung mit zu betrachten und - soweit rechtlich zulässig - auch mit zu regeln sind (siehe hierzu die folgenden Ausführungen insbesondere zu den Absätzen 1 und 5). Insoweit steht der Landesgesetzgeber im Gefahrenabwehrrecht vor der schwierigen Aufgabe, eine Regelungslage zu schaffen, die diesem EU-Regelungsgefüge gerecht wird.

Absatz 1 bestimmt, dass die Vorschriften zur Datenverarbeitung nach diesem Gesetz grundsätzlich auch für die Erfüllung von ordnungsbehördlichen und polizeilichen Aufgaben, die in den Anwendungsbereich der Verordnung (EU) 2016/679 fallen, gelten.

Mit Blick auf die tradierte Aufgabenzuweisung im Gefahrenabwehrrecht des Landes an die Polizei und die Ordnungsbehörden stellen die Vorschriften der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 sowohl den Gesetzgeber als auch den Rechtsanwender vor erhebliche Abgrenzungsprobleme. Insbesondere die Verordnung (EU) 2016/679 verfolgt zwar das Ziel, das Datenschutzrecht in der Union zu vereinheitlichen, kann aber deswegen im Bereich der öffentlichen Verwaltung nicht die jeweiligen Regelungsgefüge der Mitgliedstaaten berücksichtigen. Als Ausgleich dafür werden den Mitgliedstaaten mit einer Vielzahl von „Öffnungsklauseln“ Regelungsaufträge und -befugnisse eingeräumt.

Mit Absatz 1 werden - soweit wie rechtlich zulässig und möglich - direkte Regelungen der im gesamten Bereich des Gefahrenabwehrrechts zu beachtenden datenschutzrechtlichen Bestimmungen im SOG M-V selbst vorgenommen. Hierbei besteht das Ziel, datenschutzrechtliche Regelungen im SOG M-V zu schaffen, die sowohl der Umsetzung der Richtlinie (EU) 2016/680 dienen als auch den Regelungen der unmittelbar geltenden Verordnung (EU) 2016/679 entsprechen. Dabei wird insbesondere von den Klauseln in Artikel 6 Absatz 2 und 3 der Verordnung (EU) 2016/679 zur Schaffung spezifischer Bestimmungen Gebrauch gemacht. Diese Regelung sieht vor, dass die Mitgliedstaaten spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften der Verordnung (EU) 2016/679 in Bezug auf die Verarbeitung für die Wahrnehmung einer Aufgabe in Ausübung öffentlicher Gewalt einführen können, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten. Absatz 3 des Artikels 6 enthält zudem eine beispielhafte Aufzählung möglicher Regelungsinhalte.

Auch ist auf Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 hinzuweisen. Dieser bestimmt:

„*Durch Rechtsvorschriften […] der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:*
[…]
c) die öffentliche Sicherheit;
d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit; […]“.

Hierzu wird auch auf den Erwägungsgrund 73 der Verordnung (EU) 2016/679 Bezug genommen. Insoweit sind beschränkende und damit spezielle Regelungen im SOG M-V zum Beispiel zum Recht auf Auskunft oder Berichtigung und Löschung von personenbezogenen Daten zulässig.

Die möglichst umfassende und homogene Regelung der im Gefahrenabwehrbereich zu beachtenden datenschutzrechtlichen Bestimmungen im SOG M-V selbst bedeutet zwar einerseits einen größeren gesetzgeberischen Aufwand, anderseits wird den Gesetzesanwendern damit aber weitestgehend ein ständiges „Hineinspringen“ in verschiedene datenschutzrechtliche Regelungswerke erspart und so die bessere praktische Handhabung gewährleistet. Auch stellt dieses Vorgehen eine möglichst einheitliche Verfahrensweise bei Polizei und Ordnungsbehörden im Land Mecklenburg-Vorpommern mit Blick auf die notwendige Zusammenarbeit im Bereich der Gefahrenabwehr sicher.

Soweit im SOG M-V Wiederholungen von und Verweise auf Bestimmungen aus der Verordnung (EU) 2016/679 erfolgen, so geschieht dies aus Gründen der Verständlichkeit und Kohärenz und lässt die unmittelbare Geltung der Verordnung (EU) 2016/679 unberührt. Auf den Erwägungsgrund 8 der Verordnung (EU) 2016/679 wird hingewiesen. Danach sind Wiederholungen von Regelungen der Verordnung (EU) 2016/679 im nationalen Recht insoweit möglich, als im Falle von Präzisierungen oder Einschränkungen von Regelungen der Verordnung (EU) 2016/679 durch das nationale Recht diese erforderlich sind, um die Kohärenz zu wahren und die Vorschriften des nationalen Rechts für die Personen, für die sie gelten, verständlicher zu machen. Das Wiederholungsverbot soll verhindern, dass die unmittelbare Geltung einer Verordnung verschleiert wird, weil die Normadressaten über den wahren Urheber des Rechtsaktes oder die Jurisdiktion des Europäischen Gerichtshofes im Unklaren gelassen werden (EuGH, Rs. C-34/73, Variola, Randnummern 9 ff.; EuGH, Rs. C-94/77, Zerbone, Randnummer 22/27). Die Wiederholungen von Bestimmungen aus der Verordnung (EU) 2016/679 sind aber gerade auch dem Umstand geschuldet, dass bei der Aufgabe der Gefahrenabwehr sowohl der Anwendungsbereich der Verordnung (EU) 2016/679 als auch der Richtlinie (EU) 2016/680 betroffen ist. In einem solchen Fall hat es der EuGH dem nationalen Gesetzgeber eingeräumt, im Interesse eines inneren Zusammenhangs und der Verständlichkeit für den Adressaten notwendige punktuelle Normwiederholungen vorzunehmen (EuGH, Rs. C-272/83, Kommission/Italien, Randnummer 27).

Die Klauseln zur Schaffung spezifischer Bestimmungen sind weder nach ihrem Wortlaut noch nach den Zwecken der Verordnung (EU) 2016/679 restriktiv auszulegen (dazu auch Roßnagel in Datenschutz und Datensicherheit 8/2018 „Kontinuität oder Innovation? Der deutsche Spielraum in der Anpassung des bereichsspezifischen Datenschutzrechts“, Seite 477, 479). Artikel 6 Absatz 2 der Verordnung (EU) 2016/679 enthält keine Beschränkung der Möglichkeit zur Schaffung spezifischer Bestimmungen auf ganz bestimmte Vorschriften, sondern bezieht grundsätzlich alle Vorschriften mit ein, wenn die Verarbeitung zur Erfüllung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erfolgt. Der Umfang möglicher spezifischer Regelungen wird damit durch die jeweilige Norm bestimmt. Schon die Vielzahl von „Öffnungsklauseln“ für den Bereich der öffentlichen Sicherheit zeigt, dass das Ziel der Vereinheitlichung des Datenschutzes innerhalb des europäischen Raumes anderen Zielen nicht zwangsläufig vorgehen kann.

Die Vorgaben und Ziele der Verordnung (EU) 2016/679 ermöglichen es somit, im Bereich des SOG M-V ein weitgehend einheitliches Regelungssystem für den Datenschutz zu schaffen, das insbesondere dazu beiträgt, Vollzugsdefiziten aufgrund der Abgrenzungsschwierigkeiten zwischen Verordnung und Richtlinie entgegenzuwirken.

Absatz 1 Satz 2 enthält eine gegenüber dem Satz 1 klarstellende Ausnahme von der einheitlichen Geltung bestimmter Datenverarbeitungsvorschriften. Die dem § 25 nachfolgenden Datenverarbeitungsvorschriften sind dabei teilweise ausdrücklich auf den Anwendungsbereich der Richtlinie (EU) 2016/680 beschränkt, soweit eine einheitliche Regelung unter Anwendung der Klauseln zur Schaffung spezifischer Bestimmungen der Verordnung (EU) 2016/679 nicht erfolgen konnte, etwa im Bereich der Vorschriften zur Drittstaatenübermittlung. Ist eine solche Begrenzung einer Norm auf den Anwendungsbereich der Richtlinie erfolgt, dann richtet sich das Handeln der Gefahrenabwehrbehörden, das in den Anwendungsbereich der Verordnung fällt, ausschließlich nach den Bestimmungen der Verordnung (EU) 2016/679, gegebenenfalls in Verbindung mit den Vorschriften des Landesdatenschutzgesetzes. Andererseits können bestimmte Regelungen schon nach ihren Voraussetzungen nur dem Anwendungsbereich der Richtlinie (EU) 2016/680 unterfallen, wie zum Beispiel polizeiliche Befugnisse zur Straftatenverhütung. Zudem wird mit Satz 2 klargestellt, dass die Definitionen in § 3 Absatz 4 und 5, soweit sie denen des Artikels 4 der Verordnung (EU) 2016/679 entsprechen, nur für den Bereich der Richtlinie (EU) 2016/680 gelten, sodass ein Verstoß gegen das Wiederholungsverbot ausgeschlossen wird.

Die Absätze 2 und 3 dienen als Transparenzvorschriften, mit denen verdeutlicht wird, welche Datenschutzvorschriften im SOG M-V ihren Ursprung in den europarechtlichen Vorgaben der Verordnung (EU) 2016/679 haben (dazu auch Albers/Veit in Beck´scher Onlinekommentar Datenschutzrecht zu Artikel 6, Randnummer 62). Für den Gesetzgeber und den Normadressaten wird daher deutlich gemacht, welche Vorschrift im SOG M-V als spezifische Bestimmung welchen Artikels der Verordnung (EU) 2016/679 zu verstehen ist und bei welchen Vorschriften es sich um Einschränkungen von Vorgaben der Verordnung (EU) 2016/679 über die Regelungsbefugnis des Artikels 23 der Verordnung (EU) 2016/679 handelt.

Absatz 4 steht im unmittelbaren Zusammenhang mit den Absätzen 2 und 3 und dient als Auffangnorm. Er verdeutlicht, dass die übrigen Datenverarbeitungsvorschriften, die entsprechend der Vorgabe in Absatz 1 auch für die Aufgabenerfüllung im Anwendungsbereich der Verordnung (EU) 2016/679 Anwendung finden, als spezifische Bestimmungen zu den in Artikel 1 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 geregelten grundsätzlichen Zulässigkeitsregelung für die Datenverarbeitung anzusehen sind. Damit wird dem Transparenzgebot dahingehend Rechnung getragen, dass das SOG M-V spezielle Befugnisse enthält, die auch im Anwendungsbereich der Verordnung (EU) 2016/679 eine Datenverarbeitung erlauben, die aber keine entsprechend spezielle Vorgabe in der Verordnung (EU) 2016/679 hat. Dies ist zum Beispiel bei der Erhebung von Standortdaten eines Mobiltelefons bei Vermisstenfällen mit eindeutig fehlendem Straftatenbezug der Fall.

Mit Absatz 5 wird zukünftig ausdrücklich klargestellt, dass das neugefasste Landesdatenschutzgesetz ergänzend Anwendung findet, wenn das SOG M-V nichts Besonderes regelt.

Die im Gesetz enthaltenen Regelungen zur Verarbeitung personenbezogener Daten im Anwendungsbereich des SOG M-V sind bereichsspezifisch und gehen den Vorschriften des neugefassten Landesdatenschutzgesetzes grundsätzlich vor. Dies gilt jedenfalls insoweit, als die genannten Vorschriften des SOG M-V eine eigene tatbestandskongruente bereichsspezifische oder abschließende Datenschutzregelung enthalten und nicht andere Spezialvorschriften greifen. Liegt eine solche eigene Regelung aber nicht vor, dann hat das Landesdatenschutzgesetz den Charakter eines „Auffanggesetzes“.

Für die polizeiliche Tätigkeit im Anwendungsbereich der Richtlinie (EU) 2016/680 ist § 3 des Landesdatenschutzgesetzes maßgeblich. Er bestimmt, dass zur Umsetzung der Richtlinie (EU) 2016/680 die Regelungen der Verordnung (EU) 2016/679 und des Landesdatenschutzgesetzes entsprechend gelten, soweit gesetzlich nicht etwas anderes bestimmt ist. Insbesondere mit den §§ 25a bis 49a sind solche gesetzlichen Regelungen im Sinne des § 3 des Landesdatenschutzgesetzes vorhanden. Es handelt sich um eine in sich geschlossene Kodifikation des eingriffsbefugnisbezogenen Datenschutzes, sodass für eine subsidiäre Anwendung des § 3 des Landesdatenschutzgesetzes für die Polizei und Ordnungsbehörden im Bereich der Umsetzung der Richtlinie kaum ein Anwendungsbereich bleiben wird.

Insgesamt ist zur Abgrenzung des Anwendungsbereichs der Rechtsregime der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2016/679 für den gefahrenabwehrrechtlichen Aufgabenbereich im Grundsatz von Folgendem auszugehen:

Der Bereich der Gefahrenabwehr wird in Ansehung der praxisrelevanten Konstellationen nahezu ausschließlich beziehungsweise ganz überwiegend dem Anwendungsbereich der Richtlinie (EU) 2016/680 und somit den angepassten Datenschutzbestimmungen des SOG M-V sowie ergänzend des Landesdatenschutzgesetzes (§ 3) zuzurechnen sein. Entsprechend Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 enthält diese „Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“.

Die Erwägungsgründe 11 ff. zur Richtlinie (EU) 2016/680 enthalten nähere Erläuterungen zur Auslegung der Definition. Selbst wenn beim Handeln zur Gefahrenabwehr nicht bereits von vorherein klar die Verhütung von Straftaten als Zweck oder Ergebnis feststeht, besteht nahezu immer zumindest die Möglichkeit, dass die Gefahrenlage zu einer Straftat führen kann beziehungsweise dass dies nicht ausgeschlossen ist (wie etwa in Vermisstenfällen). Auch die mögliche Datenverarbeitung zum Schutz privater Rechte (vergleiche § 1 Absatz 3) ist nicht losgelöst von der grundsätzlichen Aufgabe der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zu sehen, sondern wird in der Regel unter diesen Rahmen zu fassen sein. Dies ist insbesondere dann der Fall, wenn ohne Handeln der Polizei und Ordnungsbehörden gegebenenfalls Straftaten drohen oder fortdauern würden (etwa Unterschlagungen und andere Eigentumsdelikte).

Dass in den Anwendungsbereich der Richtlinie (EU) 2016/680 auch Datenverarbeitungen vor allem im durchaus weiten Vorfeld der Straftatenbegehung, wie etwa Tätigkeiten im Bereich der Gefahrenvorsorge und der vorbeugenden Verbrechensbekämpfung sowie die Ausübung hoheitlicher Gewalt durch Ergreifung von Zwangsmitteln, wie polizeiliche Tätigkeiten bei Demonstrationen, großen Sportwettveranstaltungen und Ausschreitungen, aber auch insgesamt die Aufrechterhaltung der öffentlichen Ordnung als Schutz und Abwehr von entsprechend relevanten Bedrohungen der öffentlichen Sicherheit fallen, belegt nicht zuletzt auch der Erwägungsgrund 12 zur Richtlinie (EU) 2016/680 (vergleiche auch Zerdick in Ehmann/Selmayr, Datenschutz-Grundverordnung, Artikel 2 Randnummer 12). Der Begriff der „Straftat“ ist gemäß Erwägungsgrund 13 der Richtlinie (EU) 2016/680 autonom im Sinn der Rechtsprechung des Europäischen Gerichtshofs auszulegen und erfasst auch den nach dem deutschen Rechtsverständnis hiervon zu unterscheidenden Begriff der Ordnungswidrigkeiten. Der Anwendungsbereich der Richtlinie (EU) 2016/680 in Bezug auf Ordnungswidrigkeiten wird dahingehend begrenzt, dass dieser nur eröffnet ist, wenn das von der zuständigen Behörde geführte Verfahren in ein konkretes Ordnungswidrigkeitenverfahren übergeht.

In dem „Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU)“ der Bundesregierung (Drucksache 18/11325) wird auf Seite 110f in Bezug auf Ordnungswidrigkeiten ausgeführt:

„Die Ermittlung, Verfolgung, Ahndung und Vollstreckung von Ordnungswidrigkeiten ist vom Anwendungsbereich umfasst; dies wird durch Erwägungsgrund 13 der Richtlinie (EU) 2016/680 unterstützt. Hierdurch wird insbesondere erreicht, dass die polizeiliche Datenverarbeitung einheitlichen Regeln folgt, unabhängig davon, ob eine Straftat oder eine Ordnungswidrigkeit in Rede steht. Aus dem Ziel, dem Ordnungswidrigkeitenverfahren einheitliche datenschutzrechtliche Regeln gegenüberzustellen, folgt, dass somit auch in Bezug auf die Datenverarbeitung durch Behörden, die nicht Polizeibehörden sind, soweit sie aber Ordnungswidrigkeiten verfolgen, ahnden und vollstrecken, der Teil 3 des vorliegenden Gesetzes gilt und die Datenverarbeitung auch sonst Regeln folgen muss, welche die Richtlinie (EU) 2016/680 umsetzen. Daraus folgt, dass die Datenverarbeitung bei Verwaltungsbehörden […] deren Aufgabenzuweisung nicht mit den in § 45 genannten Zwecken übereinstimmt, grundsätzlich solange und soweit nicht in den Anwendungsbereich der Richtlinie und damit des Dritten Teils dieses Gesetzes fällt, wie die von ihnen geführten Verfahren nicht in ein konkretes Ordnungswidrigkeitenverfahren übergehen.“

Dieser vom Bund dargelegten Auffassung zur Zuordnung von behördlichem Handeln im Zusammenhang mit Ordnungswidrigkeiten wird - auch mit Blick auf die bereits zwischenzeitlich erfolgten Regelungen in anderen Ländern - gefolgt.

Ferner fallen einige Bereiche gefahrenabwehrrechtlichen Handelns wie
- reines Verwaltungshandeln oder Tätigkeiten, bei denen von vornherein feststeht, dass kein Zusammenhang mit der Verhütung oder Unterbindung von Straftaten bestehen kann, oder
- in bestimmten Fällen der Schutz privater Rechte (vergleiche § 1 Absatz 3), wenn im Einzelfall ein offensichtlicher Bezug zu drohenden oder andauernden Straftaten fehlt, oder
- ein vorliegender Suizid (soweit dieser eindeutig festgestellt ist und kein unklarer Todesfall vorliegt)

in den Anwendungsbereich der Verordnung (EU) 2016/679 und damit nicht in den Anwendungsbereich der Richtlinie (EU) 2016/680. Soweit das SOG M-V mithin keine tatbestandskongruente bereichsspezifische oder abschließende Datenschutzregelung enthält und keine anderen Spezialvorschriften greifen, gilt demnach in diesen genannten Bereichen die Verordnung (EU) 2016/679 unmittelbar mit den diesbezüglich ergänzenden Regelungen des Landesdatenschutzgesetzes.

Hinzuweisen ist insbesondere noch darauf, dass weder die Verordnung (EU) 2016/679 noch die Richtlinie (EU) 2016/680 spezielle Regelungen zur Videoüberwachung treffen. Insoweit gilt die Videoüberwachungsregelung in § 11 des neugefassten Landesdatenschutzgesetzes für die Ausübung des Hausrechts; die Videoüberwachung zur Erfüllung gefahrenabwehrrechtlicher Aufgaben richtet sich hingegen ausschließlich nach § 32 SOG M-V.

Ebenso ist darauf hinzuweisen, dass weder die Verordnung (EU) 2016/679 noch die Richtlinie (EU) 2016/680 spezielle Ordnungswidrigkeiten- oder Straftatbestände in Bezug auf datenschutzrechtliche Verstöße enthalten. Insoweit wird auch auf die §§ 22 und 23 des Landesdatenschutzgesetzes verwiesen. Die Verfolgung und Ahndung von Ordnungswidrigkeiten erfolgt gemäß § 19 Absatz 3 durch die Aufsichtsbehörde und damit durch die oder den Landesbeauftragten für den Datenschutz.

Im Übrigen wird auf die weiteren Begründungen zu den einzelnen Regelungen im SOG M-V verwiesen.

§ 25a (Allgemeine Grundsätze)

In § 25a werden allgemeine Grundsätze zur Verarbeitung personenbezogener Daten geregelt. Die bisherigen Regelungen in den §§ 25 und 26 werden hier inhaltlich zusammengeführt und angepasst sowie um notwendige grundsätzliche Regelungen zur Datenverarbeitung ergänzt. Im Einzelnen:

Absatz 1 entspricht im Wesentlichen dem bisherigen § 25 Absatz 1. Die Formulierungen werden an den Sprachgebrauch der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 angepasst, ein Verweis auf die neue Einwilligungsregelung in § 26 aufgenommen und die sprachliche Gleichstellung vollzogen.

Absatz 2 wird neu eingefügt und dient unter anderem der Umsetzung von Artikel 6 der Richtlinie (EU) 2016/680. Dieser sieht vor, dass soweit wie möglich zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen klar zu unterschieden ist. Es wird bestimmt, dass mindestens die Kategorien, die in § 27 Absatz 1 und 3 jeweils aufgeführt sind, zu unterscheiden sind. Der Verweis auf § 27 Absatz 1 und 3 zur Bildung von Kategorien der von einer Datenverarbeitung betroffenen Personen ist nicht abschließend, sodass eine praxisgerechte Ausgestaltung nach den jeweiligen Bedürfnissen der Sicherheitsbehörden möglich bleibt. Durch die Aufzählung der genannten Kategorien besteht auch keine Bindung dahingehend, dass nur Daten dieser Personen erhoben werden dürfen. Die konkreten Rechtsfolgen der vorgesehenen Unterscheidung bei der Verarbeitung, etwa der Unterscheidung entsprechender Aussonderungsprüffristen, Rechte- und Rollenkonzepte oder besondere Maßnahmen der Datensicherheit, werden gesondert geregelt.

Absatz 3 bis 5 entsprechen inhaltlich den bisherigen Regelungen in § 26 Absatz 1 bis 3. Die vorgenommenen Änderungen betreffen die sprachliche Gleichstellung und in Absatz 5 wird durch einen Verweis auf § 3 Absatz 4 Nummer 1 klargestellt, wer Dritte im Sinne der Regelung sind.

Wie beispielsweise auch in § 9 des Bundeskriminalamtgesetzes wird durch Absatz 3 der Grundsatz, dass Daten bei der betroffenen Person zu erheben sind, beibehalten. Dies stellt eine Verschärfung des europäischen Datenschutzniveaus dar und trägt der im Anwendungsbereich des Sicherheits- und Ordnungsgesetzes noch höheren Bedeutung der Richtigkeit der erhobenen personenbezogenen Daten Rechnung. Auch wenn fehlerhafte personenbezogene Daten in allen anderen Bereichen negative Auswirkungen auf die betroffene Person haben können, wiegen diese insbesondere, wenn im Rahmen der Gefahrenabwehr erhobene Daten Basis für Strafverfahren sind, noch deutlich schwerer. Lediglich in Ausnahmefällen, etwa wenn eine Kenntnisnahme der Datenerhebung durch die betroffene Person den Maßnahmezweck gefährden würde, ist eine Abweichung angemessen.

Absatz 6 setzt Artikel 11 der Richtlinie (EU) 2016/680 um. Es besteht ein grundsätzliches Verbot einer ausschließlich auf einer automatischen Verarbeitung beruhenden Entscheidung - einschließlich Profiling -, die eine nachteilige Rechtsfolge für die betroffene Person hat oder sie erheblich beeinträchtigt. Hiervon kann unter bestimmten Voraussetzungen durch Schaffung einer gesetzlichen Norm abgewichen werden. Es wird der Erwägungsgrund 71 der Verordnung (EU) 2016/679 aufgegriffen und klargestellt, dass selbst bei Bestehen einer abweichenden Norm keine Kinder von solchen Maßnahmen betroffen sein dürfen.

Der neue Absatz 7 setzt Artikel 7 Absatz 1 der Richtlinie (EU) 2016/680 um und bestimmt, dass Polizei und Ordnungsbehörden bei der Datenverarbeitung so weit wie möglich eine Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen vorzunehmen haben. Auf persönlichen Einschätzungen beruhende Beurteilungen sind nach Satz 2 kenntlich zu machen. Soweit eine Speicherung dieser in automatisierten Verfahren nach § 42 erfolgt, wird in § 46g Absatz 1 Satz 1 Nummer 10 eine Kennzeichnungspflicht für persönliche Einschätzungen und Beurteilungen normiert. Satz 3 enthält die Regelung aus dem bisher geltenden § 36 Absatz 2 SOG M-V. Hinzuweisen ist an dieser Stelle auch darauf, dass mit § 39b Absatz 3 Satz 2 eine Übermittlungsbeschränkung für persönliche Einschätzungen und Beurteilungen normiert wird. Die Regelung in Absatz 7 entspricht inhaltlich unter anderem dem § 73 des Bundesdatenschutzgesetzes.

§ 25b (Gerichtliche Zuständigkeit, Verfahren)

Mit § 25b wird eine grundsätzliche Norm zur Regelung der gerichtlichen Zuständigkeit sowie des Verfahrens geschaffen, soweit das Gesetz ausdrücklich eine richterliche Entscheidung bestimmt und im Gesetz selbst keine abweichenden Regelungen zur gerichtlichen Zuständigkeit oder zum gerichtlichen Verfahren enthalten sind. Soweit also im SOG M-V solche abweichenden Regelungen in den jeweiligen Normen (siehe beispielsweise § 56 Absatz 5) getroffen werden, gelten diese.

Durch die grundsätzliche Normierung in § 25b können viele Befugnisnormen zugunsten einer besseren Lesbarkeit verkürzt werden. Zu beachten ist unter anderem, dass durch die in § 25b getroffene neue Regelungslage die bisher in einigen Befugnisnormen des SOG M-V bestimmte endgültige Entscheidung des Amtsgerichtes (siehe geltender § 34 Absatz 3 Satz 5 und der in anderen Normen erfolgten Bezugnahmen auf diese Norm) entfallen ist.

Ergänzend wird angemerkt, dass sich die Zuweisung zu den Amtsgerichten am Sitz der die Maßnahme durchführenden Polizeibehörde oder Ordnungsbehörde nach § 25b nur auf die hier ausdrücklich genannten Fallgestaltungen bezieht. So bleiben zum Beispiel die (verwaltungs-)gerichtlichen Zuständigkeiten für den allgemeinen Rechtsschutz etwa gegen Polizei- oder Ordnungsverfügungen nach § 16 SOG M-V oder gegen die nach dem Gesetz getroffenen Maßnahmen, die in die ausschließliche Anordnungs- und Entscheidungskompetenz der Polizei oder Ordnungsbehörde fallen, unberührt. Für bestimmte Fälle, in denen jedoch die Anordnung der Maßnahme nur ausnahmsweise bei Gefahr im Verzug zugelassen wird und eine richterliche Entscheidung unverzüglich herbeizuführen ist (siehe §§ 54, 59, und 67a), und im Fall des § 61 Absatz 1 Satz 4, wird § 25b durch § 49a für entsprechend anwendbar erklärt. Damit wird klargestellt, dass sich das Verfahren nicht nach den Vorschriften über die allgemeine Verwaltungsgerichtsbarkeit richtet, wenn die betroffene Person bereits vor erfolgter Einholung einer richterlichen Entscheidung durch die anordnende Behörde den Rechtsweg beschreitet.

§ 77, der den Rechtsweg für Streitigkeiten nach den §§ 72 bis 74 und 76 bestimmt, bleibt von der normierten Regelungslage in § 25b ausdrücklich unberührt.

§ 26 (Einwilligung)

In § 26 finden sich die Voraussetzungen einer wirksamen Einwilligung. Die Vorschrift orientiert sich inhaltlich an § 51 des Bundesdatenschutzgesetzes, wobei die Vorschrift hier für den gesamten Aufgabenbereich der Behörden nach dem SOG M-V gilt. Die Richtlinie (EU) 2016/680 selbst enthält zwar keine Pflicht zur Regelung einer Einwilligung. Dazu wird im Erwägungsgrund 35 ausgeführt:

„*Bei der Wahrnehmung der ihnen als gesetzlich begründeter Institution übertragenen Aufgaben, Straftaten zu verhüten, zu ermitteln, aufzudecken und zu verfolgen, können die zuständigen Behörden natürliche Personen auffordern oder anweisen, ihren Anordnungen nachzukommen. In einem solchen Fall sollte die Einwilligung der betroffenen Person im Sinne der Verordnung (EU) 2016/679 keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden darstellen.*

Wird die betroffene Person aufgefordert, einer rechtlichen Verpflichtung nachzukommen, so hat sie keine echte Wahlfreiheit, weshalb ihre Reaktion nicht als freiwillig abgegebene Willensbekundung betrachtet werden kann. Dies sollte die Mitgliedstaaten nicht daran hindern, durch Rechtsvorschriften vorzusehen, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke dieser Richtlinie zustimmen kann, beispielsweise im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung ihres Aufenthaltsorts mittels elektronischer Fußfessel zur Strafvollstreckung.“

Daraus ergibt sich, dass die Richtlinie (EU) 2016/680 den Mitgliedstaaten die Möglichkeit einer Regelung der Einwilligung einräumt, wobei die Frage, ob eine Einwilligung wirksam erteilt werden kann - das zeigen auch die genannten Beispiele im Erwägungsgrund 35 - jeweils von den Umständen des Einzelfalls abhängig ist. Zur Vereinheitlichung der Regelungslage in den Anwendungsbereichen der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2016/679 sowie einer praktischen Handhabbarkeit durch die Polizei und Ordnungsbehörden ist die Schaffung einer Rechtsvorschrift erforderlich.

Absatz 1 stellt klar, dass die Verarbeitung personenbezogener Daten auch auf Grundlage einer Einwilligung erfolgen darf. In Satz 2 ist mit dem Verweis auf die Erteilung einer Einwilligung der § 8 Absatz 2 des Landesdatenschutzgesetzes (in der Fassung vom 20. Mai 2011) aufgegriffen worden. Die Nachweispflicht für die erteilte Einwilligung ergibt sich aus Artikel 7 Absatz 1 der Verordnung (EU) 2016/679.

Absatz 2 regelt die Anforderungen an die Gestaltung des Schriftstücks bei Abgabe einer schriftlichen Einwilligung, wenn mit ihr gleichzeitig andere Erklärungen eingeholt werden sollen. Die Vorschrift greift teilweise Formulierungen des § 8 Absatz 1 Satz 3 des Landesdatenschutzgesetzes (in der Fassung vom 20. Mai 2011) auf. Die Einwilligungserklärung ist in den genannten Fällen schon durch die Textgestaltung äußerlich besonders kenntlich zu machen und inhaltlich derart abzufassen, dass die betroffene Person erkennen kann, auf welchen Teil der Erklärung sich die von ihr abgegebene Einwilligung bezieht.

Absatz 3 ist inhaltsgleich mit § 51 Absatz 5 des Bundesdatenschutzgesetzes. Dieser deckt sich im Wesentlichen mit § 8 Absatz 2 des Landesdatenschutzgesetzes (in der Fassung vom 20. Mai 2011) und stellt klar, dass aus einer Einwilligung in die Verarbeitung besonderer personenbezogener Daten, die in § 3 Absatz 5 Nummer 3 aufgeführt sind, ausdrücklich der Bezug zu genau diesen Daten hervorgehen muss. Damit wird der besonderen Schutzwürdigkeit dieser Daten Rechnung getragen.

Inhalt und Umfang der Aufklärung der betroffenen Person vor Abgabe einer Einwilligung regelt Absatz 4. Er entspricht der Vorschrift des § 8 Absatz 2 des Landesdatenschutzgesetzes (in der Fassung vom 20. Mai 2011).

Absatz 5 Satz 1 entspricht § 8 Absatz 1 Satz 6 des Landesdatenschutzgesetzes (in der Fassung vom 20. Mai 2011). Er regelt, dass die betroffene Person vor Abgabe der Einwilligung über ihr Recht zur Verweigerung der Einwilligung und ihr für die Zukunft wirkendendes Recht auf Widerruf der erteilten Einwilligung sowie über die jeweiligen Rechtsfolgen aufzuklären ist. Satz 2 bestimmt, dass der Widerruf der Einwilligung so einfach wie die Erteilung der Einwilligung sein muss.

Absatz 6 entspricht § 51 Absatz 4 Satz 1 und 2 des Bundesdatenschutzgesetzes.

§ 26a (Schutz des Kernbereiches privater Lebensgestaltung)

Zur Umsetzung der Vorgaben des Bundesverfassungsgerichtes wird mit § 26a der Schutz des Kernbereiches privater Lebensgestaltung geregelt.

Nach der Rechtsprechung des Bundesverfassungsgerichtes müssen bei eingriffsintensiven Maßnahmen mit genereller Relevanz für den Kernbereich privater Lebensgestaltung einer Person sowohl auf der Erhebungsebene als auch in der Auswertungsphase hinreichende Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung getroffen werden (vergleiche Bundesverfassungsgerichtsurteil vom 27. Februar 2008 - Aktenzeichen 1 BvR 370/07 - Randnummern 270 ff; Beschluss des Zweiten Senats des Bundesverfassungsgerichtes vom 12. Oktober 2011 - Aktenzeichen 2 BvR 236/08 - Randnummer 209; Entscheidung des Bundesverfassungsgerichtes zum Bundeskriminalamtgesetz vom 20. April 2016 - 1 BvR 966/09 -, dort Randnummern 119 bis 129).

Zum Umfang des Kernbereichsschutzes führt das Bundesverfassungsgericht in seinem Urteil zum Bundeskriminalamtgesetz vom 20. April 2016 unter den Randnummern 120 bis 122 Folgendes aus:

„Der verfassungsrechtliche Schutz des Kernbereichs privater Lebensgestaltung gewährleistet dem Individuum einen Bereich höchstpersönlicher Privatheit gegenüber Überwachung. Er wurzelt in den von den jeweiligen Überwachungsmaßnahmen betroffenen Grundrechten in Verbindung mit Art. 1 Abs. 1 GG und sichert einen dem Staat nicht verfügbaren Menschenwürdekern grundrechtlichen Schutzes gegenüber solchen Maßnahmen. Selbst überragende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Bereich privater Lebensgestaltung nicht rechtfertigen (vgl. BVerfGE 109, 279 <313>; stRspr). Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen (vgl. BVerfGE 109, 279 <313>; 120, 274 <335>; stRspr). Geschützt ist insbesondere die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens, die in der berechtigten Annahme geführt wird, nicht überwacht zu werden, wie es insbesondere bei Gesprächen im Bereich der Wohnung der Fall ist. Zu diesen Personen gehören insbesondere Ehe- oder Lebenspartner, Geschwister und Verwandte in gerader Linie, vor allem, wenn sie im selben Haushalt leben, und können Strafverteidiger, Ärzte, Geistliche und enge persönliche Freunde zählen (vgl. BVerfGE 109, 279 <321 ff.>). Dieser Kreis deckt sich nur teilweise mit dem der Zeugnisverweigerungsberechtigten. Solche Gespräche verlieren dabei nicht schon dadurch ihren Charakter als insgesamt höchstpersönlich, dass sich in ihnen Höchstpersönliches und Alltägliches vermischen (vgl. BVerfGE 109, 279 <330>; 113, 348 <391 f.>).

Demgegenüber ist die Kommunikation unmittelbar über Straftaten nicht geschützt, selbst wenn sie auch Höchstpersönliches zum Gegenstand hat. Die Besprechung und Planung von Straftaten gehört ihrem Inhalt nach nicht zum Kernbereich privater Lebensgestaltung, sondern hat Sozialbezug (vgl. BVerfGE 80, 367 <375>; 109, 279 <319 f., 328>; 113, 348 <391>). Dies bedeutet freilich nicht, dass der Kernbereich unter einem allgemeinen Abwägungsvorbehalt in Bezug auf öffentliche Sicherheitsinteressen steht.

Ein höchstpersönliches Gespräch fällt nicht schon dadurch aus dem Kernbereich privater Lebensgestaltung heraus, dass es für die Aufklärung von Straftaten oder Gefahren hilfreiche Aufschlüsse geben kann. Aufzeichnungen oder Äußerungen im Zwiegespräch, die zum Beispiel ausschließlich innere Eindrücke und Gefühle wiedergeben und keine Hinweise auf konkrete Straftaten enthalten, gewinnen nicht schon dadurch einen Gemeinschaftsbezug, dass sie Ursachen oder Beweggründe eines strafbaren Verhaltens freizulegen vermögen (vgl. BVerfGE 109, 279 <319>). Auch können trotz Straftatenbezugs Situationen, in denen Einzelnen gerade ermöglicht werden soll, ein Fehlverhalten einzugestehen oder sich auf dessen Folgen einzurichten, wie Beichtgespräche oder vertrauliche Gespräche mit einem Psychotherapeuten oder einem Strafverteidiger, der höchstpersönlichen Privatsphäre unterfallen, die dem Staat absolut entzogen ist (vgl. BVerfGE 109, 279 <322>). Ein hinreichender Sozialbezug besteht demgegenüber dann, wenn Gespräche - auch mit Vertrauenspersonen - sonst unmittelbar Straftaten zu ihrem Gegenstand haben (vgl. BVerfGE 109, 279 <319>).“

§ 26a orientiert sich an § 100d der Strafprozessordnung, greift ergänzend bereits bestehende Regelungen aus dem am 5. April 2018 in Kraft getretenen § 32a (Einsatz körpernah getragener Aufnahmegeräte durch die Polizei) auf und führt bestehende Vorschriften zusammen. Er stellt nun die im Rahmen von Datenerhebungsmaßnahmen nach dem SOG M-V stets zu beachtende Regelung zum Schutz des Kernbereichs privater Lebensgestaltung dar.

In Absatz 1 wird zunächst das Verbot der Durchführung einer Maßnahme, die auf die ausschließliche Erhebung kernbereichsrelevanter Daten ausgerichtet ist, verankert (siehe auch Bundesverfassungsgerichtsurteil zum Bundeskriminalamtgesetz vom 20. April 2016, Randnummer 125). Ein ausschließlicher Kernbereichsbezug kann vor allem dann vorliegen, wenn die betroffene Person mit Personen kommuniziert, zu denen sie in einem besonderen, den Kernbereich betreffenden Vertrauensverhältnis - wie zum Beispiel engsten Familienangehörigen, Geistlichen, Telefonseelsorgern, Strafverteidigern oder im Einzelfall auch Ärzten – steht. Soweit ein derartiges Vertrauensverhältnis für Ermittlungsbehörden erkennbar ist, dürfen Maßnahmen nicht durchgeführt werden. Umgekehrt besagt der in Absatz 1 vorangestellte Grundsatz nicht, dass Maßnahmen schon deshalb von vornherein unterlassen werden müssen, weil auch Tatsachen mit erfasst werden können, die den Kernbereich des Persönlichkeitsrechts berühren (vergleiche zum Beispiel zur Maßnahme der Telekommunikationsüberwachung den Beschluss des Zweiten Senats des Bundesverfassungsgerichtes vom 12. Oktober 2011 - Aktenzeichen 2 BvR 236/08 -, Randnummern 215 f).

Absatz 2 regelt den möglichen Fall, dass im Rahmen von Maßnahmen, die nicht auf die Erhebung von kernbereichsrelevanten Daten ausgerichtet waren, im Laufe dieser auch solche Daten erhoben werden. Dann besteht ein absolutes Verwertungsverbot. Die Teile der Aufzeichnung, die Kernbereichsrelevanz besitzen, sind nach § 45 Absatz 2 Satz 1 Nummer 1 als unzulässig erhobene Daten zu löschen.

Um trotz der Löschung im Nachhinein das Einsatzgeschehen nachvollziehen zu können und insbesondere den Betroffenen Auskunft darüber erteilen zu können, wann Daten über sie - wenn auch nur kurzzeitig - erhoben wurden, ist die Tatsache der Erfassung der Daten sowie ihrer Löschung zu dokumentieren beziehungsweise zu protokollieren (Urteil des oben genannten Urteils des Bundesverfassungsgerichtes zum Bundeskriminalamtgesetz vom 20. April 2016, Randnummer 129). Dass auch für diese kernbereichsbezogenen Dokumentationen und Protokollierungen die §§ 46d und 46e gelten, wird zur Klarstellung in die Norm aufgenommen.

Aufgrund des Kernbereichsbezuges gelten auch für diese Dokumentationen und Protokollierungen strengere Weiterverwendungsregelungen; sie dürfen daher lediglich zur Datenschutzkontrolle verwendet werden. Um eine wirksame Rechtmäßigkeitskontrolle zu ermöglichen, dürfen sie nicht vor Abschluss der Datenschutzkontrolle gelöscht werden. Diese Datenschutzkontrolle ist gemäß § 48b Absatz 6 im Abstand von längstens zwei Jahren zumindest stichprobenartig durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz durchzuführen. Nach Abschluss der Kontrolle wurde der ausschließliche Verwendungszweck der Dokumentationen beziehungsweise Protokollierungen erfüllt und sie sind nach § 45 Absatz 2 Satz 1 Nummer 4 zu löschen. Sind die Dokumentationen und Protokolle nicht von der Kontrolle der Landesbeauftragten oder des Landesbeauftragte für den Datenschutz betroffen gewesen, so sind sie nach vierundzwanzig Monaten zu löschen. Maßgeblich zur Berechnung der Frist ist der Tag der Erhebung der Daten.

Ergänzend ist anzumerken, dass nach § 46g Absatz 1 Satz 1 Nummer 6 eine Kennzeichnungspflicht besteht, wenn in automatisierten polizeilichen Verfahren nach § 42 kernbereichsrelevante Daten gespeichert wurden und diese nicht unverzüglich gelöscht werden konnten.

Absatz 3 stellt klar, dass Maßnahmen, in deren Verlauf sich Anhaltspunkte für eine Kernbereichsrelevanz ergeben, abzubrechen sind, sofern mit dem Abbruch keine Gefährdung der eingesetzten Polizeibeamtinnen und Polizeibeamten oder Vertrauenspersonen oder ihrer weiteren Verwendung verbunden wäre. Sofern bereits Aufzeichnungen gestartet wurden, sind diese soweit technisch möglich, unverzüglich zu unterbrechen, um den begangenen Eingriff möglichst gering zu halten (vergleiche Bundesverfassungsgerichtsurteil zum Bundeskriminalamtgesetz vom 20. April, Randnummern 126, 128). Die Vorschriften in Absatz 2 sind auch hier zu beachten. Die Einschränkung der technischen Möglichkeit trägt dem Umstand Rechnung, dass bei einigen Maßnahmen kein sofortiges Einwirken auf den Aufzeichnungsvorgang möglich ist. Dies kann beispielsweise bei einer Telekommunikationsüberwachungsmaßnahme nach § 33d der Fall sein, wenn die Daten über den Diensteanbieter angefordert werden und allein dieser einen Abbruch der Aufzeichnung vornehmen kann. Regelmäßig wird die Zeit zwischen der Feststellung der potenziellen Kernbereichsverletzung, der Mitteilung an den Diensteanbieter und dem Abbruch der Maßnahme durch diesen dazu beitragen, dass eine Kernbereichsverletzung nicht mehr gänzlich verhindert werden kann. Diesem Umstand wird jedoch durch spezielle Regelungen zur Datenverwendung (siehe bezüglich Telekommunikationsüberwachungsmaßnahmen § 33d Absatz 8) Rechnung getragen.

Zudem unterliegt zum Beispiel die Anordnung der Telekommunikationsüberwachung bereits einem Richtervorbehalt (siehe § 33d Absatz 4). Die gerichtliche Entscheidung ist unter Abwägung des speziellen Risikos einer Kernbereichsverletzung und dem Maßnahmenziel zu treffen. Ungeachtet der Unmöglichkeit zur Unterbrechung des technischen Aufzeichnungsvorgangs ist beispielsweise bei Telekommunikationsüberwachungsmaßnahmen nach § 33d, bei denen neben der technischen Ausleitung und Aufzeichnung der Daten zeitgleich eine Person mithört und eine Kernbereichsverletzung festgestellt, das Mithören durch diese Person unverzüglich abzubrechen. Sofern händische Mitschriften angefertigt werden, sind auch diese unverzüglich zu unterlassen und kernbereichsrelevante Teile zu vernichten.

Gemäß Satz 3 darf ein Aufzeichnungsvorgang nur fortgesetzt werden, wenn sich die Umstände derart geändert haben, dass keine Kernbereichsverletzung mehr zu befürchten ist. Mit Satz 4 wird zudem bestimmt, dass die Tatsache der Unterbrechung und der Fortsetzung zu dokumentieren oder zu protokollieren ist. Die Vorschrift des Absatzes 2 Satz 3 gilt entsprechend, sodass auch diese Dokumentationen und Protokollierungen ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden dürfen; sie sind frühestens nach Abschluss der Datenschutzkontrolle gemäß § 48b Absatz 6 und spätestens nach vierundzwanzig Monaten zu löschen.

Soweit das Gesetz nichts Besonderes bezüglich der Datenverwendung bestimmt - vergleiche etwa zur Wohnraumüberwachung in § 33b Absatz 7 und 8 oder zur Online-Durchsuchung in § 33c Absatz 9 und 10 oder zur Telekommunikationsüberwachung in § 33d Absatz 8 - enthalten die Absätze 4 und 5 Regelungen zur Datenverwendung.

Absatz 4 sieht die seitens der Rechtsprechung geforderten Vorkehrungen auf der Verwertungsebene vor. Aufgrund des besonderen Schutzbereiches von Wohn- und Geschäftsräumen und befriedetem Besitztum, in denen eine kernbereichsrelevante Unterhaltung oder Handlung von Natur aus wahrscheinlicher ist, wird vor einer Verwendung von dort erhobenen Daten eine richterliche Entscheidung über die Rechtmäßigkeit der Datenerhebung und damit auch eine richterliche Auswertung der erhobenen Daten vorgesehen. Ein Anwendungsbeispiel ist die Verwendung von Daten, die mit einer Bodycam in Wohnungen nach § 32a aufgezeichnet wurden. Die Regelung in Absatz 4 schließt auch Unterbrechungsfälle des Absatzes 3 in Wohn- und Geschäftsräumen und befriedetem Besitztum ein. Die richterliche Entscheidung ist also vor der Verwendung der erhobenen Daten aus den vorgenannten sensiblen Bereichen auch in Fällen, in denen eine Unterbrechung der Aufzeichnungen nach Absatz 3 erfolgte, oder bei einer Fortsetzung der Datenerhebung nach Absatz 3 Satz 3 erforderlich.

Die gerichtliche Zuständigkeit richtet sich nach § 25b. Da jedoch im Einzelfall die Dringlichkeit der benötigten Daten derart hoch sein kann, dass eine richterliche Entscheidung nicht rechtzeitig erwirkt werden könnte, ist nach Satz 2 bei Gefahr im Verzug eine Entscheidung über die Datenverwendung durch die Behördenleitung (die Behördenleiterin oder der Behördenleiter in Persona oder die Vertretung im Amt) oder eine von ihr besonders beauftragte Beamtin oder einen besonders beauftragten Beamten zugelassen. Diese haben in einem Eilfall die erhobenen Daten vorzusichten. Wird bei dieser Sichtung festgestellt, dass kernbereichsrelevante Daten miterhoben wurden, sind diese aufgrund des absoluten Verwertungsverbotes unverzüglich zu löschen.

Lediglich nicht kernbereichsrelevante Daten dürfen die Behördenleitung oder die von ihr besonders beauftragte Beamtin oder der von ihr besonders beauftragte Beamte zur weiteren Verwendung zulassen. Ob die im Eilfall getroffene Entscheidung zur Verwendung der erhobenen Daten zulässig war, wird durch das normierte unverzügliche Nachholen der richterlichen Entscheidung kontrolliert.

Wird durch die Richterin oder den Richter die Unzulässigkeit der Datenerhebung festgestellt, sind die betroffenen Teile der Aufzeichnung nach § 45 Absatz 2 Satz 1 Nummer 1 zu löschen. Wird in den Fällen von Gefahr im Verzug nachträglich richterlich festgestellt, dass Daten unzulässig erhoben wurden und sind diese Daten gegebenenfalls an andere Stellen übermittelt worden, so ist der Empfänger nach § 45 Absatz 5 über die Unzulässigkeit der Datenverwendung zu informieren. In diesem Fall hat mithin auch der Empfänger die Daten unverzüglich nach § 45 Absatz 2 Satz 1 Nummer 1 zu löschen.

Weiterhin zu beachten sind die Benachrichtigungspflichten aus § 46a Absatz 1 Satz 1 Nummer 3. Von Absatz 4 unberührt bleiben Spezialregelungen wie in § 33c (siehe insbesondere die Begründung zu § 33c Absatz 9 und 10).

Absatz 5 trifft unter Berücksichtigung der bundesverfassungsgerichtlichen Vorgaben Vorkehrungen auf Verwertungsebene für die Daten, die in Fällen einer Unterbrechung nach Absatz 3 erhoben wurden und nicht bereits von der Regelung in Absatz 4 zu Datenerhebungen in Wohn- oder Geschäftsräumen oder auf befriedetem Besitztum erfasst sind. Bei diesen Daten besteht im Vergleich zu Absatz 4 aufgrund des Fehlens des besonderen Schutzbereiches von Natur aus ein geringeres Risiko für die Erhebung kernbereichsrelevanter Daten. Da es jedoch in Unterbrechungsfällen zuvor zu kernbereichsrelevanten Vorkommnissen gekommen ist, muss durch spezielle Anforderungen an die Auswertung der Daten vor ihrer Verwendung ausgeschlossen werden können, dass - auch nicht nur geringfügig - kernbereichsrelevante Daten erhoben worden sind. Hierzu bedarf es nach der aktuellen bundesverfassungsgerichtlichen Rechtsprechung ebenfalls der vorherigen Datensichtung durch eine unabhängige Stelle, die jedoch nicht zwingend durch ein Gericht wahrgenommen werden muss (vergleiche Urteil des Bundesverfassungsgerichtes zum Bundeskriminalamtgesetz vom 20. April 2016, Randnummer 240). Diese unabhängige Stelle ist in den von Absatz 5 erfassten Unterbrechungsfällen die oder der behördliche Datenschutzbeauftragte, deren beziehungsweise dessen Unabhängigkeit durch die Bestimmungen auf EU-Ebene (siehe Artikel 37 ff der Verordnung (EU) 2016/679 und Artikel 32ff der Richtlinie (EU) 2016/680) und auch durch die Regelungen in § 48f dieses Gesetzes gewährleistet wird. Bei Gefahr im Verzug gelten die Regelungen des Absatzes 4 Satz 2 entsprechend. Das heißt, dass bei Gefahr im Verzug ebenfalls die Behördenleitung oder eine von ihr besonders beauftragte Beamtin oder ein von ihr besonders beauftragter Beamter die Daten vorsichten und über deren Verwendung entscheiden kann. Im Fall einer solchen Eilentscheidung ist aber die Entscheidung der oder des behördlichen Datenschutzbeauftragten zur Rechtmäßigkeit der Datenerhebung unverzüglich nachzuholen. Stellt sich im Rahmen der nachträglichen Kontrolle heraus, dass Daten unzulässig erhoben wurden, und sind diese Daten gegebenenfalls an andere Stellen übermittelt worden, so ist der Empfänger nach § 45 Absatz 5 über die Unzulässigkeit der Datenverwendung zu informieren und er ist auch der Löschpflicht nach § 45 Absatz 2 Satz 1 Nummer 1 unterworfen.

§ 26b (Schutz von zeugnisverweigerungsberechtigten Personen)

Mit § 26b wird eine zentrale Regelung zum Schutz von zeugnisverweigerungsberechtigten Personen im SOG M-V geschaffen. Die bisher in § 33 Absatz 6 bestehenden Vorschriften werden unter Berücksichtigung der bundesverfassungsgerichtlichen Vorgaben und in Anlehnung an § 62 des Bundeskriminalamtgesetzes und § 9a des Polizeigesetzes Baden-Württemberg (in der ab 8. Dezember 2017 geltenden Fassung) überarbeitet.

Absatz 1 Satz 1 regelt, dass Maßnahmen grundsätzlich unzulässig sind, wenn sie sich gegen einen in § 53 Absatz 1 der Strafprozessordnung genannten Berufsgeheimnisträger richten und dadurch voraussichtlich Erkenntnisse erbringen würden, über die diese Personen das Zeugnis verweigern dürften. Das Befragungsrecht und die Auskunftspflicht nach § 28 bleiben davon unberührt. Maßnahmen, die sich gegen andere Personen - etwa einen Störer, potenziellen Straftäter oder einen Dritten - richten, bleiben dagegen zulässig, und zwar auch dann, wenn nicht ausgeschlossen werden kann oder gar zu erwarten ist, dass möglicherweise auch die Kommunikation mit den vorgenannten Berufsgeheimnisträgern über vom Zeugnisverweigerungsrecht umfasste Inhalte betroffen sein wird. Satz 3 beinhaltet ein Verwertungsverbot für entsprechende Aufzeichnungen nach Satz 1. Durch Verweis auf § 26a Absatz 2 Satz 2 und 3 in Satz 3 wird geregelt, dass Aufzeichnungen über Erkenntnisse nach Satz 1 unverzüglich gemäß § 45 zu löschen sind und die Tatsache ihrer Erlangung und Löschung gemäß § 46d zu dokumentieren ist; für die Protokollierung gilt auch hier § 46e. Die Dokumentation und entsprechende Protokollierung dürfen ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden; sie sind frühestens nach Abschluss der Datenschutzkontrolle § 48b Absatz 6 und spätestens nach vierundzwanzig Monaten zu löschen (siehe auch Begründung zu § 26a Absatz 2).

Durch Satz 4 wird das Erhebungs- und Verwertungsverbot nach Satz 1 und 3 auch auf die Konstellation einer zufälligen oder unvorhergesehenen Betroffenheit des Berufsgeheimnisträgers, bei der Erkenntnissen erhoben werden, die - nicht zielgerichtet - von dem Berufsgeheimnisträger erlangt wurden und über die dieser das Zeugnis verweigern dürfte, ausgeweitet. Aus diesem Verwertungsverbot kann sich in besonderen Einzelfällen unter Anwendung des Grundsatzes der Verhältnismäßigkeit die Verpflichtung ergeben, die Maßnahme gegen einen Dritten zu unterbrechen, so wenn es sich etwa um einen verdeckten, in Echtzeit erfolgenden verdeckten Einsatz technischer Mittel zur Tonaufzeichnung (vergleiche zum Beispiel § 33 Absatz 1 Nummer 2) handelt und dabei ein Gespräch zum Beispiel als Verteidigergespräch erkannt wird. Damit wird einer etwaigen Fortdauer der Verletzung des Erhebungsverbots nach Satz 1 vorgebeugt und die Einhaltung des Verwertungsverbots nach Satz 2 abgesichert.

Nach Absatz 2 Satz 1 liegt kein Erhebungs- und Verwertungsverbot nach Absatz 1 vor, soweit die Erhebung zur Abwehr einer gegenwärtigen Gefahr für Leben, Gesundheit oder Freiheit erforderlich ist. Dies ist entsprechend Satz 2 jedoch nur für die in § 53 Absatz 1 Satz 1 Nummern 3 bis 3b und 5 genannten Berufsgeheimnisträger der Strafprozessordnung zulässig. Für alle anderen Berufsgeheimnisträger nach § 53 Absatz 1 Satz 1 der Strafprozessordnung (Nummern 1,2 und 4) sowie für einen Rechtsanwalt, eine nach § 206 der Bundesrechtsanwaltsordnung in eine Rechtsanwaltskammer aufgenommene Person oder einen Kammerrechtsbeistand ist das Erhebungs- und Verwertungsverbot absolut ausgestaltet. Die gewählte Formulierung des Satzes 2 orientiert sich an § 62 Absatz 1 Satz 7 des Bundeskriminalamtgesetzes.

Das Bundesverfassungsgericht hat die Unterscheidung zwischen Strafverteidigern und den in anderen Mandatsverhältnissen tätigen Rechtsanwälten als Abgrenzungskriterium für einen unterschiedlichen Schutz als verfassungsrechtlich nicht tragfähig erachtet (Bundesverfassungsgerichtsurteil zum Bundeskriminalamtgesetz vom 20. April 2016, Randnummer 257). Die entsprechende Ausweitung des Anwendungsbereiches in Satz 2 trägt diesem Umstand Rechnung und bezieht sämtliche Rechtsanwälte und Kammerrechtsbeistände in den Schutzbereich ein.

Ein umfassendes - absolutes - Erhebungs- und Verwertungsverbot ist nur gerechtfertigt, wenn ein absolut geschützter Belang dies erfordert. Das Bundesverfassungsgericht hat dies mit Blick auf die Menschenwürde hinsichtlich des seelsorgerischen Gesprächs mit einem Geistlichen sowie des Gesprächs mit dem Strafverteidiger angenommen (Bundesverfassungsgerichtsurteil vom 3. März 2004, Aktenzeichen 1 BvR 2378/98, Randnummer 148). Einbezogen in den absoluten Schutz werden auch die Parlamentsabgeordneten. Deren Zeugnisverweigerungsrecht weist zwar keinen unmittelbaren Bezug zu dem Kernbereich privater Lebensgestaltung auf. Die Kommunikation mit Parlamentsabgeordneten steht aber unter einem besonderen Schutz. Artikel 47 des Grundgesetzes, Artikel 24 Absatz 3 der Landesverfassung und vergleichbare Regelungen in anderen Landesverfassungen geben für Parlamentsabgeordnete ein Zeugnisverweigerungsrecht und ein dieses flankierendes Beschlagnahmeverbot vor. Sind aber bereits diese offenen Ermittlungsmaßnahmen gegenüber Parlamentsabgeordneten von deren Einverständnis beziehungsweise der Nichtausübung des Zeugnisverweigerungsrechts abhängig, so spricht der damit vom Grundgesetzgeber und den Landesverfassungsgebern intendierte weitreichende Schutz der Parlamentsabgeordneten dafür, auch andere Ermittlungsmaßnahmen zu untersagen, soweit das Zeugnisverweigerungsrecht der Parlamentsabgeordneten reicht (vergleiche hierzu auch Beschluss des 2. Senats des Bundesverfassungsgerichtes vom 12. Oktober 2011, Aktenzeichen 2 BvR 236/08 und andere, Randnummern 258 ff).

An der Tätigkeit der übrigen (in § 53 Absatz 1 Satz 1 Nummern 3 bis 3 b der Strafprozessordnung) bezeichneten Berufsgeheimnisträger besteht ebenfalls ein hohes öffentliches Interesse. Diese Tätigkeiten setzen ihrer Natur nach das Bestehen eines Vertrauensverhältnisses zwischen dem Berufsgeheimnisträger und demjenigen, der die Leistungen des Berufsgeheimnisträgers in Anspruch nimmt, voraus. Das in den Berufsgeheimnisträger gesetzte Vertrauen und das Recht auf informationelle Selbstbestimmung der mit dem Berufsgeheimnisträger in Kontakt tretenden Person gebieten tendenziell Zurückhaltung bei der Erhebung von Erkenntnissen aus der vom Zeugnisverweigerungsrecht des Berufsgeheimnisträgers geschützten Sphäre. Da der Tätigkeit der Beratungs- und Heilberufe in einem sozialen Rechtsstaat auch gesellschaftlich ein hoher Wert zukommt, dürfen Maßnahmen der Gefahrenabwehr, die diese Tätigkeit beeinträchtigen können, nur unter strikter Wahrung der Verhältnismäßigkeit angewandt werden. Dies stellt Absatz 2 sicher, indem er ausdrücklich bestimmt, dass ein Eingriff in die relativ geschützten Vertrauensverhältnisse, vorbehaltlich der Prüfung im Einzelfall, nur erfolgen darf, soweit dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit erforderlich ist. Das öffentliche Interesse an einer wirksamen Gefahrenabwehr rechtfertigt in solchen Fällen einen Eingriff in die entsprechenden Berufsgeheimnisse. Das öffentliche Interesse an den durch die zeugnisverweigerungsberechtigten Personen wahrgenommenen Aufgaben und dem individuellen Interesse an der Geheimhaltung der einem Berufsgeheimnisträger anvertrauten oder bekannt gewordenen Tatsachen tritt in solchen Fällen zurück.

Zudem wird in Absatz 2 eine Beschränkung der Datenverwendung bestimmt. Die nach Absatz 2 Satz 1 erhobenen Daten dürfen nur für den dort bezeichneten Zweck verwendet werden.

Nach Absatz 3 sind die Regelungen der Absätze 1 und 2 entsprechend anwendbar, soweit es sich um die in § 53a der Strafprozessordnung genannten Berufshelfer handelt.

Absatz 4 beinhaltet die sogenannte Verstrickungsregelung. Dies bedeutet, dass der von den Absätzen 1 bis 3 gewährleistete besondere Schutz des Verhältnisses zu einem Berufsgeheimnisträger nach Absatz 4 dann endet, wenn der Berufsgeheimnisträger selbst für die Gefahr, welche mit der in Rede stehenden Maßnahme abgewehrt werden soll, verantwortlich ist (vergleiche §§ 69, 70). Denn der Schutz der betroffenen Vertrauensverhältnisse oder der Institutionen an sich soll nicht zur Begründung von Geheimbereichen führen, in denen die Verursachung von Gefahren einer staatlichen Aufklärung schlechthin entzogen ist.

§ 27 (Allgemeine Befugnisse zur Datenerhebung)

§ 27 enthält - wie bisher - die allgemeinen Befugnisse zur Datenerhebung, er wird jedoch teilweise angepasst. Im Absatz 1 wird durch die Aufnahme der Nummern 5 und 6 klargestellt, dass unter den hier genannten Voraussetzungen auch personenbezogene Daten von unbekannten Personen und unbekannten oder identifizierten Toten erhoben werden dürfen. Soweit eine molekulargenetische Untersuchung zur Identitätsfeststellung erfolgen soll, enthält § 31a bereits eine spezielle Regelung.

Der bisher geltende Absatz 2 wird inhaltlich unverändert übernommen. Es erfolgen lediglich redaktionelle beziehungsweise sprachliche Anpassungen.

Der bisher geltende Absatz 3 wird mit dem neu eingefügten Verweis auf § 67c (terroristische Straftat) in seinem Anwendungsbereich an die bestehende Rechtslage angepasst, um Anwendungslücken zu schließen, soweit Straftaten nach § 67c nicht bereits von den in § 49 aufgeführten Straftaten von erheblicher Bedeutung erfasst sind. Insbesondere werden die zuvor in Nummer 1 miterfassten sogenannten Kontakt- und Begleitpersonen aus der Nummer 1 herausgelöst und in eine eigene Nummer 2 überführt. Die Voraussetzungen für eine Datenerhebung über diese Kontakt- und Begleitpersonen sind in Anlehnung an § 39 Absatz 2 Nummer 2 des Bundeskriminalamtgesetzes unter Berücksichtigung der Vorgaben des Bundesverfassungsgerichtes in seiner oben genannten Entscheidung vom 20. April 2016 präzisiert worden. Denn das Gericht führt unter der Randnummer 116 unter anderem aus:

„*Eine Anordnung von anderen heimlichen Überwachungsmaßnahmen ist auch unmittelbar gegenüber Dritten nicht schlechthin ausgeschlossen. In Betracht kommt insoweit eine Befugnis zur Überwachung von Personen aus dem Umfeld einer Zielperson, etwa von - näher einzugrenzenden - Kontaktpersonen oder Nachrichtenmittlern. Solche Befugnisse rechtfertigen sich aus der objektiven Natur der Gefahrenabwehr und der Wahrheitsermittlung im strafrechtlichen Ermittlungsverfahren. Ihre Erstreckung auf Dritte steht unter strengen Verhältnismäßigkeitsanforderungen und setzt eine spezifische individuelle Nähe der Betroffenen zu der aufzuklärenden Gefahr oder Straftat voraus.*

Hierfür reicht es nicht schon, dass sie mit einer Zielperson überhaupt in irgendeinem Austausch stehen. Vielmehr bedarf es zusätzlicher Anhaltspunkte, dass der Kontakt einen Bezug zum Ermittlungsziel aufweist und so eine nicht unerhebliche Wahrscheinlichkeit besteht, dass die Überwachungsmaßnahme der Aufklärung der Gefahr dienlich sein wird (vgl. BVerfGE 107, 299 <322 f.>; 113, 348 <380 f.>). Eine Überwachung von Personen, die - allein gestützt auf die Tatsache eines Kontaktes zu einer Zielperson - erst versucht herauszufinden, ob sich hierüber weitere Ermittlungsansätze erschließen, ist verfassungsrechtlich unzulässig. Dies hindert hinsichtlich solcher Kontaktpersonen allerdings von Verfassungs wegen nicht Ermittlungsmaßnahmen geringerer Eingriffstiefe mit dem Ziel, gegebenenfalls die Eingriffsschwelle für intensivere Überwachungsmaßnahmen zu erreichen.“

Die bisherigen Nummern 2 und 3 des Absatzes 3 werden durch die Einfügung der Nummer 2 zu den Nummern 3 und 4.

In Absatz 4 wird die bestehende polizeiliche Befugnis zur Erhebung besonderer personenbezogener Daten auch ohne Einwilligung der betroffenen Person nach § 26 auf den Fall der neu eingefügten Nummern 5 und 6 in Absatz 1 (unbekannte Personen und Tote) erstreckt. Die zudem vorgenommene Aufnahme des Falls des Absatzes 3 Nummer 2 muss erfolgen, da die Kontakt- und Begleitpersonen aus der bisher bestehenden Nummer 1 des Absatzes 3 herausgelöst werden und zukünftig gesondert in Absatz 3 Nummer 2 geregelt werden. Die Befugnis wird hier demnach nicht erweitert; diese Personen waren nach der alten Regelungslage bereits von Nummer 1 miterfasst.

Im SOG M-V und damit im § 27 Absatz 4 fehlt bisher eine Befugnis für die Erhebung besonderer personenbezogener Daten für die Ordnungsbehörden. Mit Satz 2 wird für die Fälle des Absatzes 1 Nummer 1 bis 3, 5 und 6 eine solche Befugnis geschaffen. Die Befugnis für eine Datenverarbeitung nach Absatz 3 Nummer 1 und 2 steht den Ordnungsbehörden nicht zur Verfügung, da diese Norm ausschließlich in die polizeiliche Zuständigkeit fällt.

Die bisher geltende Regelung in Absatz 5 wird mit folgenden Ergänzungen übernommen:

Satz 2 wird ergänzt um die Wörter „im Einzelfall“. Damit wird klargestellt, dass über die Aufzeichnungen von Anrufen, die zur polizeilichen Aufgabenerfüllung erforderlich und nicht von Absatz 1 abgedeckt sind, im jeweiligen Einzelfall zu entscheiden ist. Zusätzlich wird aus datenschutzrechtlichen Gründen ein neuer Satz 3 eingefügt. Danach soll die oder der Anrufende auf die Aufzeichnung nach Satz 2 hingewiesen werden, soweit dadurch die polizeiliche Aufgabenerfüllung nicht gefährdet wird. Diese Regelung existiert zum Beispiel auch im § 30 des Polizei- und Ordnungsbehördengesetz des Landes Rheinland-Pfalz. Der bisherige Satz 3 zur Löschung von Aufzeichnungen wird mit einer sprachlichen Anpassung zum Satz 4. Der bisherige Satz 4, der eine Ausnahme von der Löschung der Daten normiert, wird Satz 5. Demnach dürfen die Aufzeichnungen nur dann weiterverarbeitet werden, sofern die Daten zur Verfolgung von Straftaten oder Ordnungswidrigkeiten oder zur Erfüllung der in § 1 bezeichneten Aufgaben benötigt werden. Satz 5 stellt damit eine besondere Weiterverarbeitungsvorschrift dar.

§ 27a (Polizeiliche Anhalte- und Sichtkontrollen)

Die bisher geltende Befugnis wird mit folgenden Ergänzungen und Anpassungen übernommen:

Wie in § 27 Absatz 3 werden auch in § 27a Satz 1 Nummer 1 zusätzlich zu den Straftaten von erheblicher Bedeutung nach § 49 auch die terroristischen Straftaten nach § 67c aufgenommen. Damit darf die Polizei auch zur vorbeugenden Bekämpfung dieser Straftaten im öffentlichen Verkehrsraum Anhalte- und Sichtkontrollen durchführen. Es geht hier bei der Inaugenscheinnahme um eine optische Wahrnehmung durch die Polizei. Es bleibt - wie bisher - dabei, dass weitergehende Maßnahmen wie die Identitätsfeststellung oder Durchsuchungen nach dieser Norm nicht durchgeführt werden dürfen. Für derartige weitergehende Maßnahmen sind die Voraussetzungen in den dafür vorgesehenen speziellen Regelungen - vergleiche beispielsweise die bestehenden Befugnisse in den §§ 29 oder 53 - zu beachten. Dies bedeutet zum Beispiel, dass die Identitätsfeststellung nur zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr (§ 29 Absatz 1 Satz 1) in Betracht kommt. In den Fällen nach § 29 Absatz 1 Satz 2 wird grundsätzlich das Vorliegen von tatsächlichen Anhaltspunkten für die Zulässigkeit einer Identitätsfeststellung gefordert. Im Übrigen wird der bisher geltende § 27a Satz 1 unverändert übernommen.

Darüber hinaus werden die Regelungen zur Anordnung einer Maßnahme nach Satz 1 Nummer 1 an die übrigen Regelungen im Gesetz, die eine Anordnung erfordern, angepasst und präziser ausgestaltet. Der „Behördenleiter“ wird durch „die Leitung der zuständigen Polizeibehörde“ ersetzt und es wird klargestellt, dass die Anordnung grundsätzlich schriftlich ergehen muss. Um den Umständen der Praxis gerecht zu werden, ist eine Anordnung auch durch eine von der Behördenleitung besonders beauftragte Beamtin oder einen von ihr besonders beauftragten Beamten zulässig. Die Zahl der besonders beauftragten Personen sollte demzufolge jedoch entsprechend begrenzt sein. Zudem ist die Anordnung in zeitlicher und örtlicher Hinsicht auf den zur vorbeugenden Bekämpfung der in Nummer 1 aufgeführten Straftaten erforderlichen Umfang zu beschränken und sie ist auf höchstens einen Monat zu befristen und zu begründen. Damit sind die Anordnungsvoraussetzungen zeitnah einer Prüfung zu unterziehen. Eine Verlängerung der Maßnahme wird bei weiterem Vorliegen der Voraussetzungen nach dem vorstehend beschriebenen Verfahren zugelassen.

§ 28 (Befragung und Auskunftspflicht)

Der bisher geltende Absatz 1 wird unverändert übernommen.

Absatz 2 wird mit folgenden Änderungen übernommen:

In Absatz 2 Satz 2 wird zur Vermeidung von Rechtsunsicherheiten der Verweis auf § 136a der Strafprozessordnung präziser als bisher ausgestaltet. Mit den neu eingefügten Sätzen 3 und 4 erfolgt die Klarstellung, dass § 90 (Anwendung unmittelbaren Zwangs) keine Anwendung findet und § 26b (Schutz von zeugnisverweigerungsberechtigten Personen) unberührt bleibt. Die Sätze 3 und 4 orientieren sich an § 41 Absatz 4 des Bundeskriminalamtgesetzes. Die Sätze 5 und 6 entsprechen im Wesentlichen den bisherigen Sätzen 3 bis 5.

Ergänzt wird die bisherige Regelung unter Beachtung der bundesverfassungsgerichtlichen Vorgaben (siehe hierzu die Ausführungen zu § 26b) mit Satz 7 um ein Recht zur Auskunftsverweigerung in den Fällen des Satzes 6 für Berufsgeheimnisträger nach § 53 Absatz 1 Satz 1 Nummern 1, 2 und 4 der Strafprozessordnung sowie Rechtsanwälte, nach § 206 der Bundesrechtsanwaltsordnung in eine Rechtsanwaltskammer aufgenommene Personen oder Kammerrechtsbeistände. Die Regelung orientiert sich an § 41 Absatz 3 des Bundeskriminalamtgesetzes.

Zudem wird im neu aufgenommen Satz 8 ausdrücklich normiert, dass die betroffene Person über ihr Recht zur Verweigerung der Auskunft zu belehren ist.

§ 29 (Identitätsfeststellung)

Die Regelungen des bisher geltenden § 29 werden übernommen und wie folgt angepasst:

In Absatz 1 Satz 2 Nummer 4 Buchstabe b werden neben den Straftaten nach § 129a des Strafgesetzbuches nun auch die Straftaten nach § 67c aufgenommen. Damit sind Identitätsfeststellungen durch Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte auch an einer Kontrollstelle, die von der Polizei eingerichtet worden ist, um terroristische Straftaten gemäß § 67c zu verhüten, zulässig, soweit für die Begehung dieser Straftaten tatsächliche Anhaltspunkte bestehen.

In Absatz 2 wird zusätzlich bestimmt, dass Vollzugsbeamtinnen und Vollzugsbeamte der Ordnungsbehörden die betroffene Person - jedoch nur bis zum Eintreffen der Polizei - festhalten dürfen, wenn die Identität auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann. Damit wird einer Forderung der Ordnungsbehörden nachgekommen, da diese bei der Erfüllung ihrer Aufgaben immer wieder auf Situationen treffen, die eine solche Befugnis erforderlich machen. Auch andere Gefahrenabwehrgesetze der Länder normieren Festhalterechte für Ordnungsbehörden (vergleiche etwa § 13 Absatz 2 Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung, § 181 Absatz 3 des Landesverwaltungsgesetzes Schleswig-Holstein, § 15 Absatz 2 des Ordnungsbehördengesetzes Thüringen).

Darüber hinaus wird die sprachliche Gleichstellung in Absatz 1 Satz 2 sowie in Absatz 3 vollzogen.

In Absatz 4 erfolgt in Bezug auf den darin enthaltenen Verweis auf § 56 die Klarstellung, dass eine Freiheitsentziehung zum Zwecke der Identitätsfeststellung bei gerichtlicher Anordnung höchstens 3 Tage betragen darf. Die in § 56 Absatz 5 vorgesehene Höchstfrist eines Gewahrsams von 10 Tagen kommt hier also nicht in Betracht. Im Übrigen wird der enthaltene Verweis auf § 56 nun nicht mehr nur auf dessen Absätze 2 und 5, sondern vollumfänglich auf § 56 erstreckt. Durch die entsprechende Anwendung des § 56 gelangen nur diejenigen Vorschriften zur Anwendung, die sich auf den Fall der Identitätsfeststellung übertragen lassen.

§ 30 (Prüfung von Berechtigungsscheinen)

Keine Änderung

§ 31 (Erkennungsdienstliche Maßnahmen)

§ 31 wird mit Anpassungen übernommen.

Im Absatz 1 wird das Wort „Straftat“ durch die Wörter „mit Strafe bedrohten Handlung“ ersetzt. Durch das Anknüpfen an die künftige mit Strafe bedrohte Handlung statt an die Gefahr der Begehung weitere Straftaten wird deutlicher als bisher herausgestellt, dass es für die erkennungsdienstliche Maßnahme nach § 31 nicht zwingend auf die Schuldfähigkeit (vergleiche hierzu § 19 des Strafgesetzbuches), die unter anderem Voraussetzung für das Vorliegen einer Straftat ist, ankommt. Auch gegen strafunmündige Personen können unter den genannten Voraussetzungen sowie unter besonderer Berücksichtigung des Verhältnismäßigkeitsgrundsatzes erkennungsdienstliche Maßnahmen zum Zwecke der Gefahrenabwehr durchgeführt werden. Mit der Formulierungsänderung sollen bestehende Rechtsunsicherheiten bei der Normanwendung in der Praxis vermieden werden. Im Übrigen wird in Absatz 1 die sprachliche Gleichstellung vollzogen.

Der bisherige Absatz 2 wird unverändert übernommen und der bisher geltende Absatz 3 wird mit Blick auf die im Gesetz insgesamt erfolgten datenschutzrechtlichen Anpassungen sprachlich angepasst. Die bisher enthaltenen Regelungen zum Löschen erkennungsdienstlicher Daten und zur Vernichtung erkennungsdienstlicher Unterlagen können mit Blick auf § 45 Absatz 2 Satz 1 Nummer 4 entfallen.

In den Absatz 4 wird aus dem bisherigen Absatz 3 die Vorschrift, dass das Nähere durch Verwaltungsvorschrift geregelt wird, unter Aktualisierung der Bezeichnung des Innenressorts übernommen.

§ 31a (Molekulargenetische Untersuchung zur Identitätsfeststellung)

Die im § 31a enthaltene Befugnis zur molekulargenetischen Untersuchung zur Identitätsfeststellung wird übernommen und wie folgt angepasst.

In Absatz 1 erfolgen lediglich sprachliche Anpassungen. Unter anderem wird das Wort „Leiche“ durch das Wort „Tote“ ersetzt.

Wie bisher auch, wird in Absatz 2 Satz 1 die richterliche Anordnung der molekulargenetischen Untersuchung gesetzlich festgelegt. Neu ist jedoch die zusätzliche Bestimmung in Satz 1, dass der Antrag von der Leitung der zuständigen Polizeibehörde zu stellen ist. Welches Gericht für die Entscheidung zuständig ist und welche Regelungen für das Verfahren gelten, muss aufgrund der Neuregelung in § 25b nicht mehr bestimmt werden. Insbesondere kann daher der bisherige Satz 2 in § 31a entfallen.

Wie auch in anderen Normen im SOG M-V (vergleiche unter anderem die am 5. April 2018 in Kraft getretenen §§ 67a und 67b) wird mit dem neuen Satz 2 zusätzlich festgelegt, welche Angaben der Antrag zu enthalten hat.

Der neu eingefügte Absatz 3 Satz 1 sieht vor, dass die richterliche Anordnung schriftlich ergehen muss und Satz 2 bestimmt den Inhalt dieser. Satz 3 entspricht dem bisherigen Absatz 2 Satz 3, nach dem für die Durchführung der molekulargenetischen Untersuchungen § 81f Absatz 2 der Strafprozessordnung entsprechend gilt.

§ 32 (Einsatz technischer Mittel zur offenen Bild- und Tonaufnahme sowie zur Bild- und Tonaufzeichnung)

Der bisher geltende § 32 wird zur besseren Anwendbarkeit und Übersichtlichkeit der Norm neu strukturiert und in Teilen überarbeitet und ergänzt.

Absatz 1 kommt weiterhin im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen zur Anwendung. Die Normanwendung ist bei Versammlungen, die dem Versammlungsgesetz unterliegen, nach wie vor ausgeschlossen.

Nummer 1 entspricht § 32 Absatz 1 Satz 3 der derzeit geltenden Fassung.

Nummer 2 übernimmt zum einen § 32 Absatz 1 Satz 1 und 2 in der derzeit geltenden Fassung. Auch die Bodycam, deren Einsatz grundsätzlich in § 32a geregelt ist, kann als technisches Mittel zur offenen Bild- und Tonaufzeichnung im Rahmen von öffentlichen Veranstaltungen oder Ansammlungen eingesetzt werden, wobei ihr Einsatz dann jedoch an das Vorliegen der Voraussetzungen nach Nummer 1 gebunden ist.

An dieser Stelle wird klargestellt, dass der Begriff der „Bildaufnahme“ die videotechnische Beobachtung ohne Aufzeichnung (Beobachtung mittels Bildübertragung, sogenanntes Monitoring) meint, während unter dem Begriff der „Bildaufzeichnung“ darüber hinaus eine Speicherung der Aufnahmen zu verstehen ist. Somit handelt es sich bei der Bildaufnahme um eine sogenannte „Minus-Maßnahme“ zur Bildaufzeichnung, sodass, sofern gesetzlich eine Befugnis zur Bildaufzeichnung geregelt ist, immer auch eine Bildaufnahme als milderes Mittels zulässig ist. Entsprechend verhält es sich mit den Begriffen „Tonaufnahme“ (zum Beispiel Abhören des gesprochenen Wortes) und „Tonaufzeichnung“.

Dementsprechend ist unter den Voraussetzungen des § 32 Absatz 1 Nummer 2 Satz 1 lediglich eine Übersichtsaufnahme zur Beobachtung der Veranstaltung oder Ansammlung mittels Bildübertragung zulässig. Eine Speicherung dieser Übersichtsaufnahmen als tieferer Eingriff nach Nummer 2 Satz 2 ist hingegen nur unter den strengeren Voraussetzungen der Nummer 1 zulässig.

Die Übersichtsaufnahmen nach Nummer 2 Satz 1 sind zulässig, wenn es zur Lenkung und Leitung des polizeilichen oder ordnungsbehördlichen Einsatzes erforderlich ist. Dies kann beispielsweise aufgrund einer Unübersichtlichkeit der Veranstaltung oder Ansammlung oder aber der Örtlichkeit erforderlich sein. Ob es neben Aufnahmen zur Übertragung und Beobachtung in Echtzeit auch der (vorübergehenden) Speicherung in Form einer (Übersichts-) Aufzeichnung bedarf, ist im jeweiligen Einzelfall unter Beachtung des Grundsatzes der Verhältnismäßigkeit zu entscheiden. Nummer 2 Satz 2 stellt an die Anfertigung von Übersichtsaufzeichnungen sowie eine damit mögliche Identifikation Einzelner durch ein Hineinzoomen jedoch die gleichen höheren Voraussetzungen wie an Aufzeichnungen nach Nummer 1. Dies trägt dem Umstand Rechnung, dass von diesen Aufzeichnungen eine Vielzahl von Personen betroffen ist, für die häufig nicht ersichtlich sein wird, ob sie von der Aufnahme erfasst wurden. Die Identitätsfeststellung ist der Polizei vorbehalten.

Die Absätze 2 bis 4 entsprechen inhaltlich dem derzeitigen Absatz 3 Satz 1 bis 3 und werden lediglich sprachlich angepasst.

Absatz 5 entspricht im Wesentlichen dem derzeitigen Absatz 3 Satz 5 und 6. Dieser wird um eine Angabe des Mindestinhalts der Anordnung ergänzt. Mit Satz 3 wird dem Umstand Rechnung getragen, dass die oder der Landesbeauftragte für den Datenschutz gemäß § 16 des Landesdatenschutzgesetzes (in der ab 25. Mai 2018 geltenden Fassung) Aufsichtsbehörde nach Artikel 51 Absatz 1 Verordnung (EU) 2016/679 und Artikel 41 Absatz 1 der Richtlinie (EU) 2016/680 ist.

In Absatz 6 wird die Regelung, dass die Maßnahmen auch durchgeführt werden können, wenn Dritte unvermeidbar betroffen sind, als zentrale Vorschrift für die Maßnahmen nach den Absätzen 1 bis 4 getroffen. Auch die Anforderungen an die Offenheit der Maßnahmen werden hier zusammengefasst. Gefahr im Verzug wird regelmäßig nur bei Aufzeichnungen nach Absatz 1 vorliegen können, da die Maßnahmen nach Absatz 2 bis 4 einer längeren Vorbereitung, einschließlich einer Verfahrensbeschreibung nach § 42 Absatz 4 bedürfen. In Fällen des Absatzes 1 kann bei Veranstaltungen die Information über die Bildüberwachung zur Gewährleistung der Offenheit der Maßnahme auch durch die Veranstaltungsleitung erfolgen.

In Absatz 7 werden die unterschiedlichen Löschfristen für die Maßnahmen nach Absatz 1 und die Maßnahmen nach den Absätzen 3 und 4 geregelt. Die Löschfrist von einem Monat für Maßnahmen nach Absatz 1 (in Betracht kommen nur die Aufzeichnungsermächtigungen nach Nummer 2 und Nummer 3 Satz 2) entspricht der Frist nach Absatz 2 Satz 1 der derzeit geltenden Fassung für Maßnahmen nach Absatz 1 Nummer 2 (neu). Konsequenterweise wird auch für Übersichtsaufzeichnungen nach Absatz 1 Nummer 3 (neu) diese Frist festgesetzt, da dieselbe Eingriffsschwelle wie für Maßnahmen nach Absatz 1 Nummer 2 vorliegen muss. Satz 2 schreibt eine Löschfrist von zwei Wochen für Aufzeichnungen aus Maßnahmen nach Absatz 3 und 4 fest und passt diese so an die Frist aus § 32a Absatz 5 Satz 3 der derzeit geltenden Fassung an. Mit Blick auf die Erfahrungen der Praxis, die die Notwendigkeit einer längeren Speicherungsdauer zur Sichtung und Auswertung belegen, wird die vormalige Löschfrist von einer Woche somit erweitert. Gleichzeitig wird der betroffenen Person mehr Zeit zur Geltendmachung der Verletzung seiner Rechte gewährt. Eine Ausnahme von der Löschfrist (wie im jetzigen Absatz 2 Satz 2) wird nun dahingehend geregelt, dass eine Weiterverarbeitung zulässig ist, soweit das Gesetz dies vorsieht (siehe insbesondere sind die §§ 26a und 36 zu beachten) oder § 45 Absatz 5 eine Einschränkung der Verarbeitung zulässt.

In Absatz 8 wird die bisher in § 32 Absatz 5 enthaltene Ermächtigung zur Videoüberwachung an oder in polizeilichen Fahrzeugen neu formuliert. Zum einen wird die Norm sprachlich angepasst, zum anderen entsprechen die Voraussetzungen nun denen in der Befugnis zum Pre-Recording mittels Bodycam in § 32a Absatz 1. Zwar wird bei der Datenerhebung an oder in Polizeifahrzeugen keine nur vorübergehende, sondern eine dauerhafte Aufzeichnung vorgenommen, die Eingriffsintensität ist aufgrund der festen Position der Kamera an oder in den Fahrzeugen gegenüber des flexiblen Aufnahmebereiches der Bodycam jedoch nicht höher. Zudem ist bei der statischen Videoüberwachung keine unmittelbare Einflussnahme der Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten auf den Start beziehungsweise Stopp der Aufzeichnung möglich. Daher muss bereits eine „Vorgefahr“ ausreichen, um die Wirksamkeit der Maßnahme erreichen zu können.

Bei der Regelung in Absatz 8 handelt es sich nicht um eine Spezialregelung für Personen- und Fahrzeugkontrollen, sondern für die Installation fester Videoüberwachungstechnik an oder in Einsatzfahrzeugen. Ebenso wird kein zeitgleicher Einsatz von Bodycams nach § 32a ausgeschlossen. Auch bei Maßnahmen nach Absatz 8 gilt eine zweiwöchige Löschfrist, sofern die Aufzeichnungen nicht nach diesem Gesetz weiterverarbeitet werden dürfen oder § 45 Absatz 3 eine Einschränkung der Verarbeitung vorsieht. Die Vorschriften zur Offenheit einer Maßnahme und zur Drittbetroffenheit aus Absatz 6 gelten gleichermaßen.

Mit Absatz 9 wird eine Ermächtigung zur Videoüberwachung in polizeilichen Räumen, die zur Durchführung der Gewahrsamnahme genutzt werden, geschaffen. Hierzu zählen alle Räumlichkeiten, die von der Polizei zur Vorbereitung und Durchführung eines Gewahrsams genutzt werden (meist die Gewahrsamszellen selbst sowie deren Vorräume). Die Einführung einer solchen Videoüberwachung ist sowohl zum Schutz der in Gewahrsam genommenen Personen (beispielsweise vor Suizid, gesundheitlichem Notfall, Übergriffen anderer Personen), als auch der an der Gewahrsamnahme beteiligten anderen Personen - wie vor allem Polizeivollzugsbeamtinnen und Polizeibeamten - notwendig.

Auch andere Bundesländer, wie etwa Hamburg oder das Saarland, verfügen bereits über eine solche Befugnisnorm. Sie reagierten damit auf Fälle wie den des „Ouri Jalloh“ aus Sachsen-Anhalt, der in einer Gewahrsamszelle verstorben ist. Der Bundesgerichtshof hat in seinem dazu ergangenen Urteil vom 4. September 2014, Aktenzeichen 4 StR 473/13, ausgeführt, dass in solchen Fällen, in denen beispielsweise eine Selbstgefährdung anzunehmen ist, eine permanente optische Überwachung notwendig ist (siehe Randnummer 31 a. a. O.). Bereits 2010 hat zudem die AMNESTY INTERNATIONAL Sektion der Bundesrepublik Deutschland e. V. „die Einrichtung und Ausweitung der Video- und Audioüberwachung in allen Bereichen von Polizeiwachen, in denen sich Inhaftierte aufhalten“, empfohlen, „sofern dies nicht das Persönlichkeitsrecht oder das Recht auf vertrauliche Gespräche mit ihrem Rechtsbeistand oder Arzt verletzt.“

Auch in Mecklenburg-Vorpommern gab es in der Vergangenheit Vorfälle, die die Notwendigkeit einer Videoüberwachung untermauern. So ereignete sich beispielsweise am 18. Oktober 2011 ein Übergriff auf einen Polizeivollzugsbeamten im Zentralgewahrsam in einer Polizeiinspektion. Der Beamte war aufgrund der Situation nicht in der Lage, einen im Flur vor den Gewahrsamszellen angebrachten Notfall-Knopf zu betätigen. Im Falle einer installierten Videoüberwachung hätte eine überwachende Polizeivollzugsbeamtin oder ein überwachender Polizeivollzugsbeamter - selbst oder durch Alarmierung anderer - Hilfe leisten können.

Die Möglichkeit, neben der reinen Beobachtung auch Aufzeichnungen vorzunehmen, bietet neben der möglichen präventiven Wirkung durch eine offene Videoüberwachung den Vorteil der Beweissicherung zur erleichterten Strafverfolgung. Hierdurch kann insbesondere der Vorlauf zu etwaigen Tätlichkeiten, denen häufig verbale Auseinandersetzungen vorausgehen, festgehalten werden.

Unabhängig von der Frage einer Aufzeichnung kommt auch der Tonüberwachung eine gesonderte Bedeutung zu. Sie kann zum Beispiel gewährleisten, dass den in den Gewahrsamsräumen befindlichen Polizeivollzugskräften rechtzeitig Hilfe geleistet werden kann, sollte sich bereits aus dem verbalen Verhalten der im Gewahrsam befindlichen Person eine sich konkretisierende Gefahr ergeben.

Andererseits kann die Tonüberwachung erst die Abwendung einer Gefahr von der Person im Gewahrsam ermöglichen, wenn sich diese etwa aufgrund ihres körperlichen Zustands nur akustisch bemerkbar machen kann. Jedoch ist keine anlasslose, dauerhafte Überwachung gemeint. Vielmehr ist anhand der Umstände des Einzelfalls abzuwägen, ob eine Überwachung zum Schutz einer Person erforderlich ist.

Dass auch bei der Videoüberwachung nach § 32 Absatz 9 keine kernbereichsrelevanten Daten aufgezeichnet werden dürfen, ergibt sich aus der allgemeinen Geltung des § 26a und ist in der Praxis insbesondere bei Toilettenbereichen innerhalb von Zellen von Relevanz.

Aufzeichnungen nach Absatz 9 sind nach zwei Wochen zu löschen, es sei denn, sie dürfen nach § 36 weiterverarbeitet werden. Die Vorschriften zur Offenheit einer Maßnahme und zur Drittbetroffenheit aus Absatz 6 gelten gleichermaßen.

In Absatz 10 wird klarstellend aufgenommen, dass die Polizei Bild- und Tonaufzeichnung zur Suche von Personen, deren Leben oder Gesundheit gefährdet ist, anfertigen darf. Diese Maßnahme ist jedoch nur zulässig, wenn die Erfüllung der polizeilichen Aufgabe auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Vorschriften in Absatz 6 zur Offenheit der Maßnahme und zur Drittbetroffenheit gelten entsprechend. Zudem wird festgelegt, dass nach Abschluss der Maßnahme die erhobenen personenbezogenen Daten unverzüglich zu löschen sind. Dies gilt nicht, soweit nach diesem Gesetz eine Weiterverarbeitung zulässig ist oder § 45 Absatz 3 eine Einschränkung der Verarbeitung vorsieht.

Die Ermächtigung zur Videoüberwachung aufgrund des Hausrechts (beispielsweise zur Vermeidung von Sachbeschädigungen) ist von § 32 nicht umfasst. Eine Regelung hierzu findet sich in § 11 des Landesdatenschutzgesetzes.

§ 32a (Einsatz körpernah getragener Aufnahmegeräte)

Der bisher geltende § 32a wird mit redaktionellen Anpassungen übernommen und aufgrund der Schaffung allgemeiner Regelungen (§§ 26a und 26b) sowie von Verweisen in § 32 entsprechend gekürzt.

Aufgrund der neu eingeführten Definition des „Dritten“ in § 3 Absatz 4 wird in den bisher geltenden Absätzen 1 bis 3 eine Klarstellung der Bedeutung im Zusammenhang des § 32a eingeführt. Absatz 3 wird zudem an den Sprachgebrauch des § 26a Absatz 4 angepasst.

Der bisher geltende Absatz 4 wird durch einen Verweis auf § 32 Absatz 6 um die nun bereits dort enthaltenen Regelungen zur Betroffenheit unbeteiligter Dritter und die Anforderungen an die Offenheit der Maßnahme, einschließlich der Regelung bei Gefahr im Verzug, ersetzt. Die Regelungen zu Aufzeichnungen mit Kernbereichsrelevanz sowie in Bereichen zeugnisverweigerungsberechtigter Personen sind inklusive besonderer Dokumentations- und Protokollierungspflichten nun in den allgemeinen §§ 26a und 26b enthalten und können daher in § 32a entfallen.

Der bisher geltende Absatz 5 wird übernommen und durch eine Bezugnahme auf § 26a Absatz 3 und auch auf § 32 Absatz 7 Satz 3 an die neue datenschutzrechtliche Regelungslage angepasst. Auch bei Aufzeichnungen, die im Rahmen eines Bodycam-Einsatzes auf dem dauerhaften Speichermedium gespeichert wurden, gilt die Löschfrist von zwei Wochen. Sie gilt aber nicht, soweit eine Weiterverarbeitung nach dem Gesetz zulässig ist oder § 45 Absatz 3 eine Einschränkung der Verarbeitung ermöglicht (siehe auch die Begründung zu § 32 Absatz 7). Die Löschung ist gemäß § 46d Absatz 1 Satz 1 Nummer 3 zu dokumentieren.

Die bisher geltenden Absätze 6 und 7 können aufgrund der in § 36 allgemein geregelten Vorschrift zur Datenweiterverarbeitung, der allgemeinen Regelung zur Löschung nach § 45 und zur Dokumentation nach § 46d entfallen. Auch die in Absatz 7 bisher enthaltenen Regelungen zur Verwertung von Aufzeichnungen sind aufgrund der Regelungen in § 26a entbehrlich.

Die Weiterverwendung von Daten zur Aus- und Fortbildung sowie Statistik ist nun in § 37a geregelt, sodass der bisher geltende Absatz 8 entfällt.

Der bisher geltende Absatz 9 wird unverändert als Absatz 6 in § 32a übernommen.

§ 33 (Besondere Mittel der Datenerhebung)

Der bisher geltende Absatz 1 wird in Nummer 1 wie folgt angepasst:

Die Umbenennung der verdeckten Maßnahme der „Observation“ in „längerfristige Observation“ und die Anpassung der Definition an die Regelung in § 45 Absatz 2 Nummer 1 (vorher § 20g Absatz 2 Nummer 1 in der außer Kraft getretenen Fassung) des Bundeskriminalamtgesetzes erfolgt im Zuge der Umsetzung der Vorgaben des Bundesverfassungsgerichtes in seinem Urteil vom 20. April 2016 (siehe Randnummer 174; Punkt 4 des Tenors). Dazu hat es ausgeführt:

„Demgegenüber ist eine unabhängige Kontrolle verfassungsrechtlich aber unverzichtbar, wenn Observationen im Sinne des § 20g Abs. 2 Nr. 1 BKAG längerfristig - zumal unter Anfertigung von Bildaufzeichnungen oder unter Nutzung besonderer technischer Mittel wie Peilsender - durchgeführt werden, wenn nichtöffentliche Gespräche erfasst oder Vertrauenspersonen eingesetzt werden. Diese Maßnahmen dringen unter Umständen so tief in die Privatsphäre ein, dass deren Anordnung einer unabhängigen Instanz, etwa einem Gericht, vorbehalten bleiben muss. Insoweit reicht es nicht, die Anordnung der Maßnahmen zunächst der Sicherheitsbehörde selbst zu überlassen und die disziplinierende Wirkung wegen des Erfordernisses einer richterlichen Entscheidung erst für deren Verlängerung - möglicherweise auf der Grundlage der so gewonnenen Erkenntnisse - vorzusehen.“

Wenn das Bundesverfassungsgericht nunmehr bereits die bestehende, im Vergleich zu § 33 Absatz 1 Nummer 1 weitergehende Definition für eine (längerfristige) Observation als besonders eingriffsintensiv bezeichnet und einem Richtervorbehalt unterwirft (Punkt 4 des Tenors), dann bedarf es neben der Regelung eines Richtervorbehaltes auch einer Anpassung der Definition und damit der konkreten Maßnahmen, die in zeitlicher Hinsicht darunter fallen.

Der Richtervorbehalt nach der Rechtsprechung des Bundesverfassungsgerichtes gilt nämlich bereits für Observationen, die zeitlich von der Definition in § 33 Absatz 1 Nummer 1 noch nicht erfasst sind. Insofern müssen diese Fälle neben einem Richtervorhalt bereits den gehobenen Voraussetzungen in § 33 Absatz 2 unterworfen werden. Anderenfalls läge ein verfassungsrechtlicher Wertungswiderspruch vor.

Die bisher geltende Regelung in Absatz 1 Nummer 2 wird abgesehen von einer sprachlichen Anpassung unverändert übernommen. Absatz 1 Nummer 3 entspricht der bisherigen Regelung und wird zur Klarstellung um einen Klammerzusatz mit dem Verweis auf die in § 3 Absatz 4 Nummer 2 aufgenommen Definition des Dritten und um einen Klammerzusatz mit dem Wort „Vertrauensperson“ ergänzt. Der bisher geltende Absatz 1 Nummer 4 wird unter Vollzug der sprachlichen Gleichstellung beibehalten.

Absatz 2 Satz 1 entspricht weitgehend der bisherigen Fassung. Zudem sind Maßnahmen nach § 33 anwendbar, wenn die Aufklärung des Sachverhaltes zum Zwecke der Verhütung solcher Straftaten oder ihrer möglichen Verfolgung ansonsten unmöglich oder wesentlich erschwert wäre. Satz 2 wird umstrukturiert und an die Änderungen in § 27 Absatz 3 angepasst. Eine Befugniserweiterung ist damit nicht verbunden.

Mit Satz 3 wird der Einsatz verdeckter Maßnahmen ausdrücklich zur Verhütung terroristischer Straftaten bereits im Vorfeld einer konkreten Gefahr zugelassen. Dies erfolgt unter Beachtung der Maßgabe der vom Bundesverfassungsgericht in seinem oben benannten Urteil vom 20. April 2016 aufgestellten Anforderungen an die zu treffende Prognoseentscheidung bezüglich der Gefahrenlage im Vorfeld einer konkreten Gefahr für die Begehung erheblicher, insbesondere terroristischer Straftaten. Das Bundesverfassungsgericht hat in dieser Entscheidung unter der Randnummer 165 in diesem Zusammenhang zur Regelung des § 20g die dort enthaltene Wendung „bei der Tatsachen die Annahme rechtfertigen“ kritisiert und ausgeführt:

„Die Vorschrift schließt nicht aus, dass sich die Prognose allein auf allgemeine Erfahrungssätze stützt. Sie enthält weder die Anforderung, dass ein wenigstens seiner Art nach konkretisiertes und absehbares Geschehen erkennbar sein muss, noch die alternative Anforderung, dass das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründen muss, dass sie in überschaubarer Zukunft terroristische Straftaten begeht. Damit gibt sie den Behörden und Gerichten keine hinreichend bestimmten Kriterien an die Hand und eröffnet Maßnahmen, die unverhältnismäßig weit sein können.“

Hinweise, die die konkrete Wahrscheinlichkeit eines terroristischen Anschlags begründen, können sich aus dem Vorverhalten einer Person (zum Beispiel Rückkehr aus einem ausländischen Terror-Camp) oder aus sonstigen Umständen ergeben, die Rückschlüsse auf das individuelle Verhalten zulassen (zum Beispiel glaubwürdige Aussagen eines Zeugen).

Hinsichtlich der Kontakt- und Begleitpersonen wird auf die in § 27 Absatz 3 Nummer 2 konkretisierte Definition verwiesen.

Der bisher geltende Absatz 2 Satz 3, wonach das Brief-, Post- und Fernmeldegeheimnis unberührt bleiben, wird Absatz 2 Satz 4.

Absatz 3 bestimmt, dass der Einsatz verdeckter technischer Mittel nach Absatz 1 Nummer 2 abweichend von den Bestimmungen in Absatz 2 zulässig ist, wenn er ausschließlich dem Schutz der bei einem polizeilichen Einsatz tätigen Personen dient. Diese Möglichkeit war bereits implizit in § 34 Absatz 4 vorgesehen. Soweit ein solcher Einsatz im Zusammenhang mit Wohnungen erfolgt, gilt Absatz 3 gemäß § 33b Absatz 9 entsprechend.

Absatz 4 entspricht weitgehend dem bisherigen Absatz 3. Es werden lediglich der Bezug zu Maßnahmen nach Absatz 1 und 3 klargestellt und ein Klammerzusatz eingefügt, der zum verwendeten Begriff „Dritte“ auf die Definition in § 3 Absatz 4 Nummer 2 verweist.

Die Absätze 5 und 6 entsprechen den bisherigen Absätzen 4 und 5 unter Berücksichtigung der sprachlichen Gleichstellung. Der bisherige Absatz 6 konnte aufgrund der nunmehr zentralen Schutzvorschrift in § 26b entfallen.

§ 33a (Verfahren beim Einsatz besonderer Mittel der Datenerhebung)

Die bisher geltende Verfahrensvorschrift des § 34 wird umstrukturiert, inhaltlich an die Anforderungen des Bundesverfassungsgerichtes in seinem Urteil zum Bundeskriminalamtgesetz vom 20. April 2016 angepasst und nun neu als § 33a im Gesetz verankert.

Die inhaltlichen Änderungen betreffen zunächst Absatz 1. Wie vom Bundesverfassungsgericht gefordert (siehe Randnummern 173 f und Punkt 4 des Tenors a. a. O.), wird der bisher in § 34 Absatz 1 enthaltene grundsätzliche Behördenleitervorbehalt durch einen Richtervorbehalt für bestimmte Einsätze besonderer Mittel der Datenerhebung ersetzt. Die längerfristige Observation nach § 33 Absatz 1 Nummer 1, das Abhören oder Aufzeichnen des außerhalb von Wohnungen nicht öffentlich gesprochenen Wortes und der langfristige Einsatz technischer Mittel für Observationszwecke als Maßnahmen nach § 33 Absatz 1 Nummer 2 sowie der Einsatz von Vertrauenspersonen und verdeckt Ermittelnden (§ 33 Absatz 1 Nummer 3 und 4) bedürfen zukünftig der richterlichen Anordnung. Bezüglich des Einsatzes von Vertrauenspersonen und verdeckt Ermittelnden besteht in Anlehnung an § 110b Absatz 2 der Strafprozessordnung sowie an den neugefassten § 45 Absatz 3 Satz 1 Nummer 5 des Bundeskriminalamtgesetzes ein grundsätzlicher Richtervorbehalt nur dann, wenn sich der Einsatz gegen eine bestimmte Person richtet oder eine nicht allgemein zugängliche Wohnung betreten werden soll. Das Bundesverfassungsgericht setzt unbeschadet seiner darüber hinausgehenden Übergangsmaßgaben den Einsatz einer Vertrauensperson oder eines verdeckt Ermittelnden zutreffender Weise maßgeblich in Zusammenhang mit dem Ausnutzen von Vertrauen (siehe Randnummer 160 a. a. O.), was erst bei einem zielgerichteten Einsatz zur personenbezogenen Datenerhebung angenommen werden kann.

Wegen der mit der langfristigen Observation vergleichbaren Eingriffsschwere (siehe Randnummer 174 a. a. O.) werden auch die Anfertigung von Bildaufnahmen oder Bildaufzeichnungen von Personen, die sich außerhalb von Wohnungen befinden, unter den Richtervorbehalt gestellt, soweit durchgehend länger als 24 Stunden oder an mehr als zwei Tagen Bildaufzeichnungen bestimmter Personen angefertigt werden sollen.

Bei Gefahr für Leib, Leben oder die Freiheit einer Person kann die Behördenleitung die vorgenannten Maßnahmen anordnen. Eine richterliche Entscheidung ist unverzüglich nachzuholen. Wird die behördliche Anordnung nicht in der benannten Frist bestätigt, tritt sie außer Kraft.

Bei sonstigen Maßnahmen nach § 33, deren Eingriffsgewicht geringer ist, darf die Anordnung von der Behördenleitung oder einer von ihr besonders beauftragten Beamtin oder einem besonders beauftragten Beamten erfolgen; bei Gefahr im Verzug kann von dieser Vorgabe abgewichen werden.

Der bisherige § 34 Absatz 2 wird ergänzt und in Absatz 4 aufgenommen (siehe unten). § 34 Absatz 4 Satz 1 und 2 werden umformuliert in Absatz 5 übernommen. Die übrigen Sätze werden durch die zentralen Vorschriften zum Kernbereichsschutz in § 26a und die Vorschrift zur weiteren Verwendung in § 36 abgedeckt.

Mit den Absätzen 2 und 3 werden die Anforderungen des Urteils des Bundesverfassungsgerichtes vom 20. April 2016 an die grundrechtssichernde Funktion der unabhängigen Richterkontrolle umgesetzt. Das Bundesverfassungsgericht hat hierzu ausgeführt (siehe Randnummern 117 und 118 a. a. O):

„Übergreifende Anforderungen ergeben sich aus dem Verhältnismäßigkeitsgrundsatz auch in verfahrensrechtlicher Hinsicht. Die hier ganz überwiegend in Rede stehenden eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen, bei denen damit zu rechnen ist, dass sie auch höchstprivate Informationen erfassen, und gegenüber den Betroffenen heimlich durchgeführt werden, bedürfen grundsätzlich einer vorherigen Kontrolle durch eine unabhängige Stelle, etwa in Form einer richterlichen Anordnung (vgl. dazu auch EGMR, Klass u. a. v. Deutschland,Urteil vom6. September 1978, Nr. 5029/71, § 56; EGMR [GK], Zakharov v. Russland, Urteil vom 4. Dezember 2015, Nr. 47143/06, §§ 258, 275; EGMR, Szabó und Vissy v. Ungarn, Urteil vom 12. Januar 2016, Nr. 37138/14, § 77). Dies gilt für Maßnahmen der Wohnraumüberwachung bereits gemäß Art. 13 Abs. 3 und 4 GG (vgl. hierzu BVerfGE 109, 279 <357 ff.>) und folgt im Übrigen unmittelbar aus dem Verhältnismäßigkeitsgrundsatz (vgl. BVerfGE 120, 274 <331 ff.>; 125, 260 <337 ff.>). Der Gesetzgeber hat das Gebot vorbeugender unabhängiger Kontrolle in spezifischer und normenklarer Form mit strengen Anforderungen an den Inhalt und die Begründung der gerichtlichen Anordnung zu verbinden. Hieraus folgt zugleich das Erfordernis einer hinreichend substantiierten Begründung und Begrenzung des Antrags auf Anordnung, die es dem Gericht oder der unabhängigen Stelle erst erlaubt, eine effektive Kontrolle auszuüben. Insbesondere bedarf es der vollständigen Information seitens der antragstellenden Behörde über den zu beurteilenden Sachstand.“

Der neue Absatz 2 regelt die sich daraus ergebenden Anforderungen an den Antrag der Behördenleitung. Die Einschränkung der Nummer 1 („soweit möglich“) resultiert aus dem Umstand, dass in der Praxis zum Beispiel nur die Anschrift einer Person, nur der Name oder - in seltenen Fällen - keines von beidem bekannt sein kann. Im letzteren Fall wird auf eine Personenbeschreibung abzustellen sein.

Absatz 3 Satz 1 sieht vor, dass Anordnungen grundsätzlich schriftlich zu ergehen haben. Bei Gefahr im Verzug kann dies ausnahmsweise mündlich erfolgen. Die Anordnung ist jedoch unverzüglich schriftlich zu dokumentieren. In den Anordnungen sind, um eine effektive Kontrolle des Gerichtes zu ermöglichen, nach Absatz 3 Satz 2 die Personen, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift, Art, Umfang und Dauer der Maßnahme sowie die wesentlichen Gründe zwingend anzugeben. Der neue Satz 3 bestimmt nunmehr eine konkrete Höchstdauer der Anordnung von drei Monaten; in Fällen des Einsatzes von Vertrauenspersonen und verdeckten Ermittlern von sechs Monaten.

Mit Absatz 4 wird die bisherige Regelungslage in § 34 Absatz 2 unter Aktualisierung der dort bestehenden Verweisungen übernommen. Damit wird zukünftig weiterhin sichergestellt, dass Daten, die ausschließlich über andere als die in § 33 Absatz 2, 4 oder in § 26b genannten Personen erhoben worden sind, unverzüglich gelöscht werden. Diese Löschverpflichtung gilt jedoch - wie bisher schon - dann nicht, wenn die nach § 33 Absatz 2 erhobenen Daten zur Verfolgung von Straftaten benötigt werden oder soweit die nach § 26b erhobenen Daten aufgrund gesetzlicher Bestimmungen (etwa aufgrund von § 36 des Gesetzes, siehe hierzu auch bestehende Vorschriften in der Strafprozessordnung) verwendet werden dürfen.

Auch ist auf die in § 46f Absatz 2 Nummer 2 bestehende zusätzliche Protokollierungspflicht und die in § 48h Absatz 1 Satz 1 Nummer 1 normierte Berichtspflicht für den Einsatz besonderer Mittel der Datenerhebung nach § 33 Absatz 1 besonders hinzuweisen.

Mit der Regelung in Absatz 5 Satz 1 bleibt es wie bisher bei der Anordnungsmöglichkeit durch die Einsatzleitung, wenn technische Mittel in verdeckter Weise ausschließlich zum Schutz der bei einem polizeilichen Einsatz tätigen Personen nach § 33 Absatz 3 - auch in Verbindung mit § 33b Absatz 9 - eingesetzt werden. Die Einsatzleitung ist die Beamtin oder der Beamte, der oder dem die Leitung des Einsatzes obliegt. Hinsichtlich der weiteren Verwendung erhobener Daten wird auf die Vorschriften zur Weiterverarbeitung im Gesetz (insbesondere sind die § 26a zur richterlichen Überprüfung vor einer Weiterverwendung und § 36 zu beachten) und auch ausdrücklich auf die Vorschriften zur Einschränkung der Verarbeitung in § 45 Absatz 3 verwiesen. Soweit eine Weiterverwendung der Daten aus einer Maßnahme nach § 33b Absatz 9 erfolgte, ist auch die gemäß § 48h Absatz 1 Satz 1 Nummer 2 bestehende Berichtspflicht zu beachten.

Die bisher geltenden Absätze 5 bis 7 des § 34 gehen in den neuen zentralen Regelungen zur Benachrichtigungs- und Unterrichtungspflicht in den §§ 46a und 48h auf und bedürfen daher keiner Übernahme in den § 33a.

§ 33b (Einsatz technischer Mittel zur Wohnraumüberwachung)

Die Befugnis zur Wohnraumüberwachung ist bisher im § 34b im SOG M-V verortet. Sie wird nun im § 33b aufgenommen und grundlegend überarbeitet.

In Absatz 1 Satz 1 werden die bislang in § 34b Absatz 1 Satz 1 genannten Individualrechtsgüter um wichtige Rechtsgüter der Allgemeinheit ergänzt. Mit der Neufassung des Absatzes 1 werden zudem die Vorgaben des Bundesverfassungsgerichtes aus seinem Urteil vom 20. April 2016 umgesetzt.

Das Gericht hat entschieden, dass die konkrete Ausgestaltung der Ermächtigungen im Bundeskriminalamtgesetz zum Einsatz heimlicher Überwachungsmaßnahmen zur Abwehr von Gefahren des internationalen Terrorismus teilweise unverhältnismäßig ist. Eingriffsbefugnisse, die wie die Wohnraumüberwachung oder die Online- Durchsuchung tief in die Privatsphäre eingreifen, unterliegen als Ausfluss des Verhältnismäßigkeitsgrundsatzes besonders strengen Vorgaben an ihre Ausgestaltung. Diese Maßnahmen dürfen sich unmittelbar nur gegen diejenigen als Zielpersonen richten, die für die Gefahr verantwortlich sind (siehe Randnummern 115, 192 a. a. O.).

Absatz 1 wird entsprechend der Regelung zu verdeckten Maßnahmen durch Satz 2 dahingehend angepasst, dass die Maßnahmen auch unter den Voraussetzungen des § 67a Absatz 1 durchgeführt werden dürfen.

Zu Absatz 2 ist Folgendes auszuführen:

Nach der bisherigen Regelung in § 34b Absatz 1 darf sich eine Wohnraumüberwachung nicht nur gegen die für die Gefahr Verantwortlichen, sondern auch gegen Nichtverantwortliche richten. Das ist nach Auffassung des Bundesverfassungsgerichtes unverhältnismäßig. Aus diesem Grund wird der Kreis der Adressaten einer Wohnraumüberwachung in Absatz 1 zukünftig auf die für die Gefahr Verantwortlichen beschränkt. Das Bundesverfassungsgericht hat es allerdings als verfassungsrechtlich hinnehmbar bezeichnet, wenn bei einer gegen den Verantwortlichen angeordneten Wohnraumüberwachung auch Dritte miterfasst werden. So könne die Überwachung der Wohnung eines Dritten erlaubt werden, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass sich der Verantwortliche während der Überwachung dort aufhält, für die Ermittlungen relevante Gespräche führen wird und eine Überwachung seiner Wohnung allein zur Erforschung des Sachverhalts nicht ausreicht (siehe Randnummern 115, 188 a. a. O.).

Dementsprechend wird in Absatz 2 in Anlehnung an § 46 Absatz 2 Satz 2 des Bundeskriminalamtgesetzes festgelegt, dass eine Wohnraumüberwachung unter den vom Bundesverfassungsgericht genannten Voraussetzungen auch in der Wohnung eines Dritten durchgeführt werden darf.

Absatz 3 stellt klar, dass die Maßnahme auch durchgeführt werden darf, wenn Dritte unvermeidbar betroffen sind. Die bisherigen Absätze 2 und 3 des § 34b zum Kernbereichsschutz gehen in der zentralen Vorschrift des § 26a auf und sind hier in § 33b nicht mehr gesondert zu regeln.

Absatz 3 Satz 2 stellt in Anlehnung an die bisherige Regelung in § 34b Absatz 2 Satz 2 und 3 für die Frage, ob Anhaltspunkte dafür vorliegen, dass Daten aus dem Kernbereich privater Lebensgestaltung erfasst werden (§ 26a Absatz 1), klar, dass insbesondere auf die Art der Räumlichkeiten abzustellen ist sowie auf das Verhältnis der dortigen Personen zueinander (vergleiche § 46 Absatz 6 Satz 1 des Bundeskriminalamtgesetzes). Damit bleibt es dabei, dass es vom Grundsatz her keine von vornherein festgeschriebenen Tabuzonen im Wohnungsbereich gibt, sondern die Erkenntnislage in jedem Einzelfall entscheidet.

Der bisherige Absatz 4 des § 34b wird gestrichen. Er geht in der zentralen Vorschrift zum Schutz zeugnisverweigerungsberechtigter Personen nach § 26b auf. Die neugefassten Absätze 4 bis 6 tragen den im Urteil vom 20. April 2016 aufgestellten Anforderungen des Bundesverfassungsgerichtes an die grundrechtssichernde Funktion der unabhängigen Richterkontrolle und den sich daraus ergebenden Anforderungen an den Antrag und den Inhalt der Anordnung Rechnung (vergleiche auch Begründung zu § 33). In Anlehnung an die Vorschrift in § 46 Absatz 5 Satz 3 des Bundeskriminalamtgesetzes wird insbesondere bestimmt, dass die Maßnahme auf einen Monat zu befristen ist. Die Einschränkung des Absatzes 5 Nummer 1 („soweit möglich“) resultiert aus dem Umstand, dass in der Praxis zum Beispiel nur die Anschrift der zu überwachenden Wohnung bekannt sein kann.

Die Absätze 7 und 8 orientieren sich an § 46 Absatz 7 und 8 des Bundeskriminalamtgesetzes. Hier wird wie bisher in § 34b Absatz 6 die unverzügliche Einbeziehung des anordnenden Gerichtes bei Vorliegen von Erkenntnissen aus der Wohnraumüberwachung festgeschrieben. Weiterhin wird das Verfahren zur Verwertbarkeit der Erkenntnisse spezialgesetzlich festgelegt. § 26a Absatz 4, der speziell die Verwertung von aus Wohnungen erhobenen Daten regelt, gilt hier folglich nicht.

Die bisherigen Absätze 7 bis 9 können entfallen, da deren Inhalte in den zentralen Vorschriften zur Weiterverwendung von personenbezogenen Daten in § 36 (der bereits spezielle Vorschriften zu Daten aus Wohnraumüberwachungsmaßnahmen enthält), zur Kennzeichnung in § 46g, zur Benachrichtigung in § 46a, zur parlamentarischen Kontrolle in § 48h sowie zum gerichtlichen Verfahren in § 25b aufgehen. Besonders ist auch auf die in § 46f Absatz 2 Nummer 3 aufgenommene zusätzliche Protokollierungspflicht hinzuweisen.
Absatz 9 bestimmt, dass die in den §§ 33 Absatz 3 und 33a Absatz 5 getroffenen Regelungen zum verdeckten Einsatz technischer Mittel ausschließlich zum Schutz der bei einem polizeilichen Einsatz tätigen Personen auch für den Bereich von Wohnräumen gelten.

§ 33c (Einsatz technischer Mittel zum Eingriff in informationstechnische Systeme)

Der Einsatz technischer Mittel zum Eingriff in informationstechnische Systeme ist zur Abwehr von Gefahren des internationalen Terrorismus bereits im Bundeskriminalamtgesetz (§ 49) normiert und in Fällen der Strafverfolgung dient § 100b StPO als Rechtsgrundlage. Auch die Länder Rheinland-Pfalz (§ 31c des Polizei- und Ordnungsbehördengesetzes), Hessen (§ 15c des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung) und Bayern (Artikel 34d des Gesetzes über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei) haben bereits eine entsprechende Eingriffsbefugnis für die Polizei zu gefahrenabwehrrechtlichen Zwecken geschaffen. Das Land Niedersachsen plant die Aufnahme einer Befugnis zum Eingriff in informationstechnische Systeme mit technischen Mittel in das Niedersächsische Gesetz über die öffentliche Sicherheit und Ordnung (siehe Drucksache 18/850 des Niedersächsischen Landtages, Seite 14, geplanter § 33d). Weitere Bundesländer sehen ebenfalls den Bedarf zur Schaffung einer solchen Befugnis.

Mit § 33c wird der Polizei - in Anlehnung an § 49 des Bundeskriminalamtgesetzes und bereits bestehender Länderbefugnisse - zur Abwehr von Gefahren für überragende Rechtsgüter und insbesondere terroristischer Straftaten die Ermächtigung gegeben, auf Daten zuzugreifen, die noch nicht oder nicht mehr Gegenstand einer laufenden Telekommunikation sind oder überhaupt nicht für eine Telekommunikation vorgesehen sind (sogenannte Online-Durchsuchung). In Abgrenzung zur ebenfalls verdeckten Telekommunikationsüberwachung können nicht nur neu hinzukommende Kommunikationsinhalte, sondern alle auf einem informationstechnischen System gespeicherten Inhalte sowie das gesamte Nutzungsverhalten einer Person überwacht werden. Nicht ermöglicht werden soll der Zugriff auf am Computer angeschlossene Kameras oder Mikrofone.

Die rasante technische Entwicklung im Bereich der Informationstechnik führt dazu, dass die Polizei zur Erfüllung ihrer Aufgaben kontinuierlich steigende, beträchtliche Ressourcen benötigt. Sie sieht sich in zunehmendem Maße mit einer immer weiter verbreiteten Nutzung kryptografischer Verfahren, immer größer werdenden Datenmengen und den weit verbreiteten Möglichkeiten der mobilen Nutzung des Internets (zum Beispiel Internetcafé, Hot Spot) konfrontiert. Um zukünftig eine effektive Gefahrenabwehr, insbesondere im Bereich des Terrorismus gewährleisten zu können, müssen ihr die hierfür erforderlichen Instrumente an die Hand gegeben werden. Dazu gehört auch die Maßnahme des verdeckten Eingriffs in informationstechnische Systeme.

Das Bundesverfassungsgericht hat eine solche Maßnahme bereits in älteren Entscheidungen unter bestimmten strengen Voraussetzungen als verfassungsrechtlich zulässig erkannt (siehe Urteil vom 27. Februar 2008, Aktenzeichen 1 BvR 370/07). Dabei hatte es erstmalig aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme abgeleitet. Es hat dabei aber hervorgehoben, dass dieses Grundrecht nicht schrankenlos gewährleistet ist. Eingriffe darin können sowohl zu präventiven wie auch repressiven Zwecken gerechtfertigt sein. Das setzt aber für den Bereich der Prävention (Gefahrenabwehr) das Vorliegen einer konkreten Gefahr für ein überragend wichtiges Rechtsgut voraus. Überragend wichtig sind Leib, Leben und Freiheit der Person sowie solcher Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Dabei kann die Maßnahme schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für überragend wichtige Rechtsgüter hinweisen. Die Verwendung des Begriffes „Tatsachen die Annahme rechtfertigen“ erfolgt mit Blick auf den möglichst einheitlichen Sprachgebrauch des Gesetzes. Eine Änderung der Voraussetzungen gegenüber der Bundesnorm im Bundeskriminalamtgesetz ist damit nicht verbunden. Die grundsätzlichen Anforderungen an eine entsprechende Ermächtigungsgrundlage hat das Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 (Randnummern 208 ff.) zum bisherigen § 20k des Bundeskriminalamtgesetzes weiter konkretisiert. § 33c setzt diese Anforderungen um.

Absatz 1 Satz 1 erlaubt der Polizei zur Abwehr einer im Einzelfall bestehenden Gefahr für hochrangige Rechtsgüter ohne Wissen der betroffenen Person durch technische Mittel in von ihr genutzte informationstechnische Systeme einzugreifen und aus ihnen Daten zu erheben. Dies stellt einen verfassungsgemäßen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (vergleiche hierzu Bundesverfassungsgerichtsurteil vom 27. Februar 2008, Aktenzeichen 1 BvR 370/07, Randnummer 247) dar.

Die Formulierung „durch technische Mittel in informationstechnische Systeme eingreifen und aus ihnen Daten erheben“ soll sicherstellen, dass die notwendigen technischen Maßnahmen ergriffen werden dürfen, um eine Datenerhebung aus IT-Systemen zu ermöglichen. Umfasst sind dabei etwa das Kopieren bestimmter Dateien von der Festplatte eines Rechners und deren elektronische Übertragung, aber auch der Einsatz sogenannter Keylogger, bei denen die Tastatureingaben erfasst werden, ohne dass notwendigerweise eine Zwischenspeicherung auf der Festplatte erfolgt (siehe hierzu auch Lisken/Denniger, Handbuch des Polizeirechts, 6. Auflage, 2018, Teil E, Randnummern 780 ff).

Satz 2 lässt die Maßnahme nach Absatz 1 auch zu, wenn sie der Verhütung einer terroristischen Straftat bei Vorliegen der Gefahrenvoraussetzungen des § 67a Absatz 1 dient. Damit werden die Anforderungen des Bundesverfassungsgerichtes für präventiv-polizeiliche Maßnahmen im Vorfeld einer konkreten Gefahr umgesetzt (Urteil vom 20. April 2016, Randnummer 213).

Nach Satz 3 darf sich eine Maßnahme nach Absatz 1 grundsätzlich nur gegen eine nach § 69 oder § 70 verantwortliche Person richten. Adressaten sind danach sowohl der Verhaltens- als auch der Zustandsstörer. Mit dem Verweis auf diese im Polizei- recht etablierten Begriffe wird der Kreis möglicher Adressaten der Maßnahme hinreichend bestimmt eingeschränkt. Satz 4 erlaubt hingegen auch, dass in informationstechnische Systeme anderer Personen eingegriffen werden darf, wenn Tatsachen die Annahme rechtfertigen, dass eine nach Satz 1 betroffene Person dort ermittlungsrelevante Informationen speichert. Damit soll sichergestellt werden, dass die gefahrverantwortliche Person sich nicht dadurch einer Maßnahme nach Satz 1 entziehen kann, dass sie ihre Daten auf einem fremden System speichert (vergleiche hierzu auch § 31c Absatz 1 des Polizei- und Ordnungsbehördengesetzes Rheinland-Pfalz und Artikel 34d Absatz 1 des Gesetzes über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei).

Als Konkretisierung des Verhältnismäßigkeitsgrundsatzes (siehe auch § 15) stellt Absatz 2 Satz 1 klar, dass die Maßnahme nur dann durchgeführt werden darf, wenn die Aufgabenerfüllung durch die Polizei ansonsten aussichtslos oder wesentlich erschwert wäre. Satz 2 legt fest, dass die Maßnahme nicht deswegen unzulässig ist, weil Dritte unvermeidbar betroffen sind. Ferner wird bestimmt, dass § 26a mit der zusätzlichen Maßgabe gilt, dass, soweit möglich, technisch sicherzustellen ist, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Eine vergleichbare Regelung findet sich zum Beispiel auch in § 49 Absatz 7 Satz 2 des Bundeskriminalamtgesetzes wieder.

Nach Absatz 3 sind bei der Durchführung der Maßnahme bestimmte technische Schutzvorkehrungen zu treffen, um den Eingriff in das infiltrierte System auf das unbedingt erforderliche Mindestmaß zu begrenzen und die Datensicherheit zu gewährleisten (vergleiche Bundesverfassungsgerichtsurteil vom 20. April 2016, Randnummer 215).

Satz 1 bestimmt zunächst in Nummer 1, dass beim Einsatz des technischen Mittels sicherzustellen ist, dass an dem IT-System nur solche Veränderungen vorgenommen werden, die für die Datenerhebung unbedingt erforderlich sind. Vor nicht unbedingt erforderlichen Veränderungen zu schützen sind nicht nur die von dem Nutzer des informationstechnischen Systems angelegten Anwenderdateien, sondern auch die für die Funktion des IT-Systems erforderlichen Systemdateien. Auch Beeinträchtigungen der Systemleistung sind auf das technisch Unvermeidbare zu begrenzen.

Nach Satz 1 Nummer 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 IT-System installierte Überwachungssoftware vollständig zu löschen und sind Veränderungen an den bei der Installation der Überwachungssoftware vorgefundenen Systemdateien rückgängig zu machen. Das Rückgängigmachen 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 manuell rückgängig zu machen.

Satz 2 bestimmt in Anlehnung an § 14 Absatz 1 der Telekommunikations-Überwachungsverordnung, dass das eingesetzte technische Mittel 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 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 IT-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 von Wissenschaft und Technik“ gegen unbefugte Nutzung zu schützen, bedeutet, dass sich die Polizei der fortschrittlichsten technischen Verfahren bedienen muss, die nach Auffassung führender Fachleute aus Wissenschaft und Technik auf der Grundlage neuester wissenschaftlicher Erkenntnisse erforderlich sind. Hierfür müssen die einschlägigen Aktivitäten auf den Gebieten der Wissenschaft und Technik umfassend und sorgfältig beobachtet und ausgewertet werden. Diese Anforderung trägt der besonderen Eingriffsqualität der Maßnahme Rechnung.

Satz 3 schützt in Anlehnung an § 14 Absatz 2 Satz 1 Telekommunikations-Überwachungsverordnung die Integrität und Authentizität der von dem technischen Mittel zum Zwecke der Ausleitung an die Polizei bereitgestellten Daten (Kopien von Dateien, Protokolle von Tastatureingaben) vom Zeitpunkt der Bereitstellung für die Übertragung an die Polizei an, während der Datenübertragung an die Polizei sowie während ihrer Speicherung bei der Polizei. Dies dient sowohl dem Schutz der betroffenen Person 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 soweit technisch möglich zu verschlüsseln und bei ihr beweissicher zu speichern, insbesondere mit einer elektronischen Signatur und einem elektronischen Zeitstempel zu versehen.

Absatz 4 normiert die Befugnis zum Einsatz von technischen Mitteln zur Identifikation und Lokalisation von informationstechnischen Systemen. Unter spezifischen Kennungen sind zum Beispiel Internetprotokoll- 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 beziehungsweise 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. Absatz 4 Satz 2 bestimmt darüber hinaus, dass personenbezogene Daten Dritter (§ 3 Absatz 4 Nummer 2) dabei nur erhoben werden dürfen, wenn dies aus technischen Gründen unvermeidbar ist. Diese Daten sind im Rahmen der Einzelfallprüfung nach Beendigung der Maßnahme nach § 45 Absatz 2 Nummer 4 zu löschen, da sie für die Durchführung der Online-Durchsuchung nicht mehr erforderlich sind.

Mit Absatz 5 wird für die Maßnahme der Online-Durchsuchung ein Betretungs- und Durchsuchungsrecht gesetzlich geregelt. Auch wenn der Zugriff auf das betroffene informationstechnische System im Regelfall über Kommunikationsverbindungen dieses Systems eröffnet sein wird, sind dennoch auch Fälle von nicht mit dem Internet verbundenen Systemen (sogenannte Stand-Alone-Systeme) oder Systemen, die einen unüberwindbaren Zugriffsschutz gegen Angriffe von außerhalb aufwarten, denkbar, für die im Einzelfall das Bedürfnis des Zugriffs bestehen kann. Mit der vorhandenen Möglichkeit, solche Systeme im Wege der richterlich gestatteten Wohnungsbetretung und -durchsuchung zu identifizieren und auf den Zugriff vorzubereiten, wird eine Regelungslücke bei solch abgekapselten Systemen ausgeschlossen. Die Regelung sieht dahingehend vor, dass ein Betreten und Durchsuchen zur Durchführung der Maßnahme erforderlich sein muss, mithin erst bei Unmöglichkeit des Zugriffs über die Kommunikationsverbindungen des Systems gestattet ist. In der Anordnung für die Online-Durchsuchung können die Maßnahmen nach Absatz 5 auch unter der vorgenannten Maßgabe gestattet werden, ohne dass die Unmöglichkeit bereits bei der Beantragung feststehen muss.

Die Absätze 6 bis 8 regeln die Anordnungsbefugnis, Form und Inhalt des Antrags und der Anordnung sowie die Befristung der Maßnahme. In Anlehnung an § 49 des Bundeskriminalamtgesetzes ist die Erstanordnung auf höchstens 3 Monate zu befristen. Die Fortsetzung der Maßnahme ist bei Vorliegen der Anordnungsvoraussetzungen unter Berücksichtigung der bisherigen Erkenntnisse analog zur Regelung über die Wohnraumüberwachung mit technischen Mitteln für den Zeitraum von einem Monat möglich. Die Einschränkung des Absatzes 7 Nummer 1 („soweit möglich“) resultiert aus dem Umstand, dass in der Praxis zum Beispiel nur die Anschrift einer Person, nur der Name oder - in seltenen Fällen - keines von beidem bekannt sein kann. Ähnlich verhält es sich mit der Einschränkung in Nummer 3, die darin begründet ist, dass in der Praxis nicht immer vorab ersichtlich ist, welche Sachen im Einsatzgeschehen vorgefunden werden oder welche Räumlichkeiten der betroffenen Person zuzuordnen sind.

Hinsichtlich der gerichtlichen Zuständigkeit gilt § 25b auch für die Fälle, in denen zur Durchführung der Maßnahme das Betreten und Durchsuchen einer Räumlichkeit der betroffenen Person gerichtlich angeordnet wird. Abweichend von der Regelung in § 59 Absatz 6 Satz 3, wonach grundsätzlich das Amtsgericht über die Durchsuchung von Wohn- und Geschäftsräumen entscheidet, in dessen Bezirk sich die Räume befinden, verbleibt die Zuständigkeit wegen des unmittelbaren Sachzusammenhangs bei dem die Maßnahme anordnenden Gericht.

Die Absätze 9 und 10 entsprechen wegen der besonderen Eingriffsintensität den Regelungen zur Wohnraumüberwachung in § 33b Absatz 7 und 8.

Im Übrigen ist hinsichtlich der Weiterverwendung von Daten aus Maßnahmen nach § 33c auf § 36 hinzuweisen, der hierzu spezielle Regelungen enthält. Besonders zu beachten sind des Weiteren zum Beispiel auch die in § 46f Absatz 2 Nummer 4 aufgenommene zusätzliche Protokollierungspflicht und die in § 48h Absatz 1 Satz 1 Nummer 3 bestehende Berichtspflicht für Maßnahmen nach § 33c.

§ 33d (Einsatz technischer Mittel zur Überwachung der Telekommunikation)

Die Befugnis zur Telekommunikationsüberwachung ist bisher im § 34a geregelt. Die Überwachungsbefugnis wird in § 33d übernommen, überarbeitet und teilweise in gesonderte Regelungen überführt (vergleiche etwa §§ 33f, 33g).

Die Änderungen in Absatz 1 erfolgen zur Vereinheitlichung der Anforderungen an die Anordnung verdeckter Maßnahmen. In Satz 1 Nummer 1 werden die zuvor in § 34a Absatz 1 genannten Individualrechtsgüter um wichtige Rechtsgüter der Allgemeinheit ergänzt. In Satz 1 Nummer 2 werden die Verantwortlichen für eine Gefahr der Begehung einer terroristischen Straftat nach § 67a eingefügt. Damit werden die in der Entscheidung des Bundesverfassungsgerichtes zum Bundeskriminalamtgesetz vom 20. April 2016 entwickelten Prognosekriterien aufgegriffen. Nummer 3 und 4 entsprechen § 51 Absatz 1 Satz 1 Nummer 4 und 5 des Bundeskriminalamtgesetzes. Diese sind für eine effektive Gefahrenabwehr zwingend notwendig, da die Maßnahmen zur Datenerhebung ins Leere laufen können, wenn die gefahrenverantwortliche Person ausschließlich oder maßgeblich über Dritte kommuniziert oder deren Telekommunikationsgeräte oder Telekommunikationsanschlüsse nutzt. Der bisherige Satz 2 in § 34a Absatz 1 wird unverändert übernommen und Satz 3 wird sprachlich angepasst. Satz 4 kann entfallen, da der bisher geltende § 33 Absatz 6 aufgrund der zentralen Vorschrift zum Schutz zeugnisverweigerungsberechtigter Personen in § 26b entfallen ist.

Mit Absatz 2 Satz 1 wird die bisherige Regelung in § 34a Absatz 2 Satz 1 sprachlich modifiziert und offener für technische Veränderungen im Telekommunikationsbereich gestaltet. Mit Satz 2 werden der vormalige Absatz 5 vor die Anordnungsvoraussetzungen gezogen und die Beschränkung auf die Fallgestaltungen des bisherigen Absatz 1 Satz 1 Nummer 1 aufgehoben, da dies für eine konsequente Gefahrenabwehr erforderlich ist. Auch bei gefährdeten Personen kann es erforderlich sein, vorhandene Verkehrsdaten auszuwerten, wenn etwa eine gegenwärtige Lokalisierung des Mobiltelefons zum Auffinden einer vermissten Person mangels Aktivität des Gerätes nicht möglich ist und die Verkehrsdaten Aufschluss darüber geben können, mit wem die vermisste Person vor ihrem Verschwinden kommuniziert hat und so der Aufenthaltsort ermittelt werden kann. Satz 3 wird neu aufgenommen und stellt deutlich klar, dass eine Funkzellenabfrage, wie sie etwa zu Zwecken der Strafverfolgung zugelassen ist, zur Gefahrenabwehr nicht zulässig sein soll.

Der bisherige Absatz 3 entfällt. Die Befugnis aus dem bisherigen § 34a Absatz 3 Satz 1 wird nunmehr in der Regelung zur Identifizierung und Lokalisierung von mobilen Telekommunikationsendgeräten nach § 33f konkretisiert. Die bisher in Satz 2 geregelte Befugnis zur Unterbrechung oder Verhinderung von Telekommunikationsverbindungen wird in § 33g geregelt.

Der neu aufgenommene Absatz 3 Satz 1 ergänzt die bisherige Regelung in Anlehnung an den vom Bundesverfassungsgericht in seinem Urteil vom 20. April 2018 (Randnummer 234) für verfassungskonform erklärten § 51 Absatz 2 des Bundeskriminalamtgesetzes um eine Rechtsgrundlage für den heimlichen, technischen Eingriff in ein informationstechnisches System zum Zweck der Telekommunikationsüberwachung (sogenannte Quellen-TKÜ). Die Aufnahme einer solchen Befugnis ist im Bereich der Gefahrenabwehr (vergleiche für den Bereich der Strafverfolgung § 100a Absatz 1 Satz 2 der Strafprozessordnung) unerlässlich, weil nur so der Zugriff auf verschlüsselte Telekommunikationsinhalte gewährleistet wird und die Befugnis zur präventiven Telekommunikationsüberwachung ohne eine solche Ermächtigung in Anbetracht der heute vielfach verwendeten Verschlüsselungstechnik leerliefe.

Auch andere Bundesländer verfügen bereits über eine Befugnis zur Quellen-TKÜ (vergleiche beispielsweise etwa Hamburg mit § 10c des Gesetzes über die Datenverarbeitung der Polizei, Rheinland-Pfalz mit § 31 des Polizei- und Ordnungsbehördengesetzes, Thüringen mit § 34a des Thüringer Gesetzes über die Aufgaben und Befugnisse der Polizei, Baden-Württemberg mit § 23b des Polizeigesetzes, Hessen mit § 15b des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und Bayern mit Artikel 42 des Gesetzes über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei). Das Land Niedersachsen plant die Aufnahme einer Befugnis zur Quellen-TKÜ in das Niedersächsische Gesetz über die öffentliche Sicherheit und Ordnung (siehe Drucksache 18/850 des Niedersächsischen Landtages, Seite 13, geplante Änderung des § 33a).

Entsprechend der Entscheidung des Bundesverfassungsgerichtes vom 27. Februar 2008, Aktenzeichen 1 BvR 370/07 (siehe Randnummer 190), ist das durch Artikel 10 des Grundgesetzes geschützte Fernmeldegeheimnis alleiniger grundrechtlicher Maßstab für die Beurteilung einer solchen Ermächtigung, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Kommunikationsvorgang beschränkt und dies durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt ist. Daher erklärt Absatz 2 Satz 1 Nummer 1 den Eingriff in ein informationstechnisches System zur Durchführung der Maßnahme nur dann für zulässig, wenn sichergestellt ist, dass ausschließlich laufende Telekommunikation erfasst wird. Absatz 2 Satz 1 Nummer 2 stellt eine besondere Ausgestaltung des Verhältnismäßigkeitsgrundsatzes dar und nennt mit der Gewährleistung der Aufzeichnung von Telekommunikation in unverschlüsselter Form einen der Hauptanwendungsfälle der Maßnahme.

Satz 2 greift die Regelung in § 100a Absatz 1 Satz 2 der Strafprozessordnung auf. Danach ist es erlaubt, auf dem informationstechnischen System der betroffenen Person auch gespeicherte Inhalte und Umstände der Kommunikation zu überwachen und aufzuzeichnen, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können. Mit dieser Änderung wird ausdrücklich festgelegt, dass Telekommunikationsinhalte auch auf dem Endgerät der betroffenen Person überwacht und aufgezeichnet werden dürfen. Dabei muss den Anforderungen des Bundesverfassungsgerichtes entsprechend technisch sichergestellt sein, dass nur solche Kommunikationsinhalte erfasst werden, die auch auf herkömmlichem Wege ausgeleitet werden können. Innerhalb dieses Rahmens stellt Satz 2 je nach Kommunikationsform sowohl eine Ermächtigungsgrundlage für Eingriffe in Artikel 10 Absatz 1 des Grundgesetzes (verschlüsselte Sprach- und Videotelefonie) als auch für Eingriffe in Artikel 2 Absatz 1 in Verbindung mit 1 Absatz 1 des Grundgesetzes (verschlüsselte Nachrichten über Messenger-Dienste) dar.

Bei der Überwachung und Aufzeichnung von Sprach- und Videotelefonie fallen die Ausleitung durch die Software und die Übertragung der Kommunikation zeitlich regelmäßig zusammen. Die Ausleitung erfolgt daher noch „während der Übertragung“ und nicht nach Beendigung des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers. Anders liegt es bei der Beschlagnahme beziehungsweise Sicherstellung von E-Mails. Sind diese auf dem Server eines Host-Providers (zum Beispiel Googlemail, GMX, web.de) end- oder zwischengespeichert, ist bei einem Eingriff dort der Schutzbereich des Artikels 10 des Grundgesetzes eröffnet. Ist die E-Mail dagegen auf dem Endgerät der betroffenen Person angekommen und in ihrem Mailprogramm (zum Beispiel Outlook) gespeichert, befindet sie sich in ihrem Herrschaftsbereich. Weil der Übertragungsvorgang unmittelbar mit der Ankunft der E-Mail auf dem Endgerät abgeschlossen ist, unterliegt ein Ausleiten dieser Kommunikation aus einem informationstechnischem System der betroffenen Person nicht mehr dem Fernmeldegeheimnis (siehe Bundesverfassungsgerichtsbeschluss vom 16. Juni 2009 - Aktenzeichen 2 BvR 902/06 - Randnummer 45).

Textnachrichten und sonstige Botschaften, die über Messenger-Dienste (zum Beispiel WhatsApp) versandt werden, enthalten - ebenso wie Sprach- und Videotelefonate - Kommunikationsinhalte, die IP-basiert und in der Regel verschlüsselt über das Datennetz übertragen werden können. Sie werden heute häufig als funktionales Äquivalent zu SMS-Nachrichten verwendet, um Texte, Bilder oder andere Inhalte (auch aufgezeichnete Sprachnachrichten) an Kommunikationspartner zu übermitteln. Anders als bei der Sprach- und Videotelefonie in Echtzeit ist jedoch der Übertragungsvorgang mit dem Zugang der Nachricht auf dem Endgerät der betroffenen Person abgeschlossen. Wie bei E-Mails ist die Nachricht im Herrschaftsbereich der betroffenen Person angekommen und der Schutzbereich des Persönlichkeitsrechts eröffnet.

Soweit das Bundesverfassungsgericht höhere Anforderungen an die Rechtfertigung von Eingriffen in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme stellt, so betreffen diese nicht den Fall, in dem die Überwachung und Aufzeichnung auf neu ankommende oder neu abgesendete Messenger-Nachrichten auf dem Endgerät begrenzt und technisch ausgeschlossen wird, dass das gesamte System oder auch nur die gesamte gespeicherte Kommunikation ausgelesen werden kann. In diesem Fall weist der Eingriff eine erheblich geringere Intensität und Reichweite auf, erfasst keine nur der betroffenen Person (und nicht auch Kommunikationspartnern) bekannten Inhalte und geht nicht über das hinaus, was die Strafverfolgungsbehörden mit einer herkömmlichen Telekommunikationsüberwachung ermittelt haben würden, wenn die betroffene Person diesen Kommunikationsweg gewählt hätte. Insoweit hinreichend, aber notwendig erweisen sich vielmehr die ebenfalls strengen Anforderungen, die aus Artikel 10 des Grundgesetzes für die Telekommunikationsüberwachung folgen (so auch Lisken/ Denninger, Handbuch des Polizeirechts, 6. Auflage, 2018, Teil E, Randnummer 769).

Ebenso wie bei der Sprach- und Videotelefonie darf das Ausleiten von Messenger-Nachrichten am Endgerät nur dann erfolgen, wenn dies ein funktionales Äquivalent zur Überwachung und Ausleitung der Nachrichten aus dem Telekommunikationsnetz darstellt.

Die vorgesehenen Änderungen setzen folglich ausschließlich das Ziel um, den technischen Entwicklungen der Informationstechnik Rechnung zu tragen und - ohne Zugriff auf weitere gespeicherte Inhalte des informationstechnischen Systems - eine Telekommunikationsüberwachung auch dort zu ermöglichen, wo dies mittels der alten Überwachungstechnik nicht mehr möglich ist. Um die funktionale Äquivalenz auch in zeitlicher Hinsicht zu gewährleisten, ist technisch sicherzustellen, dass über Messenger-Dienste versandte Nachrichten erst ab dem Zeitpunkt der Anordnung durch das Gericht beziehungsweise - in Eilfällen - die anordnungsbefugten Personen nach Absatz 4 ausgeleitet werden dürfen. Auch im Rahmen der herkömmlichen Telekommunikationsüberwachung können Kommunikationsinhalte erst von diesem Zeitpunkt an ausgeleitet werden. Auf dem Endgerät eines Kommunikationsinhabers sind jedoch unter Umständen auch Nachrichten gespeichert, die sich auf Zeiträume vor der Anordnung erstrecken. Die einzusetzende Software muss daher so programmiert sein, dass sie anhand der zu den einzelnen Nachrichten hinterlegten Meta-Daten, die etwa die Absende-, Empfangs- und Lesezeitpunkte enthalten, die ein- und ausgehenden Nachrichten erst ab dem Zeitpunkt der Anordnung ausleitet.

Satz 3 nimmt Bezug auf die technischen Anforderungen in § 33c Absatz 3. Auf die dortige Begründung wird verwiesen. Gleichzeitig wird mit dem Verweis auf § 33c Absatz 5 auch für die Maßnahme der Quellen-TKÜ ein Betretungs- und Durchsuchungsrecht gesetzlich geregelt. Auch wenn der Zugriff auf das betroffene informationstechnische System im Regelfall über Kommunikationsverbindungen dieses Systems eröffnet sein wird, so wird es dennoch auch Fälle geben, in denen das nicht möglich ist. Dabei sind Systeme denkbar, die einen unüberwindbaren Zugriffsschutz gegen Angriffe von außerhalb aufweisen, für die im Einzelfall das Bedürfnis des Zugriffs bestehen kann. Ferner kann eine weitgehende Abschottung des Geräts durch die betroffene Person, etwa dadurch, dass es überwiegend ausgeschaltet ist und nur in zeitlich knappen Zeitfenstern benutzt wird, dazu führen, dass ein Zugriff über die Kommunikationsverbindung praktisch unmöglich gemacht wird. Mit der vorhandenen Möglichkeit, solche Systeme im Wege der richterlich gestatteten Wohnungsbetretung und -durchsuchung zu identifizieren und auf den Zugriff vorzubereiten, wird eine Regelungslücke ausgeschlossen. Im Übrigen wird auf die Begründung zu § 33c Absatz 5 verwiesen.

Nach Satz 4 bleibt die Regelung zur Online-Überwachung unberührt, sodass deren Voraussetzungen zu beachten sind, sollten die Maßnahmen über die geregelten Fälle des Absatzes 3 hinausgehen.

Die Absätze 4 bis 6 tragen den im Urteil zum Bundeskriminalamtgesetz vom 20. April 2016 aufgestellten Anforderungen des Bundesverfassungsgerichtes an die grundrechtssichernde Funktion der unabhängigen Richterkontrolle und den sich daraus ergebenden Anforderungen an den Antrag und den Inhalt der Anordnung Rechnung. Die Einschränkung des Absatzes 5 Nummer 1 und 2 („soweit möglich“) resultiert aus dem Umstand, dass in der Praxis zum Beispiel nur die Anschrift einer Person, nur der Name oder gar nur eine Rufnummer oder andere Kennung ohne Personenzuordnung bekannt sein kann. Ähnlich verhält es sich mit der Einschränkung in Nummer 4, die darin begründet ist, dass in der Praxis nicht immer vorab ersichtlich ist, welche Sachen im Einsatzgeschehen vorgefunden werden oder welche Räumlichkeiten der betroffenen Person zuzuordnen sind.

In Absatz 7 wird der bisherige § 34a Absatz 6 mit sprachlichen Modifikationen, aber ohne Änderung der Verpflichtung übernommen.

Die bisherigen Absätze 7 bis 9 des § 34a entfallen, da sie in den zentralen Vorschriften zur Weiterverwendung in § 36, zur Kennzeichnung in § 46g, zur Benachrichtigung in § 46a, zur parlamentarischen Kontrolle in § 48h sowie zum gerichtlichen Verfahren in § 25b aufgehen. Zudem ist auch auf die in § 46f Absatz 2 Nummer 5 bestehende zusätzliche Protokollierungspflicht hinzuweisen.

Absatz 8 enthält eine ergänzende Regelung zur Vorschrift über den Schutz des Kernbereichs privater Lebensgestaltung in § 26a und erfasst die in der Praxis relevante Konstellation, dass die Telekommunikationsüberwachung durch eine automatische Aufzeichnung erfolgt. Dies geschieht durch die Ausleitung der entsprechenden Daten seitens der Diensteanbieter. Dabei kann auf der Erhebungsebene selbst bei zeitgleicher Prüfung eines Kernbereichsbezugs eine Unterbrechung und gegebenenfalls die Fortsetzung der angeordneten Maßnahme nicht zeitnah umgesetzt werden. Absatz 8 gewährleistet den Schutz des Kernbereichs privater Lebensgestaltung in Einklang mit der Rechtsprechung des Bundesverfassungsgerichtes auf der Verwertungsebene dadurch, dass automatisierte Aufzeichnungen vor einer Verwendung der oder dem behördlichen Datenschutzbeauftragten zur Entscheidung über einen möglichen Kernbereichsbezug der Maßnahme vorzulegen sind. Die Sätze 3 und 5 enthalten Regelungen für den Fall einer Gefahr im Verzug sowie bei Datenübermittlungen in dieser Konstellation analog zu § 26a Absatz 4 Satz 3 und 4. Satz 4 übernimmt aus der bisher bestehenden Regelung in § 34a Absatz 8 die Vorschrift, dass erhobene personenbezogene Daten Dritter (§ 3 Absatz 4 Nummer 2) unverzüglich nach der Entscheidung zur Datenweiterverarbeitung zu löschen sind, soweit dies technisch möglich ist.

§ 33e (Auskunft über Nutzungsdaten)

Der Auskunftsanspruch im Hinblick auf Nutzungsdaten nach dem Telemediengesetz ergänzt die in § 33d Absatz 1 geregelte Erhebungsbefugnis in Anlehnung an § 52 Absatz 2 des Bundeskriminalamtgesetzes. Auch andere Bundesländer haben bereits Befugnisse zur Erhebung von Daten nach dem Telemediengesetz in ihren Landesgesetzen verankert (siehe beispielsweise § 33b des Brandenburgischen Polizeigesetzes, § 23a des Polizeigesetzes Baden-Württemberg, § 20a des Polizeigesetzes des Landes Nordrhein-Westfalen, § 31b des Polizei- und Ordnungsbehördengesetzes Rheinland-Pfalz oder Artikel 43 des Gesetzes über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei). Das Land Niedersachsen plant die Aufnahme einer solchen Befugnis in das Niedersächsische Gesetz über die öffentliche Sicherheit und Ordnung (siehe Drucksache 18/850 des Niedersächsischen Landtages, Seite 13, geplante Änderung § 33a).

Nach Absatz 1 Satz 1 kann die Polizei unter den Voraussetzungen des § 33d Absatz 1 Auskunft über Nutzungsdaten im Sinne von § 15 Absatz 1 Satz 2 Nummer 2 und 3 des Telemediengesetzes verlangen.

Telemedien sind elektronische Informations- und Kommunikationsdienste, soweit sie nicht der Telekommunikation oder dem Rundfunk zuzuordnen sind. Die Abgrenzung kann im Einzelfall schwierig sein. Entscheidend ist letztlich der Gegenstand des Dienstes. Bei Telemediendiensten steht die Bereitstellung von Informationen im Vordergrund. Bei der Telekommunikation kommt es nicht auf die Bereitstellung von Informationen an, sondern auf die Bereitstellung von Datenübertragungsmöglichkeiten (zum Beispiel Telefon).

Zu den Unternehmen, die geschäftsmäßig Telemedien erbringen, zählen insbesondere Internetauktionshäuser oder -tauschbörsen, Anbieter von Videos auf Abruf oder Suchmaschinen im Internet. Angesichts der breiten Nutzung des Internets durch Täter, insbesondere auch des internationalen Terrorismus, können die Nutzungsdaten zur Abwehr von Gefahren und damit für die Arbeit der Polizei von großem Nutzen sein. Dies kann etwa dann der Fall sein, wenn bestimmte Gegenstände, wie Materialien zum Bau von Sprengkörpern, in Tauschbörsen angeboten werden oder Propagandamaterial, beispielsweise des islamistischen Terrorismus, über das Internet verbreitet wird. Mit der Ergänzung wird Überschneidungen und Abgrenzungsschwierigkeiten zwischen dem Telekommunikationsgesetz und dem Telemediengesetz für einzelne Internetdienste begegnet.

Vor allem mit Blick auf die praktische Handhabbarkeit für die Polizei erscheint eine ausdrückliche Bezugnahme auf Telemedienanbieter als Verpflichtete vorzugwürdig. Im Einzelfall bedarf es keiner Abgrenzung zwischen Telekommunikation oder Telemedien, die im Zweifel zur Verweigerung einer Auskunft seitens eines Diensteanbieters führt und damit eine effektive Gefahrenabwehr gefährden könnte.
Daten, die Telekommunikationsverkehrsdaten gleichzusetzen sind (§ 15 Absatz 1 Satz 2 Nummer 2 und 3 des Telemediengesetzes, zum Beispiel Dauer oder Umfang einer Telemediennutzung), dürfen nur unter den erhöhten Voraussetzungen aus § 33d Absatz 1 erhoben werden (so auch § 23a Absatz 1 des Polizeigesetzes Baden-Württemberg). Demgegenüber werden die Daten zur Identifizierung des Nutzers (§§ 14 und 15 Absatz 1 Satz 2 Nummer 1 des Telemediengesetzes) wegen der Vergleichbarkeit zu Telekommunikationsbestandsdaten an die Erhebungsvoraussetzungen des § 33h geknüpft.

Nach Satz 2 kann die Auskunft auch für die Zukunft verlangt werden. Diese Regelung ist notwendig, weil die Norm anders als die für Verkehrsdaten nicht als Erhebungsbefugnis ausgestaltet ist, sodass auch eine fortlaufende Auskunft verlangt werden können muss.

Absatz 2 bestimmt, dass für die Anordnung die Regelungen des § 33d Absatz 4 bis 6 - und damit die Vorschriften, die auch zur Erhebung von Verkehrsdaten festgelegt sind, - entsprechend gelten.

Im Übrigen gelten für die weitere Datenverarbeitung die Regelungen im Gesetz (siehe hierzu unter anderem § 36). Besonders ist hier auch auf die in § 46g Absatz 1 Satz 1 Nummer 8 normierte Kennzeichnungspflicht, auf die in § 46f Absatz 2 Nummer 5 bestehende zusätzliche Protokollierungspflicht und die in § 48h normierte Berichtspflicht hinzuweisen.

Absatz 3 Satz 1 stellt klar, dass aufgrund der getroffenen Anordnung jeder Diensteanbieter im Sinne des Telemediengesetzes der Polizei unverzüglich Auskunft über die Nutzungsdaten auf dem von ihr bestimmten Weg zu erteilen hat. Für die Entschädigung der Anbieter gilt die Regelung des § 33d Absatz 7 Satz 2 entsprechend.

§ 33f (Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten)

Die bislang in § 34a Absatz 3 Satz 1 geregelte Befugnis zur Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten wird aus Gründen der Übersichtlichkeit in eine eigene Norm überführt und an die neue Struktur der polizeilichen Datenerhebungsbefugnisse angepasst. Sie orientiert sich an § 53 des Bundeskriminalamtgesetzes.

Für die Anordnung wird bestimmt, dass § 33d Absatz 4 bis 6 entsprechend gilt.

Im Übrigen gelten für die weitere Datenverarbeitung die Regelungen im Gesetz (siehe unter anderem § 36). Besonders ist hier auch auf die in § 46g Absatz 1 Satz 1 Nummer 8 normierte Kennzeichnungspflicht, auf die in § 46f Absatz 2 Nummer 5 bestehende zusätzliche Protokollierungspflicht und die in § 48h normierte Berichtspflicht hinzuweisen.

Zudem wird klargestellt, dass aufgrund der Anordnung einer Maßnahme nach Absatz 1 Satz 1 Nummer 2 jeder Diensteanbieter im Sinne des Telekommunikationsgesetzes der Polizei unverzüglich die für die Ermittlung des Standortes des Mobilfunkendgeräts erforderliche Geräte- und Kartennummer mitzuteilen hat. Für die Entschädigung der Anbieter gilt § 33d Absatz 7 Satz 2 entsprechend.

§ 33g (Unterbrechung oder Verhinderung der Telekommunikation)

Die bislang in § 34a Absatz 3 Satz 2 geregelte Befugnis zur Unterbrechung oder Verhinderung der Telekommunikation wird aus Gründen der Übersichtlichkeit in eine eigene Norm überführt und an die neue Struktur der polizeilichen Datenerhebungsbefugnisse angepasst.

Die Anordnungsvoraussetzungen entsprechen denen des § 33d. Die Einschränkung des Absatzes 4 Nummer 1 und 2 („soweit möglich“) resultiert aus dem Umstand, dass in der Praxis zum Beispiel nur die Anschrift einer Person, nur der Name oder gar nur eine Rufnummer oder andere Kennung ohne Personenzuordnung bekannt sein kann.

Im Übrigen gelten für die weitere Datenverarbeitung die Regelungen im Gesetz (siehe unter anderem § 36). Besonders ist hier auch auf die in § 46g Absatz 1 Satz 1 Nummer 8 normierte Kennzeichnungspflicht, auf die in § 46f Absatz 2 Nummer 5 bestehende zusätzliche Protokollierungspflicht und die in § 48h normierte Berichtspflicht hinzuweisen.

§ 33h (Auskunft über Bestandsdaten)

Die Befugnis zur Auskunft über Bestandsdaten ist im bisher geltenden § 28a enthalten und wird mit Blick auf die Gesetzessystematik in § 33h mit Anpassungen übernommen.

Die in § 28a Absatz 1 bereits enthaltene Befugnis zur Beauskunftung von Telekommunikationsbestandsdaten wird in Anlehnung an entsprechende Regelungen in anderen Ländern (etwa § 31f Polizei- und Ordnungsbehördengesetzes Rheinland-Pfalz, § 180a des Landesverwaltungsgesetzes Schleswig-Holstein oder § 23a des Polizeigesetzes Baden-Württemberg) um einen Auskunftsanspruch gegenüber Telemedienanbietern erweitert, um im Bereich der Gefahrenabwehr mögliche Regelungslücken zu schließen, die wegen der teilweise schwierigen Abgrenzung zwischen Telekommunikations- und Telemediendiensten entstehen können.

Im Übrigen wird auf die Begründung zu § 33e Absatz 1 verwiesen.

Absatz 2 enthält die bislang in § 28a Absatz 2 geregelte Befugnis. Neben der zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse kann nunmehr über weitere zur Individualisierung einer Person erforderliche technische Daten Auskunft verlangt werden (so auch § 23a Absatz 9 Satz 2 des Polizeigesetzes Baden-Württemberg). Aufgrund der technischen Bedingungen kann eine solche weitere Auskunft notwendig sein. Dies ist unter anderem bei der Verbreitung findenden Network Address Port Translation-Technologie der Fall, bei der dynamische Internetprotokoll-Adressen zeitgleich mehrfach an verschiedene Nutzer vergeben werden und daher die Auskunft über einen Nutzer der Einbeziehung zusätzlicher Daten bedarf.

Die bislang in § 28a Absatz 2 vorgesehene Benachrichtigung der betroffenen Person findet sich in der zentralen Vorschrift des § 46a Absatz 1 Satz 1 Nummer 4 wieder.

Im Übrigen gelten für die weitere Datenverarbeitung die Regelungen im Gesetz (siehe unter anderem § 36). Besonders ist hier auch auf die in § 46g Absatz 1 Satz 1 Nummer 8 normierte Kennzeichnungspflicht hinzuweisen.

Absatz 3 entspricht inhaltlich dem bisherigen § 28a Absatz 3. Die Entschädigungspflicht der Diensteanbieter bleibt über den Verweis auf § 33d Absatz 7 Satz 2 erhalten.

§ 34 (Einsatz unbemannter Luftfahrtsysteme)

In § 34 wird eine klarstellende Norm geschaffen, die die Verwendung unbemannter Luftfahrtsysteme (umgangssprachlich auch als Drohnen bekannt) als Einsatzmittel bei bestimmten polizeilichen oder ordnungsbehördlichen Maßnahmen bestimmt.

Es gibt vielfältige Möglichkeiten zum Einsatz von Drohnen, etwa bei offenen Maßnahmen wie der Suche nach vermissten oder sonst polizeilich relevanten Personen, Sachen oder Tieren, der Ortung von Mobilfunkgeräten, des Zugriffs auf WLAN-Netzwerke, der Koordinierung des polizeilichen Einsatzes im Rahmen von Veranstaltungen und Ansammlungen sowie im öffentlichen Verkehrsraum mittels Übersichtsaufnahmen nach § 32 Absatz 1 Satz 1 Nummer 2. Aber auch beispielsweise bei der verdeckten Observation von Personen und Objekten kann der Einsatz von Drohnen den Maßnahmeerfolg begünstigen.

Da es sich in den genannten Fällen bei den unbemannten Luftfahrtsystemen lediglich um ein technisches Mittel handelt, wäre auch nach dem Wortlaut der bisherigen Regelungen im SOG M-V bereits jetzt deren Einsatz als technisches Mittel grundsätzlich möglich. Aufgrund der mit dem Einsatz von Drohnen einhergehenden, möglichen zusätzlichen Eingriffsqualität wird im neu eingefügten § 34 jedoch nun eine gesetzliche Klarstellung normiert, bei welchen Maßnahmen nach dem SOG M-V ihr Einsatz zulässig ist.

Unter den Voraussetzungen der in Satz 1 Nummer 1 bis 5 aufgeführten Befugnisnormen ist dabei auch ein Drohneneinsatz zur Datenerhebung zulässig. Das bedeutet zugleich, dass keine Ausweitung der genannten Befugnisnormen erfolgt. Gestatten diese beispielsweise keine Datenerhebung aus Wohnungen, so darf dies auch nach § 34 nicht erfolgen. Vielmehr ist bei dem Einsatz einer Drohne sicherzustellen, dass eine Einsichtnahme in Wohnräume, die schon beim Überfliegen privater Grundstücke denkbar ist, soweit möglich, verhindert wird, wenn ein solcher Zugriff nicht durch die entsprechende Befugnisnorm zulässig wäre.

Auch die Offenheit einer Maßnahme, wie beispielsweise in § 32 Absatz 1 normiert, darf durch den Drohneneinsatz nicht gefährdet werden. Es sind gegebenenfalls zusätzliche Maßnahmen zur Aufklärung der betroffenen Personen, wie etwa zusätzliche Hinweisschilder (zum Beispiel am Eingang einer Veranstaltung oder auf der Kleidung der die Drohne führenden Person), entsprechende Einstellungen an der Drohne selbst (akustische oder optische Hinweise) oder mündliche Ankündigungen, zu treffen, wobei bestehende Ausnahmeregelungen bei Gefahr im Verzug hiervon unberührt bleiben. Zudem ist bei einem Einsatz von Drohnen ebenfalls der Grundsatz der Verhältnismäßigkeit (§ 15) zu beachten.

Auch wenn § 21a Absatz 2 Nummer 1 der Luftverkehrs-Ordnung keinen Kenntnisschein im Sinne von § 21a Absatz 4 LuftVO verlangt, werden interne Schulungen zur Bedienung der Drohnen schon aus Haftungsgründen unabdingbar sein. Der Personenkreis, der in der Praxis eine Drohne gefahrenabwehrend einsetzen darf, ist schon allein daher aufgrund ergänzender Voraussetzungen (Schulungen zur Steuerung von Drohnen) ohnehin begrenzt. Vertrauenspersonen sind nach Satz 2 jedoch ausdrücklich nicht zur Verwendung von Drohnen befugt.

Der Einsatz von konventionellen Luftfahrzeugen, die der Bevölkerung etwa durch lautere Fluggeräusche und/oder größere Abmessungen auffälliger und letztlich auch vertrauter sind, wie zum Beispiel Hubschrauber, bleibt von der Vorschrift unberührt.

§ 35 (Ausschreibung zur polizeilichen Beobachtung und gezielten Kontrolle)

Die in § 35 verankerte Norm zur Ausschreibung zur polizeilichen Beobachtung wird teilweise umgestaltet und an den üblichen Aufbau der Datenerhebungsvorschriften angepasst sowie um die gezielte Kontrolle ergänzt.

Mit dem in Absatz 1 eingefügten Verweis auf § 67c wird der Anwendungsbereich der Norm so erweitert, dass Straftaten nach § 67c, soweit sie nicht bereits von § 49 erfasst sind, miterfasst sind. So sollen Anwendungslücken vermieden werden. Zudem wird die Norm dahingehend geändert, dass die bisherige Aufzählung der erhebbaren personenbezogenen Daten durch das Einfügen des Wortes „insbesondere“ nicht mehr als abschließende Aufzählung ausgestaltet ist. Damit erfolgt eine Anpassung des Anwendungsbereiches an bereits bestehende Bundes- und Länderregelungen (siehe hierzu unter anderem § 47 Absatz 1 des Bundeskriminalamtgesetzes, § 32 Absatz 1 Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz, § 36 Absatz 1 Brandenburgisches Polizeigesetz oder Artikel 40 Absatz 1 des Gesetzes über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei). Mit der Einfügung zu den Kontakt- und Begleitpersonen wird zur Klarstellung auf die präzisierte Definition in § 27 Absatz 3 Nummer 2 verwiesen. Die Maßnahmen nach Absatz 1 und 2 können gemäß Satz 2 auch dann angewendet werden, wenn die in § 67a Absatz 1 beschriebene Gefahrensituation vorliegt.

Zudem wird mit Absatz 2 die Befugnis entsprechend den Regelungen in anderen Bundesländern (vergleiche etwa § 25 Polizeigesetz Baden-Württemberg, § 17 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung, § 37 Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei) oder bundesrechtlich im neugefassten § 47 des Bundeskriminalamtgesetzes dadurch ergänzt, dass nunmehr auch die Ausschreibung zur gezielten Kontrolle ermöglicht wird.

Die Ausschreibung zur polizeilichen Beobachtung dient lediglich dem Zweck, polizeiliche Zufallserkenntnisse über das Antreffen einer bestimmten ausgeschriebenen Person zusammenzuführen und an die ausschreibende Dienststelle zu übermitteln, um dort insbesondere punktuell die Reisewege der Person sowie Zusammenhänge und Querverbindungen nachvollziehen zu können. Demgegenüber dient die Ausschreibemöglichkeit zur gezielte Kontrolle darüber hinausgehend dem Zweck, Ausschreibungen mit der Intention zu veranlassen, dass weitergehende polizeiliche Maßnahmen der Identitätsfeststellungen sowie der Personen- und Sachdurchsuchung durch die kontrollierende Polizeidienststelle getroffen und auch die aus diesen Maßnahmen erlangten Erkenntnisse der ausschreibenden Dienststelle mitgeteilt werden. Hierdurch wird die Möglichkeit geschaffen, wichtige Informationen, wie zum Beispiel schriftliche Unterlagen über Personenzusammenhänge und den Organisierungsgrad extremistischer oder terroristischer Gruppierungen, potenzielle Anschlagsziele, Anschlagsvorbereitungen oder illegale Finanztransaktionen erheben zu können sowie in der offenen Ermittlungsphase den Druck zu erhöhen, potentielle Gefährder zu verunsichern und hierdurch gegebenenfalls von ihrem beabsichtigten Tun abzubringen. Zur Erreichung des mit der gezielten Kontrolle verfolgten Ziels werden in Satz 2 für die Polizei bereits nach anderen Vorschriften zustehende Befugnisse zur Identitätsfeststellung sowie zur Durchsuchung von Personen und Sachen gesondert geregelt. Aus Satz 3 ergibt sich diesbezüglich die Einschränkung, dass die in den anderen Regelungen vorgesehenen Verfahrensvorschriften auch für die im Rahmen der gezielten Kontrolle durchgeführten Maßnahmen Anwendung finden, so etwa § 54 bei der Durchsuchung vom Personen oder § 58 bei der Durchsuchung von Sachen.

Die Absätze 3 bis 5 regeln die Antrags- und Anordnungsbefugnisse sowie die Befristung der Ausschreibung. Inhaltlich entsprechen diese bis auf die präzisierten Antragserfordernisse der bisherigen Regelungslage in § 35. Insbesondere werden die Befugnis der Leitung der zuständigen Polizeibehörde zur erstmaligen Anordnung sowie die erst bei der Fortsetzung der Maßnahme erforderliche richterliche Anordnung beibehalten. Die Einschränkung des Absatzes 4 Nummer 1 („soweit möglich“) resultiert aus dem Umstand, dass in der Praxis zum Beispiel nur die Anschrift einer Person oder nur der Name bekannt sein kann.

Satz 1 des bisher geltenden § 35 Absatz 3 wird in den neuen Absatz 5 übernommen. Er bleibt trotz der bestehenden Regelung zur Löschung im § 45 bestehen, da hier ein unverzügliches aktives Tun zur Löschung der Ausschreibung im hierfür genutzten technischen System gefordert wird, um eine erneute Datenspeicherung oder die Durchführung von Kontrollen auszuschließen. Im Übrigen bleibt der bisherige Absatz 3 als Absatz 5 erhalten.

Im Übrigen können die weiteren Regelungen im bisher geltenden § 35 Absatz 2 und 3 zur gerichtlichen Zuständigkeit oder Benachrichtigung der betroffenen Personen mit Blick auf die hierzu neu geschaffenen gesonderten Normen im Gesetz entfallen.

§ 36 (Zweckbindung, Grundsatz der hypothetischen Datenneuerhebung)

Mit den Änderungen in § 36 wird das vom Bundesverfassungsgericht in seinem Urteil zum Bundeskriminalamtgesetz vom 20. April 2016 konkretisierte und geprägte Kriterium der hypothetischen Datenneuerhebung präzisiert und die Maßgaben des Gerichtes für besonders eingriffsintensive Maßnahmen umgesetzt. Die Regelung entspricht weitgehend § 12 des Bundeskriminalamtgesetzes und wird an den Anwendungsbereich des SOG M-V angepasst.

In seinem vorgenannten Urteil hat das Bundesverfassungsgericht festgestellt, dass sich die Anforderungen an die Nutzung und Übermittlung staatlich erhobener Daten nach den Grundsätzen der Zweckbindung und Zweckänderung und sich die Reichweite der Zweckbindung nach der jeweiligen Ermächtigung für die Datenerhebung richten. Die Datenerhebung selbst bezieht ihren Zweck zunächst aus dem jeweiligen Verfahren.

Das Bundesverfassungsgericht führt im angegebenen Urteil unter den Randnummern 286f aus, dass die Ermächtigung zu einer Zweckänderung am Verhältnismäßigkeitsgrundsatz zu messen ist und sich die Verhältnismäßigkeitsanforderungen für eine Zweckänderung der Verarbeitung von personenbezogenen Daten, die aus besonders eingriffsintensiven Maßnahmen stammen, am Grundsatz der hypothetischen Datenneuerhebung orientieren:

„Hierbei orientiert sich das Gewicht, das einer solchen Regelung im Rahmen der Abwägung zukommt, am Gewicht des Eingriffs der Datenerhebung. Informationen, die durch besonders eingriffsintensive Maßnahmen erlangt wurden, können auch nur zu besonders gewichtigen Zwecken benutzt werden (vgl. BVerfGE 100, 313 <394>; 109, 279 <377>; 133, 277 <372 f. Rn. 225> m. w. N.). Für Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen wie denen des vorliegenden Verfahrens kommt es danach darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben neu auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln erhoben werden dürften.“

Das Kriterium der hypothetischen Datenneuerhebung wird in § 36 als allgemeiner Grundsatz formuliert, der bei jeder Datenverarbeitung durch die Ordnungsbehörden und die Polizei - unabhängig von der jeweiligen Eingriffsintensität der ursprünglichen Erhebungsmaßnahme - zu beachten ist, soweit das Gesetz nichts Besonderes bestimmt.

Absatz 1 Satz 1 stellt klar, dass die Verarbeitung von personenbezogenen Daten zur Erfüllung derselben Aufgabe und zum Schutz derselben Rechtsgüter oder zur Verhütung derselben Straftaten oder Ordnungswidrigkeit durch die Ordnungsbehörden beziehungsweise durch die Polizei nicht den verfassungsrechtlichen Anforderungen an eine Zweckänderung unterliegt. Das Bundesverfassungsgericht führt hierzu im vorbenannten Urteil unter den Randnummern 278 f und 282 aus:

„Der Gesetzgeber kann eine Datennutzung über das für die Datenerhebung maßgebende Verfahren hinaus als weitere Nutzung im Rahmen der ursprünglichen Zwecke dieser Daten erlauben. Er kann sich insoweit auf die der Datenerhebung zugrundeliegenden Rechtfertigungsgründe stützen und unterliegt damit nicht den verfassungsrechtlichen Anforderungen an eine Zweckänderung. Die zulässige Reichweite solcher Nutzungen richtet sich nach der Ermächtigung für die Datenerhebung. Die jeweilige Eingriffsgrundlage bestimmt Behörde, Zweck und Bedingungen der Datenerhebung und definiert damit die erlaubte Verwendung. Die Zweckbindung der auf ihrer Grundlage gewonnenen Informationen beschränkt sich folglich nicht allein auf eine Bindung an bestimmte, abstrakt definierte Behördenaufgaben, sondern bestimmt sich nach der Reichweite der Erhebungszwecke in der für die jeweilige Datenerhebung maßgeblichen Ermächtigungsgrundlage. Eine weitere Nutzung innerhalb der ursprünglichen Zwecksetzung kommt damit nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für die Datenerhebung maßgeblich. [….]

Für die Wahrung der Zweckbindung kommt es demnach darauf an, dass die erhebungsberechtigte Behörde die Daten im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutzt, wie es die jeweilige Datenerhebungsvorschrift erlaubt.“

Abweichend von § 12 des Bundeskriminalamtgesetzes enthält Satz 1 keine Regelung zur Weiterverwendung von Daten zu Strafverfolgungszwecken, da hier die Weiterverwendung von Daten zu Zwecken des SOG M-V geregelt wird und keine Zweckänderung wie in Absatz 2.

Satz 2 trägt den besonderen Anforderungen des Bundesverfassungsgerichtes (siehe angegebenes Urteil Randnummer 283) an die Zweckbindung für Daten aus Maßnahmen durch den Einsatz technischer Mittel in oder aus Wohnungen (§ 33b) und durch verdeckte Eingriffe in informationstechnische Systeme (§ 33c) Rechnung. Aufgrund des besonderen Eingriffsgewichts solcher Datenerhebungen gilt hier eine besonders enge Bindung jeder weiteren Nutzung der bei diesen Maßnahmen gewonnenen Daten an die Voraussetzungen und Zwecke der Datenerhebung. Das Bundesverfassungsgericht führt hierzu aus:

„Weiter reicht die Zweckbindung allerdings für Daten aus Wohnraumüberwachungen und Online-Durchsuchungen: Hier ist jede weitere Nutzung der Daten nur dann zweckentsprechend, wenn sie auch aufgrund einer den Erhebungsvoraussetzungen entsprechenden dringenden Gefahr (vgl. BVerfGE 109, 279 <377, 379>) oder im Einzelfall drohenden Gefahr (vgl. BVerfGE 120, 274 <326, 328 f.>) erforderlich ist. Das außerordentliche Eingriffsgewicht solcher Datenerhebungen spiegelt sich hier auch in einer besonders engen Bindung jeder weiteren Nutzung der gewonnenen Daten an die Voraussetzungen und damit Zwecke der Datenerhebung. Eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz unabhängig von einer dringenden oder im Einzelfall drohenden Gefahr kommt hier nicht in Betracht.“

Für die Verarbeitung von personenbezogenen Daten, die aus Maßnahmen durch den Einsatz technischer Mittel in oder aus Wohnungen (§ 33b) und durch verdeckte Eingriffe in informationstechnische Systeme (§ 33c) erlangt wurden, sieht Satz 2 daher vor, dass im Einzelfall eine Gefahrenlage im Sinne der §§ 33b und 33c Maßnahme vorliegen muss, was eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz ausschließt.

In Absatz 2 werden die Vorgaben des Bundesverfassungsgerichtes an die zweckändernde Verarbeitung von personenbezogenen Daten umgesetzt und der bereits zuvor in Absatz 1 Satz 3 der derzeitigen Fassung des § 36 enthaltenen Grundsatz der hypothetischen Datenneuerhebung dabei entsprechend konkretisiert.

Das Bundesverfassungsgericht hat im vorbenannten Urteil unter den Randnummern 288 bis 290 zum Grundsatz der hypothetischen Datenneuerhebung ausgeführt:

„Voraussetzung für eine Zweckänderung ist danach aber jedenfalls, dass die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten [...]. Nicht in jedem Fall identisch sind die Voraussetzungen einer Zweckänderung mit denen einer Datenerhebung hingegen hinsichtlich des erforderlichen Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts.

Die diesbezüglichen Anforderungen bestimmen unter Verhältnismäßigkeitsgesichtspunkten primär den Anlass nur unmittelbar für die Datenerhebung selbst, nicht aber auch für die weitere Nutzung der erhobenen Daten. Als neu zu rechtfertigender Eingriff bedarf aber auch die Ermächtigung zu einer Nutzung für andere Zwecke eines eigenen, hinreichend spezifischen Anlasses. Verfassungsrechtlich geboten, aber regelmäßig auch ausreichend, ist insoweit, dass sich aus den Daten - sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde - ein konkreter Ermittlungsansatz ergibt. Der Gesetzgeber kann danach - bezogen auf die Datennutzung von Sicherheitsbehörden - eine Zweckänderung von Daten grundsätzlich dann erlauben, wenn es sich um Informationen handelt, aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter wie die ergeben, zu deren Schutz die entsprechende Datenerhebung zulässig ist.“

Die „Vergleichbarkeit“ ergibt sich aus den rechtsgutsbezogenen Erhebungsschwellen. Ergeben sich etwa aus einer Telekommunikationsüberwachung, die nach § 33d Absatz 1 Nummer 1 zur Abwehr einer Lebensgefahr erfolgt, Zufallserkenntnisse zu einem anderen Lebenssachverhalt mit Anhaltspunkten für eine Freiheitsgefahr beziehungsweise eine entsprechend schwerwiegende Verletzung (vergleiche § 100a Absatz 2 der Strafprozessordnung), kann auch diese andere Gefahr mit diesem Spurenansatz weiter erforscht beziehungsweise einer Straftat entsprechend nachgegangen werden. Das Rechtsgut „Freiheit“ erscheint zwar gegenüber dem Rechtsgut „Leben“ nicht gleichgewichtig, mit Blick auf die Erhebungsschwelle der Art der jeweiligen Maßnahme aber vergleichbar gewichtig. Dies wird durch den eingefügten Passus „unter Berücksichtigung der jeweiligen Datenerhebungsvorschrift“ hervorgehoben. Dadurch wird insbesondere dem Umstand Rechnung getragen, dass eine Erhebung personenbezogener Daten nach den allgemeinen Vorschriften etwa zur Abwehr einer gegenwärtigen oder erheblichen Gefahr nicht dazu führt, dass eine Zweckänderung nur bei Vorliegen einer entsprechenden Gefahr erlaubt ist, wenn die Datenneuerhebung zu diesem Zweck mangels einer erhöhten Eingriffsschwelle auch nach den allgemeinen Erhebungsvorschriften erfolgen könnte.

Der Begriff „in einem übersehbaren Zeitraum drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter“ in Satz 2 Nummer 2b, zu deren Schutz die entsprechende Datenerhebung verfassungsrechtlich zulässig wäre, bezieht sich nicht ausschließlich auf das klassische Polizei- und Gefahrenabwehrrecht. Das Bundesverfassungsgericht wollte vielmehr ausschließen, dass eine Datennutzung „ins Blaue hinein“ eröffnet ist. Erforderlich und ausreichend ist daher, dass sich eine Gefahr für mindestens vergleichbar bedeutsame Rechtsgüter, zu deren Schutz die ursprüngliche Datenerhebung vorgenommen wurde, nicht nur abstrakt, sondern vielmehr als eine in ersten Umrissen absehbare und konkretisierte Möglichkeit eines Schadenseintrittes für ein solches Rechtsgut darstellt. Der Begriff des Rechtsgutes bezeichnet das rechtlich geschützte Interesse einzelner Rechtspersonen (Individualrechtsgüter) und der Gesellschaft sowie des Staates als solcher (Universalrechtsgüter).

Besonders bedeutsame Individualrechtsgüter sind insbesondere das Leben, die Freiheit, die körperliche Unversehrtheit oder die sexuelle Selbstbestimmung. Unter die besonders bedeutsamen Universalrechtsgüter fallen insbesondere die in § 3 des Bundesverfassungsschutzgesetzes genannten Rechtsgüter. Als besonders gewichtiges Rechtsgut ist auch der Schutz der Sicherheit der Bundesrepublik Deutschland anzusehen, der ausländerrechtliche Maßnahmen insbesondere gegen ausländische Gefährder oder erheblich straffällig gewordene Ausländerinnen oder Ausländer rechtfertigt und für den die Ausländerbehörden polizeiliche Erkenntnisse benötigen. Insoweit ist eine Datenverarbeitung zu diesen Zwecken zulässig, wenn die ursprüngliche Datenerhebung zum Schutz von vergleichbar bedeutsamen Rechtsgütern erfolgte.

Die Ergänzung „soweit Rechtsvorschriften dieses Gesetzes oder anderer Gesetze die zweckändernde Weiterverarbeitung nicht besonders regeln oder wenn andere Rechtsvorschriften dieses Gesetzes oder anderer Gesetze eine Datenerhebung zu dem anderen Zweck mit vergleichbaren Mitteln zulassen.“ dient dem Ausschluss von Gesetzeskonkurrenzen. In der Praxis wird dies insbesondere Regelungen der Strafprozessordnung betreffen, wenn personenbezogene Daten, die im Rahmen der Gefahrenabwehr erhoben wurden, als Beweis im Strafverfahren genutzt werden sollen. So hat der Bundesgesetzgeber etwa für die Regelung des Strafverfahrens die konkurrierende Gesetzgebungskompetenz nach Artikel 74 Absatz 1 des Grundgesetzes, die als Annex auch das jeweilige Datenschutzrecht umfasst. Von dieser hat er beispielsweise in § 100e Absatz 6 Nummer 3 der Strafprozessordnung Gebrauch gemacht. Die Umwidmung von Daten, die zu Gefahrenabwehrzwecken erhoben wurden, richtet sich damit grundsätzlich nach den vorhandenen spezialgesetzlichen Vorschriften. Gleichzeitig wird klargestellt, dass der allgemeine Grundsatz durch eine spezielle Regelung zur zweckändernden Weiterverarbeitung verdrängt wird.

Satz 2 stellt klar, dass der Grundsatz der hypothetischen Datenneuerhebung die Nutzung personenbezogener Daten zu Zwecken der wissenschaftlichen Forschung, der Aus- und Fortbildung sowie zu statistischen Zwecken (siehe hierzu § 37a) nicht ausschließt.

Absatz 3 Satz 1 trägt den besonderen Anforderungen des Bundesverfassungsgerichtes an die zweckändernde Nutzung von Daten aus Maßnahmen durch den Einsatz technischer Mittel in oder aus Wohnungen (§ 33b) und durch verdeckte Eingriffe in informationstechnische Systeme (§ 33c) Rechnung. Ihre Verwendung zu einem geänderten Zweck ist im Falle des Vorliegens einer Gefahr nur möglich, wenn im Einzelfall die für die Datenerhebung maßgeblichen Anforderungen an die Gefahrenlage erfüllt sind.

Das Bundesverfassungsgericht stellt in seinem vorbenannten Urteil vom 20. April 2016 als Anforderung an das Kriterium der hypothetischen Datenneuerhebung die Voraussetzung auf, dass die Verwendung der erhobenen personenbezogenen Daten zu einem neuen Zweck nur zulässig ist, wenn für den neuen Zweck eine entsprechende Datenerhebung nach verfassungsrechtlichen Maßstäben zulässig wäre. Das Bundesverfassungsgericht führt hierzu unter der Randnummer 317 aus:

„Verfassungsrechtlich zu beanstanden ist weiterhin, dass Daten aus optischen Wohnraumüberwachungen von einer Übermittlung an die Strafverfolgungsbehörden nicht ausgeschlossen sind. Artikel 13 Absatz 3 GG erlaubt für die Strafverfolgung nur den Einsatz der akustischen Wohnraumüberwachung. Dies darf durch eine Übermittlung von Daten aus einer präventiv angeordneten optischen Wohnraumüberwachung nicht unterlaufen werden."

Satz 2 dient der Umsetzung dieser Anforderung des Bundesverfassungsgerichtes, indem er untersagt, dass Erkenntnisse aus optischen Wohnraumüberwachungen zu Strafverfolgungszwecken verwendet werden dürfen.

Absatz 4 sieht vor, dass die strengen Vorgaben der Zweckbindung und der Grundsatz der hypothetischen Datenneuerhebung nicht gelten, wenn die Grunddaten einer Person zu Identifizierungszwecken verwendet werden sollen.

Da die Datenverwendung so eng begrenzt ist - nur Grunddaten nach § 3 Absatz 5 Nummer 2 des Gesetzes (nicht Daten nach Nummer 3) und nur zum Zweck der Identifizierung -, ist das Eingriffsgewicht dieser Maßnahme mit der Rechtsprechung des Bundesverfassungsgerichtes vereinbar. Weitere Daten - etwa die weiteren zu einer als „Treffer" identifizierten Person gespeicherten Ereignisse - sind hingegen nach Absatz 4 nicht verfügbar; insoweit bleibt es bei den Begrenzungen nach den Absätzen 2 und 3.

Die zweifelsfreie Klärung der Identität einer Person ist notwendig, um Identitätsverwechslungen auszuschließen und damit zu verhindern, dass Eingriffe in die Grundrechte von unbeteiligten Personen stattfinden. Die Sicherheitsbehörden müssen daher zur Erfüllung ihrer Aufgaben die Grunddaten einer Person stets zu diesem Zweck verarbeiten können.

Absatz 5 sieht die Verpflichtung der Gefahrenabwehrbehörden vor, bei der Verarbeitung von personenbezogenen Daten durch technische und organisatorische Vorkehrungen sicherzustellen, dass die Voraussetzungen des Grundsatzes der hypothetischen Datenneuerhebung beachtet werden.

Die in Absatz 5 geregelte Verpflichtung findet ihre nähere Ausgestaltung unter anderem in der Regelung zur Kennzeichnung nach § 46g.

§ 37 (Voraussetzungen der Verarbeitung personenbezogener Daten aus Strafermittlungsverfahren)

§ 37 entspricht weitgehend der bisherigen speziellen Regelung zur zweckändernden Weiterverwendung von personenbezogenen Daten aus strafrechtlichen Ermittlungsverfahren.

Der Verweis in Absatz 1 auf § 36 Absatz 2 und 3 dient der Klarstellung, dass auch für diese Zweckänderung der Grundsatz der hypothetischen Datenneuerhebung gilt inklusive der Regelung zum Ausschluss von Gesetzeskonkurrenzen (vergleiche dazu auch die Begründung zu § 36 Absatz 2). Satz 2 stellt klar, dass die Nutzung personenbezogener Daten zu Zwecken der wissenschaftlichen Forschung, der Aus- und Fortbildung sowie zu statistischen Zwecken auch hier nicht ausgeschlossen ist.

Absatz 2 bleibt unverändert und Absatz 3 enthält lediglich eine sprachliche Anpassung.

Absatz 4 regelt die Anwendbarkeit des § 36 Absatz 5. Auf die dortige Begründung wird verwiesen.

§ 37a (Verarbeitung zu Zwecken der wissenschaftlichen und historischen Forschung, Aus- und Fortbildung und Statistik)

Der bisher geltende § 36 Absatz 4 enthält Vorschriften zur Nutzung personenbezogener Daten zu Aus- und Fortbildungszwecken und zu statistischen Zwecken. Sie werden in § 37a überführt und angepasst. Mit § 37a wird eine einheitliche Vorschrift über die Verarbeitung von Daten zu Zwecken der wissenschaftlichen und historischen Forschung, Aus- und Fortbildung und Statistik im SOG M-V verankert.

Absatz 1 stellt gleich zu Beginn ein Verbot der weiteren Nutzung personenbezogener Daten zu Zwecken der wissenschaftlichen und historischen Forschung sowie zur Aus- und Fortbildung auf, die in oder aus Wohn- oder Geschäftsräumen oder befriedetem Besitztum oder aus einer Maßnahme nach § 33c (Befugnis zum Eingriff in informationstechnische Systeme) erhoben wurden oder aus kernbereichsrelevanten Fällen des § 26a Absatz 3 oder des § 26b (Schutz zeugnisverweigerungsberechtigter Personen) stammen. Wegen der besonderen Eingriffsintensität der Maßnahmen beziehungsweise der möglichen Sensibilität der Daten sollen diese nicht zu den entsprechenden Zwecken verwendet werden dürfen. Die grundlegenden Verwendungsverbote beanspruchen unabhängig davon Geltung.

Absatz 2 regelt die Verwendung von Daten zu Zwecken der wissenschaftlichen oder historischen Forschung, die nicht unter Absatz 1 fallen. Diese richtet sich nach § 9 des Landesdatenschutzgesetzes.

Absatz 3 regelt abweichend von § 4 des Landesdatenschutzgesetzes die Verwendung personenbezogener Daten zu Zwecken der Aus- und Fortbildung durch Polizei und Ordnungsbehörden und durch die mit der Aus- und Fortbildung ihrer Beschäftigten beauftragten öffentlichen Stellen (wie beispielsweise die Fachhochschule für öffentliche Verwaltung, Polizei und Rechtspflege M-V). Vor allem im Rahmen der polizeilichen Aus- und Fortbildung ist die Verwendung von Videomaterialien aus Einsatzgeschehen unabdingbar. Dabei sollen personenbezogene Daten der Gefahrenabwehrbehörden nur verwendet werden, wenn auf andere Weise das Ziel der Aus- oder Fortbildung nicht erreichbar ist und nicht überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen. Soweit der Zweck der Weiterverarbeitung dieses zulässt und kein unvertretbarer Verwaltungsaufwand entgegensteht, sind diese Daten zu anonymisieren. Durch den Einsatz entsprechender Bildbearbeitungsprogramme dürfte dies in der Regel der Fall sein.

Absatz 4 übernimmt die bisherige Regelung des § 36 Absatz 4 unter sprachlicher Anpassung.

§ 38 (Weiterverarbeitung personenbezogener Daten zur Vorgangsverwaltung und befristeten Dokumentation)

Die Bezeichnung des § 38 und sein Inhalt werden sprachlich angepasst und die Bezeichnung des Innenressorts wird aktualisiert. Die bisher in Satz 2 geregelte Nichtanwendung der §§ 36 und 37 ist nun auch auf den neu aufgenommenen § 37a zu erweitern. Denn die Regelungen zur Verarbeitung von personenbezogenen Daten zum Zwecke der Aus- und Fortbildung ist nicht mehr wie bisher in § 36 Absatz 4, sondern im neuen § 37a enthalten. Darüber hinaus enthält § 37a weitere Regelungen zur Verarbeitung personenbezogener Daten zu Zwecken der wissenschaftlichen und historischen Forschung sowie der Statistik. Auch diese Regelungen des § 37a sollen zukünftig aufgrund der in § 38 Satz 1 geregelten strengen Zweckbindung nicht zur Anwendung gelangen.

§ 39 (Grundsätze der Datenübermittlung)

Die bisher in den §§ 39 bis 41 SOG M-V enthaltenen Regelungen zur Datenübermittlung bedurften einer Überarbeitung, da sie insbesondere mit Blick auf die Umsetzung der Richtlinie (EU) 2016/680 und der Umsetzung des vorbenannten Urteils des Bundesverfassungsgerichtes zum Bundeskriminalamtgesetz vom 20. April 2016 differenzierter und umfassender auszugestalten sind. Dies erfolgt mit den §§ 39 ff.

§ 39 bestimmt nun zunächst die Grundsätze, die für jede Datenübermittlung gelten.

Absatz 1 dient der Umsetzung von Artikel 7 Absatz 2 der Richtlinie (EU) 2016/680. Im Hinblick auf die Vervollständigung unvollständiger Daten als möglichen Sinn und Zweck einer Datenübermittlung wird die in der Richtlinie (EU) 2016/680 enthaltene Vermeidung der Übermittlung „unvollständiger“ Daten nicht übernommen.

Ferner ist bei der Anwendung und Auslegung der Anforderungen des § 39 zu beachten, dass sich die Frage nach der „Aktualität“ von Daten und der damit verbundenen Vorgabe, keine „nicht mehr aktuellen“ Daten zu übermitteln beziehungsweise bereitzustellen, stets nur im konkreten Ermittlungszusammenhang und unter Beachtung des konkreten Verarbeitungszwecks beantworten lässt. In bestimmten Ermittlungszusammenhängen kann auch die Übermittlung nicht (mehr) aktueller Daten wie alte Meldeadressen oder alte (Geburts-)Namen bedeutsam und für die Aufgabenerfüllung erforderlich sein.

Absatz 2 wiederum setzt Artikel 9 Absatz 3 der Richtlinie (EU) 2016/680 um. Beispiele für die vorgesehene Mitgabe besonderer Bedingungen können Zweckbindungsregelungen bei der Weiterverarbeitung durch den Empfänger, das Verbot der Weiterübermittlung ohne Genehmigung oder Konsultationserfordernisse vor der Beauskunftung betroffener Personen durch den Empfänger sein.

Absatz 3 setzt Artikel 9 Absatz 4 der Richtlinie (EU) 2016/680 um.

§ 39a (Datenübermittlungsverbote und Verweigerungsgründe)

In § 39a werden die Übermittlungsverbote und Verweigerungsgründe in einer Zentralnorm zusammengefasst, neu systematisiert und zur Umsetzung der Vorgaben des Bundesverfassungsgerichtes in seinem Urteil vom 20. April 2016 zum Bundeskriminalamtgesetz ergänzt. Die Regelung orientiert sich weitgehend an § 28 des Bundeskriminalamtgesetzes.

Absatz 1 entspricht § 28 Absatz 1 des Bundeskriminalamtgesetzes. Die in ihm genannten Gründe, die einer Übermittlung im Wege stehen, gelten für Übermittlungen ins Inland, an Stellen in Mitgliedstaaten der Europäischen Union und in Drittstaaten. Bei den Änderungen handelt es sich um redaktionelle Änderungen.

Bei der nach Absatz 1 Satz 1 Nummer 1 vorzunehmenden Güterabwägung sind vor allem die Sensibilität der betreffenden Daten sowie die Art ihrer Erhebung und die damit verbundene Intensität des Eingriffs in das Persönlichkeitsrecht der betroffenen Person zu berücksichtigen.

Satz 1 Nummer 2 soll zum einen das Verhältnis der Übermittlungsregelungen dieses Gesetzes zu besonderen gesetzlichen Verwendungsregelungen klarstellen. Unter letztere fallen Übermittlungsverbote, zu denen auch Berufs- und besondere Amtsgeheimnisse zählen, sowie spezielle, abschließende Zweckbindungsregelungen.
Darunter sind Regelungen zu verstehen, aus denen sich ergibt, dass eine Verwendung nur für die im Gesetz geregelten Zwecke und unter den im Gesetz geregelten Voraussetzungen zulässig ist. Zugleich stellt Nummer 2 ausdrücklich fest, dass auch gesetzlich nicht geregelte Geheimhaltungspflichten von den Übermittlungsregelungen dieses Gesetzes unberührt bleiben.

Satz 2 enthält eine Privilegierung der Staatsanwaltschaften hinsichtlich der grundsätzlich nach Satz 1 Nummer 1 vorzunehmenden Güterabwägung.

Absatz 2 entspricht im Wesentlichen § 28 Absatz 2 des Bundeskriminalamtgesetzes und nimmt in Ergänzung des Absatzes 1 weitere Übermittlungsverbote für die Datenübermittlung an Stellen in Mitgliedstaaten der Europäischen Union und im internationalen Ausland auf. Um den Anforderungen des Bundesverfassungsgerichtes in der vorbenannten Entscheidung unter der Randnummer 328 gerecht zu werden, wird die drohende Verletzung von elementaren Rechtsstaatsgrundsätzen und Menschenrechten explizit genannt.

Der Absatz 3 trägt den vom Bundesverfassungsgericht in der vorbenannten Entscheidung vom 20. April 2016 aufgestellten Anforderungen an die Vergewisserung der übermittelnden Stellen über das Vorhandensein eines datenschutzrechtlich angemessenen und mit elementaren Menschenrechtsgewährleistungen zu vereinbarenden Umgangs mit den übermittelten Daten im Empfängerstaat Rechnung. Das Bundesverfassungsgericht führt unter der Randnummer 339 dieser Entscheidung aus:

„Die Vergewisserung über das geforderte Schutzniveau - sei es generalisiert, sei es im Einzelfall - ist eine nicht der freien politischen Disposition unterliegende Entscheidung deutscher Stellen. Sie hat sich auf gehaltvolle wie realitätsbezogene Informationen zu stützen und muss regelmäßig aktualisiert werden. Ihre Gründe müssen nachvollziehbar dokumentiert werden. Die Entscheidung muss durch die Datenschutzbeauftragten überprüfbar sein und einer gerichtlichen Kontrolle zugeführt werden können.“

§ 28 Absatz 3 des Bundeskriminalamtgesetzes, auf den Absatz 3 verweist, verpflichtet das Bundeskriminalamt, für den polizeilichen Informationsaustausch und Rechtshilfeverkehr eine Aufstellung über die Einhaltung der elementaren rechtsstaatlichen Grundsätze und Menschenrechtsstandards sowie das Datenschutzniveau in den jeweiligen Drittstaaten zu erstellen. Hierbei hat das Bundeskriminalamt insbesondere die jeweiligen Erkenntnisse der Bundesregierung und die Angemessenheitsbeschlüsse der Europäischen Kommission gemäß Artikel 36 der oben genannten Richtlinie zu berücksichtigen. Diese Aufstellung ist regelmäßig zu aktualisieren. Aus Gründen der Praktikabilität und Verwaltungsökonomie haben die Sicherheitsbehörden die Aufstellung bei der Beurteilung von Ausschluss- und Verweigerungsgründen zu beachten.

§ 39b (Datenübermittlung im innerstaatlichen Bereich)

Der neue § 39b systematisiert die bislang in den §§ 39 bis 41 enthaltenen Vorschriften zur innerstaatlichen Datenübermittlung neu. Die Vorschrift orientiert sich in Teilen an § 25 des Bundeskriminalamtgesetzes und dient gleichzeitig der Umsetzung des Urteils des Bundesverfassungsgerichtes zum Bundeskriminalamtgesetz vom 20. April 2016 (Aktenzeichen 1 BvR 966/09). Unter den Randnummern 276 f des genannten Urteils hat das Gericht ausgeführt, dass sich auch die Anforderungen an die Übermittlung staatlich erhobener Daten an den Grundsätzen der Zweckbindung und Zweckänderung ausrichten müssen und damit dem Grundsatz der hypothetischen Datenneuerhebung unterliegen.

Absatz 1 greift die bisherige Regelungslage in § 40 Absatz 1 Satz 1 und Absatz 2 auf. Er entspricht weitgehend § 25 Absatz 1 des Bundeskriminalamtgesetzes. Die Änderung dient der Umsetzung der vom Bundesverfassungsgericht im vorgenannten Urteil aufgestellten Anforderungen des Grundsatzes der hypothetischen Datenneuerhebung an die Datenübermittlung im innerstaatlichen Bereich.

In Satz 2 wird die bisherige Regelung aus § 40 Absatz 1 Satz 3 insoweit übernommen, als personenbezogene Daten von Personen nach § 27 Absatz 3 Nummer 2 bis 4 nur an Polizeidienststellen übermittelt werden dürfen. Da die verantwortliche Stelle nach § 25a Absatz 2 bei der Datenverarbeitung zwischen verschiedenen Kategorien personenbezogener Daten zu unterscheiden hat und gerade die Daten von den in § 27 Absatz 3 genannten Personen verpflichtend jeweils als Kategorie zu unterscheiden sind, wird sichergestellt, dass die Regelung in Satz 2 in der Praxis umgesetzt werden kann. Eine Übermittlung von personenbezogenen Daten über Personen nach § 27 Absatz 3 Nummer 1 ist damit vor dem Hintergrund, dass entsprechende Erkenntnisse zur Aufgabenerfüllung der Ordnungsbehörden zum Beispiel im Rahmen von Entscheidungen über den Widerruf einer waffenrechtlichen Erlaubnis erforderlich sein können, gestattet.

In Absatz 2 wird auf die Möglichkeit der Einrichtung automatisierter Verfahren nach § 42 verwiesen, was bislang in § 40 Absatz 3 geregelt war.

Absatz 3 regelt die Datenübermittlung an Behörden und sonstige öffentliche Stellen, die nicht in Absatz 1 genannt sind.

Satz 1 entspricht weitgehend § 25 Absatz 2 des Bundeskriminalamtgesetzes und wird an die im SOG M-V geregelten Aufgabenbereiche angepasst. Gleichzeitig setzt er den Grundsatz der hypothetischen Datenneuerhebung für die Übermittlungen an öffentliche Stellen, die keine polizeilichen oder ordnungsbehördlichen Aufgaben wahrnehmen, um.

In seinem vorbenannten Urteil vom 20. April 2016 führt das Bundesverfassungsgericht unter der Randnummer 287 aus, dass, „*die Tatsache, dass die Zielbehörde bestimmte Datenerhebungen, zu denen die Ausgangsbehörde berechtigt ist, ihrerseits wegen ihres Aufgabenspektrums nicht vornehmen darf, einem Datenaustausch nicht prinzipiell“* entgegensteht. Entscheidend für eine Datenübermittlung an sonstige öffentliche Stellen ist demnach, dass neben konkreten Ermittlungsansätzen für die Aufdeckung von Straftaten oder Gefahren für Rechtsgüter zugleich auch Erkenntnisse zu einer Gefährdung von mindestens gleichwertigen Rechtsgütern vorliegen, die zur Erfüllung der Aufgabe der jeweiligen Behörde bedeutsam sein können.

In Satz 2, der im Wesentlichen der bisherigen Regelung des § 39 Absatz 1 Satz 2 entspricht, wird klargestellt, dass persönliche Einschätzungen oder Beurteilungen sowie gespeicherte personenbezogene Daten über Personen nach § 27 Absatz 3 Nummer 2 bis 4 nicht übermittelt werden dürfen. Eine Übermittlung von Daten über Personen nach § 27 Absatz 3 Nummer 1 ist damit grundsätzlich gestattet, denn entsprechende Erkenntnisse können auch zur Aufgabenerfüllung der betreffenden Behörden oder öffentlichen Stellen, zum Beispiel Schulen, erforderlich sein.

In Satz 4 wird die bisherige Regelung des § 41 Absatz 5 übernommen, wonach sich die Datenübermittlung zwischen der Verfassungsschutzbehörde und den Ordnungsbehörden oder der Landespolizei weiterhin nach den Vorschriften des Landesverfassungsschutzgesetzes regelt.

Absatz 4 bestimmt die Voraussetzungen für eine Datenübermittlung an nicht-öffentliche Stellen. Die Regelung orientiert sich an § 25 Absatz 3 und 4 des Bundeskriminalamtgesetzes und wird an die im SOG M-V geregelten Aufgabenbereiche angepasst. In Satz 2 wird die bisherige Regelung in § 41 Absatz 4 zum Unterbleiben einer Übermittlung weitgehend übernommen. Satz 3 betrifft die Konstellation, dass die betroffenen personenbezogenen Daten von einer anderen Stelle stammen. Liegen Anhaltspunkte vor, dass durch die Übermittlung an eine nichtöffentliche Stelle die ursprünglichen Zwecke der Datenerhebung gefährdet sein könnten, muss vor einer erneuten Übermittlung die Zustimmung der vormals übermittelnden Stelle eingeholt werden. Gleiches gilt, wenn die übermittelnde Stelle der empfangenden Stelle den Hinweis erteilt hat, dass ihre Zustimmung vor einer Übermittlung an nichtöffentliche Stellen einzuholen ist.

Absatz 5 regelt die Zweckbindung und Verarbeitung der übermittelten Daten durch die empfangende Stelle. Dabei ist die Hinweispflicht in § 39 Absatz 2 zu beachten. Der bisherige § 39 Absatz 5 wird an die vom Bundesverfassungsgericht in seinem oben genannten Urteil vom 20. April 2016 aufgestellten Anforderungen des Grundsatzes der hypothetischen Datenneuerhebung an die weitere Verarbeitung der Daten durch die empfangende Stelle angepasst. Auch die empfangende Stelle hat zukünftig die Voraussetzungen des Grundsatzes der hypothetischen Datenneuerhebung zu berücksichtigen, wenn sie die übermittelten Daten zu anderen Zwecken, als zu denen die Daten übermittelt wurden, verarbeiten will.

In Absatz 6 wird die bisherige Regelung in § 39 Absatz 3 an die Änderungen in den vorherigen Regelungen angepasst. Das Gefüge der Verantwortlichkeit für die Zulässigkeit der Übermittlung bleibt dabei erhalten.

Absatz 7 entspricht der Regelung des § 25 Absatz 8 des Bundeskriminalamtgesetzes und nimmt hinsichtlich eines Dritten Bezug auf die in § 3 Absatz 4 Nummer 2 enthaltene Definition.

§ 39c (Übermittlung an Mitgliedstaaten und Organisationen der Europäischen Union)

Der neue § 39c regelt die Datenübermittlung an Mitgliedstaaten und Organisationen der Europäischen Union und stellt sie mit den Datenübermittlungen im Inland gleich. Durch den Verweis auf die Regelungen des § 39b, mit Ausnahme des § 39b Absatz 6, gilt der in § 36 verankerte Grundsatz der hypothetischen Datenneuerhebung auch für die innereuropäische Datenübermittlung. Die Norm entspricht weitgehend § 26 des Bundeskriminalamtgesetzes und wird an die im SOG M-V geregelten Aufgabenbereiche angepasst. Die Ausnahme des § 39b Absatz 6 erfolgt vor dem Hintergrund, dass nach § 39c Absatz 2 die Verantwortlichkeit für die Datenübermittlung in jedem Fall bei der übermittelnden Stelle liegen soll.

Ein effektiver und wirksamer Informationsaustausch zwischen den Sicherheitsbehörden der Mitgliedstaaten der Europäischen Union ist ein Schlüsselelement für die Gewährleistung der Sicherheit der Bundesrepublik Deutschland und der Europäischen Union. Nur durch die intensive grenzübergreifende Zusammenarbeit der europäischen Sicherheitsbehörden bei der Gefahrenabwehr und der Straftatenverhütung und -verfolgung können europaweit insbesondere terroristische Anschläge und Straftaten verhindert, aufgedeckt und verfolgt werden.

Vor diesem Hintergrund und der sich stetig vertiefenden europäischen Integration, welche die Europäische Union zu einem gemeinsamen Raum der Freiheit, der Sicherheit und des Rechts gemacht hat, setzt § 39c Absatz 1 den Gleichbehandlungsgrundsatz konsequent um und stellt künftig Datenübermittlung an Mitgliedstaaten der Europäischen Union den innerstaatlichen Datenübermittlungen gleich. Die bisher im SOG M-V in § 40 Absatz 3 und § 41 Absatz 3 undifferenzierte Regelung für ausländische Stellen kann mit Blick auf die bezüglich der Datenübermittlung an Drittstaaten restriktiven Vorgaben der Artikel 35 bis 40 Richtlinie (EU) 2016/680 und Artikel 44 bis 50 Verordnung (EU) 2016/679 nicht bestehen bleiben.

Durch Absatz 1 Satz 1 Nummer 1 wird die Übermittlung an Behörden, sonstige öffentliche und nicht öffentliche Stellen anderer Mitgliedstaaten der Europäischen Union den Regelungen über Übermittlung an innerstaatliche Stellen gleichgestellt. Über Satz 1 Nummer 2 wird klargestellt, dass sich auch Datenübermittlungen an zwischen- und überstaatliche Stellen der Europäischen Union oder deren Mitgliedstaaten, die mit Aufgaben entsprechend denen des SOG M-V befasst sind, nach den Regelungen über die Übermittlung an Polizei- und Ordnungsbehörden der Mitgliedstaaten richten. Dies betrifft die nach Kapitel 4 und 5 des V. Titels des dritten Teils des Vertrags über die Arbeitsweise der Europäischen Union errichteten Einrichtungen und sonstigen Stellen, so etwa Europol.

Den Regelfall von Übermittlungen nach Satz 1 Nummer 1 stellen Übermittlungen an Polizeibehörden oder sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stelle eines Mitgliedstaates der Europäischen Union dar. Als solche können insbesondere jene Stellen gelten, die von diesem Staat gemäß Artikel 2 Buchstabe a des Rahmenbeschlusses 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (ABl. L 386 vom 29.12.2006, S. 89, L 75 vom 15. März 2007, S. 26) benannt wurden.

§ 39d (Datenübermittlung in Drittstaaten im Anwendungsbereich der Richtlinie (EU) 2016/680)

§ 39d regelt die Datenübermittlung im internationalen Bereich über den der Übermittlung an Mitgliedstaaten der Europäischen Union hinaus. Die §§ 39d bis 39h orientieren sich an § 27 des Bundeskriminalamtgesetzes sowie den §§ 78 bis 81 des Bundesdatenschutzgesetzes mit entsprechenden Anpassungen für die nach dem SOG M-V geregelten Aufgabenbereiche.

Mit den genannten Normen werden an dieser Stelle lediglich die Artikel 35 bis 39 der Richtlinie (EU) 2016/680 umgesetzt, da eine einheitliche Regelung für den gesamten Aufgabenbereich des SOG M-V durch eine Präzisierung der Regelungen in den Artikeln 44 bis 49 der Verordnung (EU) 2016/679 nicht möglich ist. Soweit die Datenübermittlung außerhalb des Anwendungsbereichs der Richtlinie (EU) 2016/680 erfolgt, richtet sich diese somit direkt nach den Vorgaben der Artikel 44 bis 49 der Verordnung (EU) 2016/679. Für die Praxis wird dies keine nachteiligen Auswirkungen haben, da eine Übermittlung an Stellen außerhalb der Mitgliedstaaten der Europäischen Union in der Regel zu Zwecken der Richtlinie erfolgt, sodass die nach dem SOG M-V zuständigen Behörden in den übrigen Fällen auf die Vorschriften der Verordnung verwiesen werden können.

Die §§ 39a und 39d sind hinsichtlich der Übermittlungsverbote und Verweigerungsgründe (§ 39a) und der positiv formulierten Übermittlungsbefugnisse (§ 39d) im Zusammenhang mit den Übermittlungsvorschriften in den §§ 39e bis 39h zu lesen. Das gilt insbesondere für die in § 39h enthaltene, die Rechtslage an die Praxis des polizeilichen Informationsaustausches anpassende Befugnis zur Übermittlung personenbezogener Daten, insbesondere in Form von Ersuchen um Beauskunftung an nicht für die Verhütung und Verfolgung von Straftaten zuständige öffentliche und auch nicht-öffentliche Stellen in Drittstaaten. Damit wird gewährleistet, dass insbesondere die Polizei ihre Ersuchen direkt an eine andere Behörde oder eine nichtöffentliche Stelle richten kann. Dies betrifft beispielsweise Ersuchen an große Internetdienstleister mit zentraler Datenhaltung im Ausland.

Absatz 1 entspricht weitgehend dem § 27 Absatz 1 des Bundeskriminalamtgesetzes.
Satz 1 bestimmt die Datenübermittlung in Drittstaaten im Anwendungsbereich der Richtlinie (EU) 2016/680 unter Beachtung des § 36 Absatz 2 bis 4, der §§ 39 und 39a sowie der §§ 39e bis 39g. Die Bezugnahme auf § 36, dort die Absätze 2 bis 4, dient einerseits der Umsetzung der vom Bundesverfassungsgericht in seinem vorbenannten Urteil vom 20. April 2016 aufgestellten Anforderungen des Grundsatzes der hypothetischen Datenneuerhebung an die Übermittlung von Daten aus besonders eingriffsintensiven Maßnahmen im internationalen Bereich. Das Bundesverfassungsgericht hat unter den Randnummern 343 und 344 ausgeführt:

„§ 14 Abs. 1 Satz 1 Nummer 1 BKAG genügt, soweit er als eigene Ermächtigungsgrundlage zu verstehen ist (vgl. Graulich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2014, § 14 BKAG, Rn. 6), den verfassungsrechtlichen Anforderungen an eine Zweckänderung nicht. Indem er dem Bundeskriminalamt eine Datenübermittlung allgemein zur Erfüllung der ihm obliegenden Aufgaben erlaubt, fehlt es an Maßgaben, die sicherstellen, dass Daten aus eingriffsintensiven Überwachungsmaßnahmen nur für Zwecke übermittelt werden dürfen, die dem Kriterium der hypothetischen Datenneuerhebung entsprechen. (...) Gleichfalls zu weit und deshalb mit den verfassungsrechtlichen Anforderungen nicht vereinbar ist § 14 Abs. 1 Satz 1 Nummer 3 BKAG in Bezug auf Daten aus Wohnraumüberwachungen. Nach den oben entwickelten Maßgaben ist für diese sicherzustellen, dass sie nur bei Vorliegen einer dringenden Gefahr übermittelt werden dürfen (siehe oben D I 2 b bb; vgl. ferner BVerfGE 109, 279 <377, 379>). Eine solche Begrenzung enthält die Vorschrift nicht.“

Durch den Verweis auf die Absätze 2 bis 4 des § 36 werden diese Anforderungen erfüllt. Andererseits erfolgt ein Hinweis auf die Geltung der in den §§ 39e bis 39g vorgesehenen Drittstaatenübermittlungsvorschriften.

In Nummer 1 wird auf die spezifischen Aufgaben nach dem SOG M-V verwiesen, die in den Regelungsbereich der Richtlinie (EU) 2016/680 fallen.

In Nummer 2 wird im Weiteren auf die in § 39g Absatz 1 Satz 1 Nummer 1 bis 3 und 5 verwiesen. Eine entsprechende Datenübermittlung ist auch zu diesen Zwecken im Einzelfall zulässig, da eine solche nach Artikel 38 Absatz 1 Richtlinie (EU) 2016/680 bereits ohne das Vorliegen eines Angemessenheitsbeschlusses nach Artikel 36 oder geeigneter Garantien nach Artikel 37 zu gestatten ist, im Umkehrschluss also erst recht bei Vorliegen der übrigen Voraussetzungen des Absatzes 1 erfolgen darf.

Mit Satz 2 wird geregelt, dass § 39b Absatz 1 Satz 2, der bestimmt, dass über Personen nach § 27 Absatz 3 Nummer 2 bis 4 gespeicherte personenbezogene Daten nur an andere Polizeidienststellen übermittelt werden dürfen, entsprechend gilt.

Absatz 2 entspricht weitgehend dem § 27 Absatz 7 des Bundeskriminalamtgesetzes. Mit Blick auf die geregelte Verwendungsbeschränkung wird insbesondere darauf hingewiesen, dass der Empfänger nach § 39 Absatz 2 auf diese besondere Verarbeitungsbedingung hinzuweisen ist.

Es ist zudem besonders auf § 48h hinzuweisen, nach dem Datenübermittlungen an Drittstaaten und weitere zwischen- und überstaatliche Stellen nach den §§ 39d bis 39h auch einer Berichtspflicht unterliegen (siehe § 48h Absatz 1 Satz 1 Nummer 7).

§ 39e (Grundsätze der Datenübermittlung in Drittstaaten im Anwendungsbereich der Richtlinie (EU) 2016/680)

§ 39e dient der Umsetzung von Artikel 35 der Richtlinie (EU) 2016/680 und statuiert Voraussetzungen, die bei jeder Datenübermittlung an Stellen in Drittstaaten oder an internationale Organisationen vorliegen müssen. Er entspricht in angepasster Form der Regelung des § 78 des Bundesdatenschutzgesetzes.

Darüber hinaus enthält die Vorschrift zusätzliche Anforderungen an die Datenübermittlung an Stellen in Drittstaaten oder an internationale Organisationen - auch an die insbesondere nach den §§ 39e bis 39h erforderliche Abwägungsentscheidung - aufgrund der Rechtsprechung des Bundesverfassungsgerichtes. Dieses hat in seinem vorbenannten Urteil vom 20. April 2016 unter den Randnummern 335 und 338 ausgeführt:

„Erlaubt ist eine Übermittlung der Daten ins Ausland jedoch nur, wenn auch durch den dortigen Umgang mit den übermittelten Daten nicht die Garantien des menschenrechtlichen Schutzes personenbezogener Daten unterlaufen werden. Dies bedeutet nicht, dass in der ausländischen Rechtsordnung institutionelle und verfahrensrechtliche Vorkehrungen nach deutschem Vorbild gewährleistet sein müssen; insbesondere müssen nicht die formellen und institutionellen Sicherungen vorhanden sein, die datenschutzrechtlich für deutsche Stellen gefordert werden (siehe oben C IV 6). Geboten ist in diesem Sinne die Gewährleistung eines angemessenen materiellen datenschutzrechtlichen Niveaus für den Umgang mit den übermittelten Daten im Empfängerstaat […] Erforderlichenfalls können und müssen verbindliche Einzelgarantien abgegeben werden.“

In besonderer Ausprägung dessen fordert Absatz 2 ein Unterbleiben der Übermittlung, wenn im Einzelfall Anlass zur Besorgnis besteht und diese Besorgnis auch nach einer Prüfung durch die übermittelnde Stelle weiter besteht, dass ein elementaren rechtsstaatlichen Grundsätzen genügender Umgang mit den übermittelten Daten nicht gesichert ist. Hierbei ist besonders zu berücksichtigen, wenn der Empfänger einen angemessenen Schutz der Daten garantiert.

§ 39f (Datenübermittlung in Drittstaaten bei geeigneten Garantien im Anwendungsbereich der Richtlinie (EU) 2016/680)

In § 39f werden Regelungen zur Datenübermittlung an Drittstaaten bei geeigneten Garantien übernommen. Die Norm entspricht weitgehend § 79 des Bundesdatenschutzgesetzes und sie dient der Umsetzung von Artikel 37 der Richtlinie (EU) 2016/680.

In der Vorschrift werden ergänzende Voraussetzungen für Datenübermittlungen an Stellen in Drittstaaten, zu denen die Europäische Kommission keinen Angemessenheitsbeschluss gemäß Artikel 36 gefasst hat, formuliert. Bei solchen Konstellationen kommt der übermittelnden Stelle - insbesondere nach § 39f Absatz 1 Nummer 2 - die Aufgabe zu, das Vorliegen geeigneter Garantien für den Schutz personenbezogener Daten beim Empfänger zu beurteilen. Nach einer solchen Beurteilung kann die Datenübermittlung etwa mit der Mitgabe von Verarbeitungsbedingungen - zum Beispiel Löschverpflichtungen nach Zweckerreichung, Weiterübermittlungsverbote, Zweckbindungen - verbunden werden, die dazu geeignet sind, diese Beurteilung zu dokumentieren und ihr Ergebnis zu sichern. Im Zusammenhang mit dem auch hier anwendbaren § 39e Absatz 2 entfaltet der dort erwähnte Gesichtspunkt der Einzelfallgarantie des Empfängerstaates bei der Prüfung des Vorhandenseins geeigneter Garantien besondere Bedeutung.

Die Umsetzung von Artikel 37 Absatz 3 der Richtlinie (EU) 2016/680 zur Dokumentation der Übermittlungen nach § 39f wird in § 46d geregelt.

Der Umsetzung von Artikel 37 Absatz 2 und 3 der Richtlinie (EU) 2016/680 dient Absatz 2, der die Unterrichtung der oder des Landesbeauftragten für den Datenschutz regelt, wenn aufgrund einer Beurteilung ohne das Vorliegen eines Angemessenheitsbeschlusses der Kommission, aber wegen des Bestehens geeigneter Garantien für den Schutz personenbezogener Daten im Drittstaat eine Übermittlung erfolgt ist. Die Gründe für die Beurteilung sind zu dokumentieren und zusammen mit den nach § 46d zu erstellenden Dokumentationen der oder dem Landesbeauftragten für den Datenschutz auf Anforderung zu übermitteln.

§ 39g (Datenübermittlung in Drittstaaten ohne Garantien im Anwendungsbereich der Richtlinie (EU) 2016/680)

In § 39g werden Regelungen zur Datenübermittlung an Drittstaaten ohne Garantien übernommen. Die Norm entspricht weitgehend der Regelung des § 80 des Bundesdatenschutzgesetzes und setzt Artikel 38 der Richtlinie (EU) 2016/680 um.

§ 39g bestimmt die Übermittlungskonstellationen, in denen weder ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, noch die in § 39f erwähnten Garantien in Form eines rechtsverbindlichen Instruments oder nach Beurteilung durch die übermittelnde verantwortliche Stelle bestehen.

Die in § 80 Absatz 3 des Bundesdatenschutzgesetzes vorgesehene Dokumentationspflicht ist über § 46d erfasst.

§ 39h (Sonstige Datenübermittlung an Empfänger in Drittstaaten im Anwendungsbereich der Richtlinie (EU) 2016/680)

§ 39h dient der Umsetzung von Artikel 39 der Richtlinie (EU) 2016/680 und entspricht weitgehend der Regelung des § 81 des Bundesdatenschutzgesetzes.

Die hier geregelte Konstellation zeichnet sich dadurch aus, dass der Kreis der möglichen Empfänger über öffentliche Stellen, die im Rahmen der Strafverfolgung tätig sind, hinaus auf sonstige öffentliche Stellen und Private ausgeweitet wird. Abgebildet werden etwa unmittelbare Ersuchen an Finanzinstitutionen oder Telekommunikationsdienstleister, die notwendigerweise mit der Übermittlung personenbezogener Daten verbunden sind. Für solche Übermittlungen „im besonderen Einzelfall“ sind zusätzlich zu den übrigen für die Datenübermittlung in Drittstaaten geltenden Voraussetzungen (siehe § 39d ff) die hier in § 39h Absatz 1 normierten Voraussetzungen zu beachten. Darüber hinaus wird in Absatz 1 Satz 2 bestimmt, dass § 39b Absatz 3 Satz 2, der bestimmt, dass gespeicherte personenbezogene Daten über Personen nach § 27 Absatz 3 Nummer 2 bis 4, einschließlich der persönlichen Einschätzungen oder Beurteilungen, nicht übermittelt werden dürfen, entsprechend gilt. Absatz 2 und 3 regeln notwendige Unterrichtungspflichten und in Absatz 4 wird eine zu der in § 39d Absatz 2 geregelten Zweckbindung verstärkte Hinweispflicht in Form einer Verpflichtung zu den gemäß § 39h übermittelten Daten vorgesehen.

Es ist zudem besonders darauf hinzuweisen, dass insbesondere die Dokumentationspflichten nach § 46d zu beachten sind.

§ 40 (Datenübermittlung zum Zwecke der Zuverlässigkeitsüberprüfung)

Die Bestimmung ermächtigt die Polizei zur Datenübermittlung an öffentliche oder nichtöffentliche Stellen im Zusammenhang mit der Durchführung sogenannter „Akkreditierungsverfahren“ bei Veranstaltungen, bei denen eine besondere Gefahr entstehen kann. In der Praxis kann es insbesondere bei Großveranstaltungen wie Fußballspielen oder anderen Veranstaltungen, die im besonderen Fokus der Öffentlichkeit stehen, notwendig sein, dass der Veranstalter einzusetzendes Sicherheitspersonal auf seine Zuverlässigkeit überprüfen muss, um die Sicherheit der Veranstaltung zu gewährleisten. Hierzu ist er auf die bei der Polizei gegebenenfalls vorhandenen Erkenntnisse angewiesen.

Bereits mit der Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurde kritisiert, dass die Zuverlässigkeitsüberprüfungen bei Großveranstaltungen und die damit erfolgenden Datenübermittlungen der Polizei an Personen oder Stellen außerhalb des öffentlichen Bereichs ohne spezielle gesetzliche Rechtsgrundlage durchgeführt und lediglich auf informierte Einwilligungen der hiervon betroffenen Personen gestützt werden. Denn Betroffene müssten oft Nachteile zum Beispiel beim Arbeitgeber befürchten, wenn sie die Einwilligung verweigern und insoweit fehle es faktisch an einer echten Freiwilligkeit. Die Datenschutzbeauftragten forderten seinerzeit daher eine spezielle gesetzliche Regelung für Zuverlässigkeitsüberprüfungen. Der 8. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern enthielt diese Forderung ebenfalls.

Zur Schaffung von Rechtssicherheit für die Polizei soll nunmehr eine konkrete Regelung ins Gesetz aufgenommen werden (dazu auch Petri in Lisken/Denninger, Handbuch des Polizeirechts, 6. Auflage, 2018, Randnummer G 982). Unter anderem verfügen die Länder
- Berlin (§ 45a Allgemeines Sicherheits- und Ordnungsgesetz),
- Hamburg (§ 21 Gesetz über die Datenverarbeitung der Polizei),
- Hessen (§§ 13a, b Hessisches Gesetz über die öffentliche Sicherheit und Ordnung), - Sachsen (§ 44 Polizeigesetz des Freistaates Sachsen) und
- Thüringen (§ 41a Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei)

bereits über eine solche Rechtsvorschrift (Stand Mai 2018).

Die Datenübermittlung nach Absatz 1 setzt die vorherige schriftliche Einwilligung der betroffenen Person nach § 26 voraus. Insbesondere bei Großveranstaltungen muss bereits mit einem erheblichen zeitlichen Vorlauf über die Frage der Durchführung von Zuverlässigkeitsüberprüfungen entschieden werden. Deswegen ist unter einer „besonderen Gefahrlage’“ eine abstrakt-generelle Gefahr zu verstehen. Hierfür reicht nicht jede Gefahr, vielmehr muss sich die Besonderheit der Gefahr aus den Umständen der jeweiligen Veranstaltung ableiten lassen. Die Frage der Erforderlichkeit von Zuverlässigkeitsüberprüfungen ist jeweils im Einzelfall anhand der jeweiligen Veranstaltung zu beantworten, wobei besondere Umstände, zum Beispiel ob die betroffene Person Zugang zu bestimmten Bereichen der Veranstaltung hat, einzubeziehen sind. Satz 2 stellt klar, dass sich die Übermittlung gegenüber nichtöffentlichen Stellen inhaltlich auf die ausschließliche Aussage beschränkt, ob aus polizeilicher Sicht Sicherheitsbedenken bestehen oder nicht. Weitergehende Informationen dürfen an die privaten Veranstalter nicht übermittelt werden.

Absatz 2 regelt die Pflicht der Polizei, den Empfänger, insbesondere eine private Person, schriftlich zu verpflichten, die Zweckbindung einzuhalten und die Daten spätestens nach der Veranstaltung zu löschen. Die betroffene Person ist zu unterrichten, soweit dies nicht bereits auf andere Weise, zum Beispiel durch den Arbeitgeber, sichergestellt ist.

Absatz 3 stellt klar, dass die Vorschriften des Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen im Land Mecklenburg-Vorpommern unberührt bleiben.

§ 41 (Bekanntgabe an die Öffentlichkeit)

§ 41 entspricht dem bisher geltenden § 41 Absatz 2 und reiht sich nunmehr in die neu gestalteten Übermittlungsvorschriften ein.

Ergänzt wird ausschließlich die Nummer 2 um die terroristische Straftat nach § 67c.

§ 42 (Automatisierte Verfahren, Verfahrensbeschreibung)

§ 42 wird durch die Übernahme der bisher in § 47 enthaltenen Regelungen sowie aufgrund des Wegfalls der §§ 17 bis 19 des Landesdatenschutzgesetzes (in der vor dem 25. Mai 2018 geltenden Fassung) zu einer umfassenden Vorschrift über automatisierte Verfahren sowie Verfahrensbeschreibungen ergänzt.

Absatz 1 entspricht im Wesentlichen dem bisher geltenden § 17 Absatz 1 Satz 1 und 2 des Landesdatenschutzgesetzes in der vor dem 25. Mai 2018 geltenden Fassung.

Absatz 2 Satz 1 übernimmt die ehemals in § 3 Absatz 8 bis 10 des Landesdatenschutzgesetzes (in der vor dem 25. Mai 2018 geltenden Fassung) enthaltenen Definitionen der Arten automatisierter Verfahren. Satz 2 verdeutlicht in Anlehnung an den bisher geltenden § 42 Satz 1, dass Abrufverfahren in der Praxis insbesondere zwischen Ordnungsbehörden, Polizeibehörden oder Ordnungs- und Polizeibehörden vereinbart werden können und Abrufverfahren mit anderen Stellen einer besonderen Rechtsvorschrift (siehe beispielsweise § 20a des Landesverfassungsschutzgesetzes) bedürfen. Satz 3 stellt klar, dass der Empfänger die Verantwortung für die Rechtmäßigkeit des Abrufs trägt. Satz 4 begrenzt entsprechend des bisher geltenden § 40 Absatz 3 Satz 1 die Befugnis zur Vereinbarung von Datenverbünden, die eine automatisierte Datenübermittlung zwischen Polizeidienststellen des Landes und Polizeidienststellen des Bundes und der Länder ermöglichen und die zur Erfüllung polizeilicher Aufgaben, die überörtliche Bedeutung haben, erforderlich sind, auf das Ministerium für Inneres und Europa als oberste Landesbehörde.

Der Absatz 3 dient der Umsetzung des Artikels 21 der Richtlinie (EU) 2016/680 und orientiert sich an § 63 des Bundesdatenschutzgesetzes. Im Regelungskontext mit den Vorgaben zur Vereinbarung zwischen verantwortlichen Stellen wird diese Norm so verstanden, dass eine öffentlich zugängliche Information zum wesentlichen Inhalt der Vereinbarung ähnlich der in Fällen einer Vorgabe durch Rechtsvorschrift erfolgen kann. In diesem Zusammenhang ist der Begriff „wesentlich“ aus der Perspektive der von der Datenverarbeitung betroffenen Person auszulegen.

Wesentlich sind somit nicht sämtliche Inhalte, die für die verantwortlichen Stellen im Rahmen ihrer Vereinbarung essentiell sind, sondern nur solche, die die betroffenen Personen grundsätzlich zur Geltendmachung ihrer Rechte benötigen und deren Kenntnis im Zusammenhang mit der Aufgabe der Gefahrenabwehr nicht zu einer wesentlichen Erschwerung der Aufgabenwahrnehmung durch die verantwortlichen Stellen führen.

Absatz 4 entspricht weitgehend dem ehemaligen § 18 des Landesdatenschutzgesetzes in der vor dem 25. Mai 2018 geltenden Fassung. Verfahrensbeschreibungen sind zwar weder in der Richtlinie (EU) 2016/680, noch der Verordnung (EU) 2016/679 vorgesehen, weshalb auch das neugefasste Landesdatenschutzgesetz keine Regelungen enthält. Gleichwohl stehen diese Regelwerke der Fortführung dieses bewährten und praxiserprobten Instruments keineswegs entgegen. Sie dienen seit jeher als wesentlicher Maßstab, um zu beurteilen, welchem Zweck gespeicherte Daten im Einzelfall dienen sollen und ob sie dafür erforderlich sind. Damit sind sie gleichzeitig wesentliche Grundlage für die Selbstkontrolle und für die Datenschutzkontrolle. Da bisher nicht festgestellt werden kann, dass dieser Regelungsinhalt anderweitig in vollem Umfang kompensiert werden kann, soll die Verfahrensbeschreibung aufgrund des Wegfalls des bisher geltenden § 18 des Landesdatenschutzgesetzes (in der vor dem 25. Mai 2018 geltenden Fassung) in dieses Gesetz übernommen werden. Sie ist zudem bestens als „Trägermedium“ für die in § 45b geregelte neue Datenschutz-Folgenabschätzung geeignet. Der bisher erforderliche Mindestinhalt der Verfahrensbeschreibung wird durch die Nummern 5 und 8 bis 10 ergänzt.

Satz 2 schreibt in Anlehnung an den bisher geltenden § 18 Absatz 2 Satz 1 des Landesdatenschutzgesetzes (in der vor dem 25. Mai 2018 geltenden Fassung) die fortlaufende Aktualisierung und die elektronische Form der Verfahrensbeschreibungen vor. So soll insbesondere gewährleistet werden, dass sie als Zuarbeit zum Verzeichnis der Verarbeitungstätigkeiten nach § 45c inhaltlich und formell genutzt werden können.

Absatz 5 schreibt aufgrund der neuen Stellung der oder des Landesbeauftragten für den Datenschutz ihre oder seine Beteiligung vor dem erstmaligen Einsatz beziehungsweise einer wesentlichen Änderung des Verfahrens vor. Damit wird gleichzeitig die Öffnungsklausel des Artikels 36 Absatz 5 der Verordnung (EU) 2016/679 genutzt.

Zur Gewährleistung der Vollständigkeit des Verzeichnisses der Verarbeitungstätigkeiten schreibt Absatz 6 die Aufnahme der Verfahrensbeschreibungen vor.

In der nach Absatz 7 zu fertigenden Verwaltungsvorschrift wird - wie bisher auch schon - zumindest für den Polizeibereich das künftige Verfahren samt der Verteilung von Zuständigkeiten (insbesondere hinsichtlich der Freigabe) zu regeln sein, da aufgrund der Vielzahl der polizeilichen automatisierten Verfahren in der Vergangenheit entsprechend viele Verfahrensbeschreibungen notwendig waren und auch zukünftig notwendig sein werden. Sie muss insbesondere die mit § 19 des Landesdatenschutzgesetzes (in der vor dem 25. Mai 2018 geltenden Fassung) weggefallenen Regelungen zur Freigabe abdecken. Die Freigabe hat jedenfalls schriftlich zu erfolgen.

Die derzeit geltende Verwaltungsvorschrift des Ministeriums für Inneres und Europa für den Polizeibereich wird aufgrund der datenschutzrechtlichen Neuregelungen anzupassen sein.

§ 43 (Datenabgleich)

Die Datenabgleichsbefugnis im bisher geltenden § 43 wird mit folgenden Anpassungen und Ergänzungen übernommen:

Da § 27 Absatz 3 Nummer 1 aufgrund der bundesverfassungsgerichtlichen Vorgaben im Urteil vom 20. April 2016 (Aktenzeichen 1 BvR 966/09) dahingehend eine Anpassung erfahren hat, dass die Kontakt- und Begleitpersonen aus der Nummer 1 herausgelöst und nun gesondert in § 27 Absatz 3 Nummer 2 enthalten sind (siehe hierzu ergänzend die Ausführungen zu § 27), ist Absatz 1 Satz 1 zu ändern. Der Verweis muss folglich auch auf § 27 Absatz 3 Nummer 2 erstreckt werden, damit der Datenabgleich - wie bisher auch - auf diesen Personenkreis erstreckt werden kann. Eine Ausweitung der Befugnis ist damit nicht verbunden.

Der bisher geltende Absatz 1 Satz 2 wird hinsichtlich der Voraussetzungen für einen Datenabgleich personenbezogener Daten von anderen als den in Satz 1 genannten Personen präziser ausgestaltet. Die Formulierung „dies zur Erfüllung polizeilicher Aufgaben erforderlich erscheint“ wird durch „dass dies zur Erfüllung polizeilicher Aufgaben erforderlich ist“ ersetzt. Der bisherige Satz 3 bleibt unverändert bestehen.

Neu aufgenommen wird mit Satz 4, dass die betroffene Person für die Dauer des Datenabgleichs angehalten werden darf. Die Aufnahme erfolgt zur Klarstellung und vor dem Hintergrund, dass in bereits bestehenden Normen ebenfalls das Anhalterecht gesondert normiert ist (vergleiche etwa §§ 28 Absatz 1, 29 Absatz 2). Das kurzzeitige Anhalten beinhaltet jedoch nicht auch das Mitnehmen zur Polizeidienststelle. Die Mitnahme der betroffenen Person etwa zum Zwecke der Identitätsfeststellung bestimmt sich nach den Voraussetzungen des § 29.

Der bisher geltende Satz 4 wird unter Vollzug der sprachlichen Gleichstellung der neue Satz 5.

Im Vergleich zu anderen Ländergesetzen, die keine ausschließlichen Polizeigesetze sind und ebenfalls Befugnisse der Ordnungsbehörden enthalten (vergleiche etwa § 37 des Polizei- und Ordnungsbehördengesetzes Rheinland-Pfalz, § 28 des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin, § 45 des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung, § 25 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung), existiert in § 43 bisher keine Datenabgleichsbefugnis für die Ordnungsbehörden. Mit Absatz 2 wird eine solche Befugnis neu in das Gesetz aufgenommen. Sie gibt den Ordnungsbehörden die Möglichkeit, personenbezogene Daten der in den §§ 69 und 70 genannten Personen (sogenannte Verhaltens- und Zustandsstörer) mit dem Inhalt anderer Dateisysteme, die von ihnen geführt werden, im Rahmen der Zweckbindung dieser Dateisysteme abzugleichen. Der Datenabgleich zu anderen Personen wird - vergleichbar der polizeilichen Befugnis in Absatz 1 Satz 2 - unter der Voraussetzung zugelassen, dass tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass der Datenabgleich zur Erfüllung der ordnungsbehördlichen Aufgaben nach dem SOG M-V erforderlich ist.

Der bisher geltende Absatz 2 wird als Absatz 3 übernommen.

§ 43a (Datenerhebung und Datenabgleich zur Erkennung von Kraftfahrzeugkennzeichen)

Die in § 43a normierte polizeiliche Befugnis zur Erkennung von Kraftfahrzeugkennzeichen wird mit folgenden Änderungen übernommen:

In § 43a Absatz 1 Satz 1 wird infolge der Aufnahme der gezielten Kontrolle in § 35 eine neue Nummer 4 und damit ein weiterer Anlass zum Einsatz technischer Mittel zur Erkennung von Kraftfahrzeugkennzeichen im Gesetz normiert. Die Maßnahme zur Erkennung von Kraftfahrzeugkennzeichen darf nur durchgeführt werden, wenn eine Person oder ein Fahrzeug zur gezielten Kontrolle ausgeschrieben wurde und Tatsachen die Annahme rechtfertigen, dass die für die Ausschreibung relevante Begehung von Straftaten in absehbarer Zeit mit hinreichender Wahrscheinlichkeit bevorsteht. Damit gelten auch hier die Voraussetzungen, die in Nummer 3 bereits im Zusammenhang mit einer Ausschreibung zur polizeilichen Beobachtung normiert sind. Auch in anderen Ländern ist die Maßnahme zur Erkennung von Kraftfahrzeugkennzeichen im Zusammenhang mit Ausschreibungen zur gezielten Kontrolle zugelassen (vergleiche etwa Artikel 36a des Brandenburgischen Polizeigesetzes oder auch Artikel 39 des Gesetzes über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei).

Die bisherigen Nummern 4 und 5 werden die Nummern 5 und 6, wobei in Nummer 5 neben den Straftaten von erheblicher Bedeutung nach § 49 auch ausdrücklich die terroristischen Straftaten nach § 67c aufgenommen werden.

In Satz 4 wird wegen des dort verwendeten Begriffes „Dritte“ ein Klammerzusatz mit dem Verweis auf die in § 3 Absatz 4 Nummer 2 aufgenommene Definition eingefügt.

Die bisher geltenden Absätze 2 und 3 werden unverändert übernommen.

Absatz 4 bedarf wegen der Einfügung der neuen Nummer 4 in Absatz 1 Satz 1 der Ergänzung. Satz 2, der das Anhalten des von einem Treffer betroffenen Fahrzeuges und die Information der fahrzeugführenden Person vorschreibt, wird auch auf die Nummer 4 erstreckt, da die Ausschreibung zur gezielten Kontrolle selbst unter anderem gerade auch das Durchsuchen bezweckt (vergleiche Ausführungen zu § 35) und damit ein Anhalten in einem Trefferfall erfordert. Die Sätze 4 bis 6 sind um den Fall des Absatzes 1 Satz 1 Nummer 4 zu ergänzen. Folglich dürfen die Daten gespeichert, polizeilich genutzt sowie zusammen mit den gewonnenen Erkenntnissen an die ausschreibende Stelle übermittelt werden. Sie dürfen zudem zu einem Bewegungsbild verbunden werden.

Der bisher geltende Absatz 5 wird unverändert übernommen.

Im Übrigen ist darauf hinzuweisen, dass schon der bisher geltende § 43a den Vorgaben des Bundesverfassungsgerichtes in seinen Entscheidungen vom 18. Dezember 2018 zur „Kfz-Kennzeichenkontrolle“ (Aktenzeichen 1 BvR 142/15 sowie Aktenzeichen 1 BvR 2795/09 und andere) gerecht wird und insoweit keiner Änderung bedarf. Die nun vorgenommene Ergänzung der Norm im Zusammenhang mit der im Gesetz neu unter § 35 verankerten Ausschreibung zur gezielten Kontrolle (siehe Absatz 1 Nummer 4 neu) erfolgt unter Beachtung dieser Entscheidungen des Bundesverfassungsgerichtes.

Mit Blick auf die in § 43a Absatz 1 Satz 1 Nummer 2 vorgesehene Möglichkeit der Erfassung und des Abgleichs von Kfz-Kennzeichen auch an einer polizeilichen Kontrollstelle, die den Zugang zu einer Versammlung kontrolliert, ist allerdings § 78, der die Einschränkung von Grundrechten normiert, um Artikel 8 Absatz 1 des Grundgesetzes und damit um das Recht auf Versammlungsfreiheit zu ergänzen (siehe hierzu ausführlicher die Begründung zu § 78).

§ 44 (Rasterfahndung)

Die schon bisher in § 44 normierte Befugnis zur Rasterfahndung wird mit Änderungen übernommen.

Unter Berücksichtigung der bundesverfassungsgerichtlichen Vorgaben im Urteil zum Bundeskriminalamtgesetz vom 20. April 2016 (Aktenzeichen 1 BvR 966/09, siehe hierzu insbesondere Randnummer 112) wird eine Rasterfahndung durch Ergänzung des Absatzes 1 nun auch unter den Voraussetzungen des § 67a Absatz 1 und damit zur Verhütung terroristischer Straftaten nach § 67c zugelassen (siehe Satz 1 Nummer 1). Der bereits im Beschluss des Bundesverfassungsgerichtes vom 4. April 2006 - Aktenzeichen 1 BvR 518/02 - zur Zulässigkeit der Rasterfahndung geforderte Schutz hochrangiger Rechtsgüter ist schon durch die Definition der terroristischen Straftat in § 67c gewährleistet. Auch § 48 Absatz 1 in Verbindung mit § 5 Absatz 1 Satz 2 des Bundeskriminalamtgesetzes lässt die Rasterfahndung zur Abwehr von Gefahren der Verwirklichung von Straftaten nach den § 129a Absatz 1 und 2 des Strafgesetzbuchs zu.

In Satz 1 Nummer 2 werden die bisherigen Voraussetzungen zur Zulässigkeit der Rasterfahndung übernommen und um die Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Sachen von bedeutendem Wert ergänzt. Diese Regelung orientiert sich an § 48 Absatz 1 Satz 1 des Bundeskriminalamtgesetzes (Vorgängerregelung § 20j). Diese Eingriffsvoraussetzung wurde durch das Bundesverfassungsgericht in der Entscheidung vom 20. April 2016 als verfassungsrechtlich unbedenklich beurteilt (vergleiche Randnummern 206 f a. a. O.)

Absatz 1 Satz 2 stellt mit Blick auf die Ausformung des funktionalen Trennungsgebots klar, dass eine Verpflichtung der dort genannten Behörden zur Datenübermittlung zum Zweck der Rasterfahndung nicht erfolgen darf.

Die Regelung in Absatz 2 Satz 1, dass Übermittlungsersuchen auf Namen, Anschrift, Tag und Ort der Geburt sowie auf im einzelnen Falle festzulegende Merkmale zu beschränken sind, bleibt bestehen und wird ergänzt um den klarstellenden Zusatz, dass sich das Ersuchen nicht auf personenbezogene Daten erstrecken darf, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Zudem wird in Satz 2 aus datenschutzrechtlichen Gründen bestimmt, dass von Übermittlungsersuchen nicht erfasste personenbezogene Daten übermittelt werden dürfen, wenn wegen erheblicher technischer Schwierigkeiten oder wegen eines unangemessenen Zeit- oder Kostenaufwands eine Beschränkung auf die angeforderten Daten nicht möglich ist. Diese Daten unterliegen aber einem ausdrücklichen Verwendungsverbot; die Löschung richtet sich nach § 45. Die zusätzlich aufgenommenen Regelungen in Absatz 2 enthalten auch § 48 Absatz 2 des Bundeskriminalamtgesetzes und andere Landesgesetze (vergleiche etwa § 46 Brandenburgisches Polizeigesetz, § 31 des Polizeigesetzes des Landes Nordrhein-Westfalen, § 40 Polizeigesetz Baden-Württemberg).

Die bisherigen Regelungen in Absatz 3 zur Dokumentation, Protokollierung und Kennzeichnung sind in § 44 aufgrund der in das Gesetz hierzu eingeführten zentralen Normen nicht mehr aufzunehmen. Die spezielle Regelung zur Weiterverwendung der Daten und zur Löschung im bisherigen Absatz 3 Satz 1 wird im neuen Absatz 7 aufgenommen. Rasterfahndungen nach § 44 unterliegen als in § 46f Absatz 2 aufgeführte Maßnahmen zudem der nach in § 48b Absatz 6 normierten Kontrolle durch die oder den Landesbeauftragten für den Datenschutz. Die Inanspruchnahme der Befugnis unterliegt zudem ausdrücklich den Berichts- und Unterrichtungspflichten nach § 48h.

Im Absatz 3 wird daher nun die Anordnung der Maßnahme bestimmt. Bisher war in § 44 Absatz 4 Satz 1 festgelegt, dass nur das Innenministerium die Maßnahme anordnen darf. Dieser Anordnungsvorbehalt wird nunmehr durch einen Richtervorbehalt ersetzt. Der Antrag auf richterliche Anordnung ist durch die Leitung der zuständigen Polizeibehörde zu stellen. Die gerichtliche Zuständigkeit und das Verfahren ergeben sich aus § 25b des Gesetzes. Zusätzlich aufgenommen wird eine Anordnungsregelung für den Eilfall. Ausschließlich in Fällen von Gefahr im Verzug, die im Falle einer Rasterfahndung jedoch nur im absoluten Ausnahmefall denkbar sind, wird der Leitung der Polizeibehörde das Recht eingeräumt, die Maßnahme selbst anzuordnen. In diesem Fall ist die richterliche Entscheidung jedoch unverzüglich nachzuholen und es wird zusätzlich bestimmt, dass die Anordnung zur Rasterfahndung außer Kraft tritt, wenn sie nicht binnen 3 Tagen durch das Gericht bestätigt wird. Über eine Anordnungsregelung im Eilfall verfügen auch andere Landesgesetze (vergleiche zum Beispiel § 38 Absatz 3 des Polizei- und Ordnungsbehördengesetzes des Landes Rheinland-Pfalz).

In den Absätzen 4 und 5 werden die Angaben, die der Antrag und die schriftliche Anordnung aufzuweisen haben, ausdrücklich festgelegt. Die Einschränkung des Absatzes 4 Nummer 1 („soweit möglich“) resultiert aus dem Umstand, dass es in der Praxis vorkommen kann, dass nicht alle in Absatz 2 Satz 1 genannten Angaben (beispielsweise die Anschrift) bekannt sein können.

In Absatz 6 wird die Regelung aus dem bisherigen Absatz 4 Satz 2 zur Unterrichtung der oder des Landesbeauftragten für den Datenschutz übernommen.

Absatz 7 enthält die bisher im Absatz 3 Satz 1 enthaltene spezielle Regelungen zur Datenweiterverarbeitung und Löschung.

§ 45 (Berichtigung, Ergänzung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten)

§ 45 enthält auch weiterhin die Pflicht der verantwortlichen Stelle zur Berichtigung, Ergänzung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten bei Unrichtigkeit, Unvollständigkeit oder Vorliegen sonstiger Gründe, die eine Löschung oder alternativ Einschränkung der Verarbeitung begründen. Dieses Recht wird - neben der Schaffung des neuen § 48a - zur Umsetzung von Artikel 16 Richtlinie (EU) 2016/680 angepasst. Aus dem in Artikel 16 Richtlinie (EU) 2016/680 enthaltenen Recht der betroffenen Person auf „Berichtigung oder Löschung personenbezogener Daten und Einschränkung der Verarbeitung“ ergibt sich sogleich die Pflicht der verantwortlichen Stelle, diese Verarbeitungsvorgänge vorzunehmen (siehe Artikel 16 Absatz 1 und 2 Richtlinie (EU) 2016/680). Diese Pflicht besteht jedoch unabhängig davon, ob die betroffene Person darum ersucht.

Der bisher geltende Absatz 1 wird um Satz 2 gekürzt. Die darin bisher enthaltene Pflicht zur Dokumentation ist bereits durch § 46d geregelt. Weiterhin enthalten ist die Pflicht zur Berichtigung unrichtiger und Ergänzung unvollständiger Daten.

Im Absatz 2 werden in Satz 1 dahingehend Klarstellungen vorgenommen, dass die Pflicht zur Löschung zum einen im Rahmen einer Einzelfallprüfung (die insbesondere nach Beendigung einer Datenerhebungsmaßnahme unverzüglich durchzuführen oder beispielsweise aus Anlass der Änderung des der Speicherung zugrunde liegenden Sachverhaltes vorzunehmen ist), zum anderen aufgrund des Endes der festgesetzten Prüffrist nach § 45a festgestellt werden kann. Zudem wird unterstrichen, dass in beiden Szenarien die Löschung unverzüglich zu erfolgen hat. Eine Löschung umfasst bei nicht-elektronisch gespeicherten Daten auch die Vernichtung von Unterlagen.

Auch die Löschgründe erfahren eine Änderung. So werden die bisher geltenden Nummern 1 und 2 aufgrund des neuen Verarbeitungsbegriffs in Nummer 1 zusammengefasst und um die Ausnahmemöglichkeit der Zulässigkeit durch ein anderes Gesetz ergänzt. Eine Zulässigkeit der weiteren Speicherung ist beispielsweise in dem Fall denkbar, dass zwar eine Datenverarbeitung nach dem SOG M-V unzulässig ist, jedoch die erhobenen Daten zur Verfolgung einer Straftat benötigt werden und die Strafprozessordnung eine Verarbeitung der erhobenen Daten zulässt (vergleiche §§ 161ff der Strafprozessordnung).

In Nummer 2 wird in Anlehnung an § 75 Absatz 2 des Bundesdatenschutzgesetzes der Artikel 16 Absatz 2 Richtlinie (EU) 2016/680 dahingehend umgesetzt, dass die Löschpflicht bei Vorliegen einer rechtlichen Verpflichtung zur Löschung eingeführt wird. Dies ist zum Beispiel der Fall, wenn kernbereichsrelevante Daten erhoben wurden (vergleiche § 26a).

Nummer 3 entspricht dem bisher geltenden Absatz 2 Satz 2 Nummer 1.

Nummer 4 entspricht dem bisher geltenden Absatz 2 Satz 2 Nummer 2 mit der Erweiterung, dass die Daten nicht gelöscht werden müssen, wenn ihre Weiterverarbeitung (zu einem anderen Zweck) nach § 36 Absatz 2 bis 4 zulässig ist.

Die neu eingeführte Nummer 5 berücksichtigt den Fall, dass eine zuvor freiwillig abgegebene Einwilligung nach § 26 widerrufen wird. In diesen Fällen sind die Daten zu löschen, es sei denn, die Erhebung wäre auch aufgrund einer Rechtsvorschrift zulässig gewesen.

Absatz 2 Satz 2 stellt klar, dass das Nichtvorhandensein eines Löschgrundes zum Zeitpunkt der Prüfung keine automatische unbefristete anschließende Speicherung bedeutet. Es muss in Anwendung des § 45a gleichzeitig mit dem (vorläufigen) Absehen von der Löschung eine Frist zur erneuten Prüfung festgelegt werden. Die Entscheidung über das Absehen von der Löschung sowie die Festlegung der neuen Prüffrist muss nach § 46d Absatz 1 Satz 1 Nummer 4 und 6 dokumentiert werden, um nachträglich die Rechtmäßigkeit der Entscheidung prüfen zu können. Gleichzeitig verhindert es ein automatisches Verlängern der Aufbewahrungsdauer.

Absatz 3 entspricht weitestgehend dem bisher geltenden Absatz 4 und wird zur Umsetzung von Artikel 16 Absatz 3 der Richtlinie (EU) 2016/680 auch sprachlich angepasst.

Satz 1 Nummer 1 bleibt inhaltlich unverändert. Nach § 1 Absatz 3 gehört der Schutz privater Rechte zur Gefahrenabwehr, wenn gerichtlicher Schutz nicht rechtzeitig zu erlangen ist und ohne die Hilfe die Gefahr besteht, dass die Verwirklichung des Rechts vereitelt oder wesentlich erschwert wird. Dies ist in der Praxis beispielsweise bei einem Antrag auf Akteneinsicht nach § 48 in Aufzeichnungen nach § 32a denkbar, die als Beweismittel in Betracht kämen.

Die Erweiterung des Katalogs der Tatbestände, bei deren Vorliegen eine Verarbeitungseinschränkung an die Stelle einer Löschung treten kann, um Satz 1 Nummer 2 nimmt ein entsprechendes Element aus Artikel 16 Absatz 3 Buchstabe b der Richtlinie (EU) 2016/680 auf und versteht den dort verwendeten Begriff „Beweiszwecke“ im Sinne von „Zwecke eines gerichtlichen Verfahrens“.
Nummer 2 ist dahingehend auszulegen, dass ein gerichtliches Verfahren oder Verwaltungsverfahren nur dann ein Hinderungsgrund sein kann, wenn es innerhalb der gesetzlichen Frist begonnen wurde. Dementsprechend können Daten, die nur aufgrund von Nummer 2 nicht gelöscht wurden, gelöscht werden, sofern kein solches Verfahren (aufgrund Fristablaufs) mehr in Betracht kommt.
Nummer 3 orientiert sich an der Formulierung des § 58 Absatz 3 Satz 1 Nummer 3 des Bundesdatenschutzgesetzes. Die Möglichkeit, von der Löschung wegen unverhältnismäßigen Aufwands abzusehen, ist als restriktiv auszulegende Ausnahmeregelung anzusehen. Im Grundsatz sollte die bei der verantwortlichen Stelle zum Einsatz kommende IT-Infrastruktur darauf ausgelegt sein, eine Löschungsverpflichtung auch technisch umsetzen zu können. In ihrer Verarbeitung eingeschränkte Daten dürfen selbstverständlich nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand (vergleiche auch § 58 Absatz 3 Satz 2 des Bundesdatenschutzgesetzes); in Fällen der Nummer 1 nur mit Einwilligung der betroffenen Person, da die Verfolgung des Zwecks maßgeblich von dem Einverständnis der betroffenen Person abhängig ist. Im Übrigen dürfen solche Daten - wie bisher in § 45 Absatz 4 Satz 2 geregelt - zu wissenschaftlichen Zwecken nach Maßgabe des § 37a Absatz 2 verwendet werden. In Satz 3 wird die Regelung aus § 58 Absatz 4 des Bundesdatenschutzgesetzes übernommen, dass bei automatisierten Dateisystemen zum Schutz der Daten technisch ausreichende Vorkehrungen zu treffen sind, die eine Einschränkung der Verarbeitung eindeutig erkennbar machen und eine Verarbeitung für andere Zwecke nicht ohne weitere Prüfung ermöglichen.

In Absatz 4 wird der bisher geltende Absatz 5 übernommen und an die neue Struktur der Vorschrift angepasst.

In Absatz 5 wird der bisher geltende Absatz 6 zum einen mit sprachlichen Anpassungen übernommen. Zudem wird der Hinweis auf die besondere Mitteilungspflicht im Falle eines zu befürchtenden Nachteils der betroffenen Person gestrichen. In Umsetzung von Artikel 7 Absatz 2 und 3 der Richtlinie (EU) 2016/680 ist jede zuständige Behörde verpflichtet, die Qualität der übermittelten Daten zu überprüfen und - unabhängig von einem möglichen Nachteil der betroffenen Person im Einzelfall - dementsprechend bei Abweichungen die Empfänger zu informieren. Die Datenqualität ist ein allgemeiner Datenschutzgrundsatz, der ebenso in Artikel 5 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679 verankert ist. Durch Satz 2 ist in Umsetzung von Artikel 16 Absatz 5 Richtlinie (EU) 2016/680 zudem bei Berichtigungen für die Fälle, in denen Daten nicht selbst erhoben, sondern zuvor von anderen Stellen empfangen wurden, eine Information an die übermittelnden Stellen vorgesehen.

In der Praxis ist es durchaus denkbar, dass beispielsweise Polizeibehörden auf Basis von Daten des Einwohnermeldeamtes Bescheide erstellen und im Zuge des Verfahrenslaufes - vor Kenntnisnahme durch das Einwohnermeldeamt - feststellen, dass Daten (wie etwa die Adresse) unrichtig sind. Dies muss jedoch nicht lediglich von Behörden übermittelte Daten betreffen, sodass im Wortlaut des Satzes 2 (abweichend von Artikel 16 Absatz 5 der Richtlinie (EU) 2016/680) auch sonstige Stellen berücksichtigt werden.

§ 45a (Festlegung von Prüffristen)

Auf Basis des bisher geltenden § 46 werden zur Umsetzung des Artikels 5 der Richtlinie (EU) 2016/680 die Festlegungen zur Festsetzung von Prüffristen ergänzt und in § 45a zusammengeführt.

In Absatz 1 wird die allgemeine Pflicht zur Festlegung von Prüffristen (bisher § 46 Satz 1) in Anlehnung an § 75 Absatz 4 des Bundesdatenschutzgesetzes umformuliert. Durch die neue Formulierung wird noch einmal klargestellt, dass es sich bei diesen Fristen lediglich um Zeitpunkte der erneuten Prüfung, ob Daten weiterhin gespeichert werden müssen, handelt. Damit sollen die in der Vergangenheit häufig verzeichneten Verwechslungen mit Höchstspeicher- oder Löschfristen zukünftig vermieden werden. Zusätzlich wird darauf hingewiesen, dass die Einhaltung dieser Prüffristen durch angemessene verfahrensrechtliche Vorkehrungen zu gewährleisten ist (beispielsweise bei automatisierten Verfahren durch automatische Erinnerungsfunktionen). Absatz 1 weist auch darauf hin, dass in Rechtsvorschriften festgesetzte Höchstspeicher- oder Löschfristen unbeschadet bleiben (zum Beispiel § 37 Absatz 3).

Absatz 2 greift die bisher in § 46 Satz 2 enthaltenen Regelungen zu maximalen Prüffristen auf. Die Höhe der maximalen Prüffristen bleibt in Satz 1 unverändert. Der bisherige Wortlaut zum Fristbeginn, der auch § 77 Absatz 3 des Bundeskriminalamtgesetzes entspricht, wird um die Möglichkeit einer Entlassung aus einer Jugendanstalt, die bisher unberücksichtigt blieb, ergänzt. Zudem erfolgt mit Satz 3 nunmehr eine Festlegung hinsichtlich des Fristendes in Fällen, in denen weitere personenbezogene Daten nachträglich hinzugefügt werden. Diese Regelung ist jedoch auf solche personenbezogenen Daten beschränkt, die für die Gefahrenprognose maßgebend sind.

Absatz 3 stellt darüber hinaus klar, dass in dem Fall, dass auch bei Ablauf der Prüffrist keine Löschung der Daten in Betracht kommt, die Notwendigkeit ihrer weiteren Speicherung in regelmäßigen Abständen zu prüfen ist. Diese dürfen selbstverständlich nicht die in Absatz 2 Satz 1 genannten Zeitspannen überschreiten. Tritt vor Ablauf der neu festgesetzten Prüffrist eine Änderung des die Speicherung begründenden Sachverhaltes ein, ist die weitere Speicherung oder Löschung der Daten unverzüglich zu prüfen.

§ 45b (Durchführung einer Datenschutz-Folgenabschätzung)

§ 45b wird als Regelung zur Durchführung einer Datenschutz-Folgenabschätzung neu in das Gesetz eingefügt. Sie dient der Umsetzung von Artikel 27 der Richtlinie (EU) 2016/680 und greift weitgehend die Regelung des § 67 des Bundesdatenschutzgesetzes auf.

Die Datenschutz-Folgenabschätzung ist ein zentrales Element der strukturellen Stärkung des Datenschutzes. Die Voraussetzungen zur Durchführung einer Datenschutz-Folgenabschätzung können nur unvollkommen gesetzlich konkret ausgestaltet werden. So lässt sich dennoch feststellen, dass hinsichtlich des Umfangs der Verarbeitung nicht eine Einzelverarbeitung, sondern lediglich die Verwendung maßgeblicher Systeme und Verfahren zur Verarbeitung personenbezogener Daten mithilfe einer Datenschutz-Folgenabschätzung vorab in den Blick genommen werden müssen. Insoweit lässt sich eine Vergleichbarkeit mit den in § 48c Absatz 2 normierten Voraussetzungen zur Durchführung einer Anhörung der oder des Landesbeauftragten für den Datenschutz begründen. Kriterien für die Entscheidung, ob die vorgesehene Verarbeitung qualitativ erhöhte Gefahren für die Rechtsgüter der betroffenen Person in sich birgt, können beispielsweise der Kreis der betroffenen Personen, die Art der zur Datenerhebung eingesetzten Mittel oder der Kreis der zugriffsberechtigten Personen, mithin die Eingriffsintensität der mit der Verarbeitung verbundenen Maßnahmen im Sinne einer Gesamtwürdigung sein.

Die Konkretisierung der in Absatz 1 genannten Voraussetzungen obliegt letztlich der Praxis. Bei diesem Konkretisierungsvorgang wird allerdings zu beachten sein, dass die entstehenden Aufwände angemessen und beherrschbar bleiben müssen. Ferner ist festzuhalten, dass das Erfordernis einer Datenschutz-Folgenabschätzung nur für neue Verarbeitungssysteme oder wesentliche Veränderungen an bestehenden Verarbeitungssystemen gilt.

Im Zusammenhang mit den Vorgaben in Artikel 35 der Verordnung (EU) 2016/679 ist zu beachten, dass die Datenverarbeitung der nach diesem Gesetz zuständigen Behörden immer eine solche nach Artikel 6 Absatz 1 Buchstabe c oder e dieser Verordnung ist und auf der Grundlage einer hinreichend bestimmten Rechtvorschrift erfolgt, begleitet von weiteren Vorschriften des Datenschutzes, die die Anforderungen aufgrund der Form der Datenverarbeitung festlegen. Zugunsten des Datenschutzes wird daher zur einheitlichen Handhabung im Bereich des SOG M-V das mögliche Ermessen nach Artikel 35 der Verordnung (EU) 2016/679 hinsichtlich der Geltung der Absätze 1 bis 7 auf Null reduziert.

Im Absatz 2 wird zur besseren praktischen Handhabung festgelegt, dass für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlichem Gefahrenpotenzial eine gemeinsame Datenschutz-Folgenabschätzung erfolgen kann.

Absatz 3 verpflichtet die verantwortliche Stelle zur Beteiligung der oder des behördlichen Datenschutzbeauftragten bei der Durchführung der Datenschutz-Folgenabschätzung. Damit wird ein konkreter Beteiligungsfall normiert.

Absatz 4 legt den Inhalt der Folgenabschätzung fest und konkretisiert die in Artikel 27 Absatz 2 enthaltenen allgemeinen Angaben unter angepasster Übernahme der in Artikel 35 Absatz 7 der Verordnung (EU) 2016/679 enthaltenen Punkte.

Absatz 5 schreibt eine Überprüfungspflicht der verantwortlichen Stelle hinsichtlich der Verarbeitungsmaßgaben, die sich aus der Datenschutz-Folgenabschätzung ergaben, vor.

§ 45c (Verzeichnis von Verarbeitungstätigkeiten)

§ 45c wird neu in das Gesetz eingefügt und dient insbesondere der Umsetzung von Artikel 24 der Richtlinie (EU) 2016/680. Er entspricht weitgehend § 70 des Bundesdatenschutzgesetzes.

Hervorzuheben ist, dass sich die Absätze 1 und 2 ausschließlich auf die Datenverarbeitung zu Zwecken der Richtlinie (EU) 2016/680 beziehen. Die Schaffung einer einheitlichen Regelung für alle Aufgabenbereiche der zuständigen Stellen nach diesem Gesetz unter Präzisierung oder Schaffung spezifischer Bestimmungen der Regelung in Artikel 30 der Verordnung (EU) 2016/679 war wegen des weitgehend gleichen Regelungsinhalts nicht möglich. Soweit eine Datenverarbeitung in den Regelungsbereich der Verordnung fällt, richten sich die Angaben der Verzeichnisse nach den Vorgaben in Artikel 30 Absatz 1 und 2 der Verordnung (EU) 2016/679.

Absatz 1 verpflichtet die verantwortliche Stelle zur Führung eines Verzeichnisses über alle bei ihr durchgeführte Kategorien von Datenverarbeitungstätigkeiten. Dieses Verzeichnis dient vor allem der oder dem Landesbeauftragten für den Datenschutz dazu, einen Überblick über die bei der verantwortlichen Stelle durchgeführten Datenverarbeitungen zu erhalten. Das Zusammenspiel von Zurverfügungstellung von Protokolldaten (§ 46e Absatz 5), Anhörung der Datenschutzaufsicht (§ 48c) und Einsicht in das Verzeichnis (Absatz 3) gewährt der oder dem Landesbeauftragten für den Datenschutz ein umfassendes Bild über die bei der verantwortlichen Stelle durchgeführten Datenverarbeitungen. Dies ermöglicht es ihr oder ihm, ihre oder seine Aufgaben und Befugnisse im Hinblick auf die jeweils verantwortliche Stelle zielgerichtet, effizient und verhältnismäßig auszurichten und zu nutzen. Die Beteiligung der oder des Landesbeauftragten für den Datenschutz wird abgerundet und ergänzt durch die interne Beratungs- und Kontrolltätigkeit der oder des behördlichen Datenschutzbeauftragten (vergleiche §§ 48e bis g) und die Regelung zum umfassenden Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen. In Absatz 1 werden die in das Verzeichnis aufzunehmenden Angaben benannt. Die Begrifflichkeit „Kategorien von Datenverarbeitungstätigkeiten“ stellt hierbei klar, dass sich das Verzeichnis nicht auf einzelne Datenverarbeitungsvorgänge, sondern auf sinnvoll abgrenz- und kategorisierbare Teile der beim Verantwortlichen durchgeführten Datenverarbeitungen bezieht. Es kann sich anbieten, die nach Satz 1 Nummer 2 aufzunehmenden Angaben zu den Zwecken der Verarbeitung an den gesetzlichen Aufgabenzuschreibungen der betreffenden öffentlichen Stelle auszurichten.

Absatz 2 verpflichtet den Auftragsverarbeiter, ein Verzeichnis, wenngleich in geringerem Umfang als im Falle der verantwortlichen Stelle (Absatz 1), für Verarbeitungen zu führen, die er im Auftrag verarbeitet.

In Absatz 3 wird einheitlich für den Bereich der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2016/679 die elektronische Form der Führung des Verzeichnisses vorgeschrieben. Dies soll sowohl die Pflege des Verzeichnisses, als auch dessen Bereitstellung zur Prüfung durch die oder den Landesbeauftragten für den Datenschutz nach Absatz 4 erleichtern.

§ 46 (Allgemeine Informationspflicht)

§ 46 wird zur Bestimmung der Informationspflichten ebenfalls neu in das Gesetz aufgenommen.

Absatz 1 dient der Umsetzung des Artikels 13 der Richtlinie (EU) 2016/680 und orientiert sich an § 55 des Bundesdatenschutzgesetzes. Es geht hier um aktive Informationspflichten der verantwortlichen Stelle gegenüber betroffenen Personen unabhängig von der Geltendmachung von Betroffenenrechten. Dieser Informationspflicht müssen verantwortliche Stellen in allgemeiner Form nachkommen, denn betroffene Personen sollen sich unabhängig von der Datenverarbeitung im konkreten Fall in leicht zugänglicher Form einen Überblick über die Zwecke der bei der verantwortlichen Stelle durchgeführten Verarbeitungen verschaffen können und eine Übersicht über die ihnen zu Gebote stehenden Betroffenenrechte bekommen. Hierzu kann die Information beispielsweise über die Internetseite der verantwortlichen Stelle erfolgen (siehe Erwägungsgrund 42 der Richtlinie (EU) 2016/680).

Absatz 2 regelt die Informationspflicht im Anwendungsbereich der Verordnung (EU) 2016/679 unter Verweis auf § 5 des Landesdatenschutzgesetzes sowie auf die Artikel 13 und 14 der Verordnung (EU) 2016/679. Danach kann die verantwortliche Stelle von ihren Informationspflichten aus den Artikeln 13 und 14 der Verordnung (EU) 2016/679 in bestimmten Fällen in gewissem Umfang absehen.

§ 46a (Benachrichtigungspflichten bei verdeckten und eingriffsintensiven Maßnahmen)

§ 46a dient der Umsetzung der Vorgaben des Bundesverfassungsgerichtes hinsichtlich zu gewährleistender Benachrichtigungspflichten, insbesondere bei heimlichen Überwachungsmaßnahmen (siehe Urteil zum Bundeskriminalamtgesetz vom 20. April 2016, Aktenzeichen 1 BvR 966/09, Randnummer 136). Gleichzeitig wird der aktiven Informationspflicht aus Artikel 13 der Richtlinie (EU) 2016/680 Rechnung getragen. Die Regelung orientiert sich an § 74 des Bundeskriminalamtgesetzes.

Absatz 1 Satz 1 führt zunächst alle grundsätzlich zu einer Benachrichtigungspflicht führenden Datenerhebungsbefugnisse und die jeweils zu benachrichtigenden Personen abschließend auf.

Insbesondere ist darauf hinzuweisen, dass nach Nummer 1 eine Benachrichtigungspflicht in Bezug auf eine Maßnahme nach § 32 Absatz 1 Satz 1 Nummer 2 Satz 2 nur dann besteht, wenn die Befugnis zur gezielten Feststellung der Identität von Personen auf Übersichtsaufzeichnungen genutzt wurde. Da diese Maßnahme nicht bereits im Vorfeld offen erfolgen kann, muss die identifizierte Person benachrichtigt werden. Von der Benachrichtigungspflicht nach Nummer 2 sind ausschließlich verdeckte Maßnahmen nach § 33 Absatz 1 erfasst. Maßnahmen nach § 33 Absatz 3 sind mithin nicht benachrichtigungspflichtig, da diese allein den Schutz der bei einem Ersatz tätigen Personen bezwecken. In Bezug auf die in den Nummern 3 bis 7 genannten Befugnisnormen handelt es sich stets um Maßnahmen, die ohne Wissen der betroffenen Personen durchgeführt werden und somit einer grundsätzlichen Benachrichtigungspflicht unterliegen.

Hinsichtlich der in Nummer 4 erfolgten Herausnahme der Benachrichtigung in Fällen des § 33h Absatz 1 Satz 1, der die Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes oder nach § 14 Absatz 1 und § 15 Absatz 1 Satz 2 Nummer 1 des Telemediengesetzes gespeicherten Daten zulässt, ist anzumerken, dass es sich hierbei um keine eingriffsintensiven Maßnahmen handelt. Insofern wird hier den bundesrechtlichen Regelungen (siehe § 40 Absatz 4 des Bundeskriminalamtgesetzes oder § 100j Absatz 4 der Strafprozessordnung) und auch den landesrechtlichen Regelungen (siehe beispielsweise § 23a Absatz 9 des Polizeigesetzes Baden-Württemberg, § 36 Absatz 3 Satz 1 Nummern 7 und 8 des Polizeiaufgabengesetzes Thüringen, Artikel 50 Absatz 1 Satz 1 Nummer 7 des Polizeiaufgabengesetzes Bayern), die ebenfalls für derartige Maßnahmen keine Benachrichtigungspflicht normieren, gefolgt. Im Fall der Nummer 7 (elektronische Aufenthaltsüberwachung mit erstellten Bewegungsbildern) wird die Benachrichtigung als absolutes Recht der betroffenen Person spätestens zwei Monate nach Beendigung der Maßnahme ausgestaltet. Ein Unterbleiben oder gar ein Zurückstellen der Benachrichtigung nach Ablauf der zwei Monate kommt in Fällen der Nummer 7 nicht in Betracht. In Ausnahmefällen kann in Abwägung mit verfassungsrechtlich geschützten Rechtsgütern Dritter vom Grundsatz der Benachrichtigungspflicht abgesehen werden. Solche Abweichungen sind jedoch auf das unbedingt Erforderliche zu beschränken (vergleiche vorbenanntes Urteil des Bundesverfassungsgerichtes zum Bundeskriminalamtgesetz vom 20. April 2016, Randnummer 136). Die zulässigen Abweichungsszenarien sind Absatz 1 Satz 3 bis 6 geregelt.

Satz 3 orientiert sich an § 101 Absatz 4 Satz 3 der Strafprozessordnung und gibt vor, dass bei entgegenstehenden schutzwürdigen Belangen anderer von einer Benachrichtigung abgesehen werden kann. Abzuwägen ist dabei das Interesse der anderen betroffenen Person an der Information über die sie berührende Maßnahme mit dem Interesse der Zielperson an einer möglichst geringen Publizität. Entgegenstehende schutzwürdige Interessen sind vor allem der persönliche Lebens- und Intimbereich, die Gefährdung von Leib oder Leben oder von bedeutenden Sachwerten. Insbesondere kann die beschuldigte Person, gegen die sich der Tatverdacht nicht erhärtet hat, ein schutzwürdiges Interesse daran haben, dass ihre Kommunikationspartner nichts von den gegen sie durchgeführten Maßnahmen erfahren. Dies ist etwa in Fällen zu bejahen, in denen die beschuldigte Person eine Schädigung ihres Rufs und ihres wirtschaftlichen Erfolgs zu befürchten hat, würden ihre Geschäftspartner von der gegen sie gerichteten Telekommunikationsüberwachung Kenntnis erlangen (vergleiche auch Bundestagsdrucksache 15/4533 vom 15. Dezember 2004, Seite 19). Auch bei losen Bekanntschaften hat die beschuldigte Person häufig einen weiteren Eingriff in ihren sozialen Achtungsanspruch allein schon dadurch zu befürchten, dass sich zum Beispiel der Umstand einer Telekommunikationsüberwachung herumspricht. Dem mit einer Benachrichtigung von mit der beschuldigten Person bekannten betroffenen Personen verbundene Risiko einer neuen oder vertieften Verdächtigung oder Stigmatisierung kommt daher bei der Abwägung ein erhebliches Gewicht zu. Je privater und vertrauter aber der Kontakt zwischen der Zielperson und der mitbetroffenen Person ist, umso höher ist deren Interesse an einer Benachrichtigung zu bewerten. Dies gilt zum einen für private Vertrauensverhältnisse, bei denen wegen der engen persönlichen Beziehung der Kommunikationspartner in der Regel nicht damit zu rechnen ist, dass sich die Benachrichtigung zum Nachteil der Zielperson auswirkt. Zum anderen wiegen bei Berufsgeheimnisträgern, die ohnehin nur unter besonderen Einschränkungen überwacht werden dürfen, Eingriffe in die Vertraulichkeit der Kommunikation besonders schwer (BeckOK StPO/Hegmann StPO § 101, Randnummern 26 bis 31).

Entsprechend Satz 4 wird auch bei den in Absatz 1 Satz 1 Nummer 2, Nummer 4 (teilweise) und Nummer 5 in Bezug genommenen Maßnahmen, bei denen eine große Zahl lediglich mitbetroffener Personen in Betracht kommen kann, bei bloß marginaler Betroffenheit und damit einhergehendem, mutmaßlich fehlendem Interesse an einer Benachrichtigung, regelmäßig auf eine Benachrichtigung verzichtet werden können.

Ist der Polizei nach Beendigung noch nicht bekannt, um wen es sich bei den grundsätzlich zu benachrichtigenden Personen handelt, sind Nachforschungen zur Identität nach Satz 5 nur dann zu veranlassen, wenn das Benachrichtigungsinteresse der Person in Anbetracht der Eingriffsintensität der jeweiligen Maßnahme deutlich überwiegt.

Ebenso unterbleibt die Benachrichtigung in Fällen des Satz 6, wenn die dort benannten Stellen der Benachrichtigung nicht zustimmen. Hier ist davon auszugehen, dass das öffentliche Interesse an der Geheimhaltung der Datenverarbeitung das Interesse der betroffenen Person an der Benachrichtigung überwiegt. Die verantwortliche Stelle ist an die Entscheidung der Stellen gebunden.

Eine Benachrichtigung darf nach Absatz 2 nur dann erfolgen, wenn dies ohne Gefährdung des Zwecks der Maßnahme, der eingesetzten Polizeibeamtinnen und Polizeibeamten oder Vertrauenspersonen oder der in der jeweiligen Befugnisnorm genannten Rechtsgüter geschehen kann. Zu dem Kreis der Polizeibeamtinnen und Polizeibeamten zählen selbstverständlich auch verdeckt Ermittelnde. Auch wenn die Datenerhebung allein zum Schutz der eingesetzten Beamtinnen oder Beamten erfolgte, sind diese Umstände zu berücksichtigen. Satz 3 sieht zudem ein Abstimmungserfordernis mit der zuständigen Staatsanwaltschaft vor, falls der zunächst nur Anlass zur Vornahme präventivpolizeilicher Maßnahmen bietende Sachverhalt im Nachgang zur Einleitung eines strafprozessualen Ermittlungsverfahrens geführt hat. Sofern im Ergebnis die Benachrichtigung zurückgestellt wird, sind die Gründe der Staatsanwaltschaft, die zur Zurückstellung geführt haben, durch die die Maßnahme durchführende Stelle zu dokumentieren.

Absatz 3 definiert den Mindestinhalt der Benachrichtigung.

Absatz 4 regelt im Einklang mit Artikel 13 Absatz 3 Richtlinie (EU) 2016/680 die Möglichkeit der Zurückstellung der Benachrichtigung. Nach Ablauf bestimmter Fristen ist eine weitere Zurückstellung nur mit richterlicher Zustimmung zulässig (vergleiche Bundesverfassungsgerichtsurteil zum Bundeskriminalamtgesetz vom 20. April 2016, Randnummer 136). Während bei den besonders eingriffsintensiven Maßnahmen der Wohnraumüberwachung, der Online-Durchsuchung und der Quellen-TKÜ eine richterliche Zustimmung zur Zurückstellung bereits nach sechs Monaten erforderlich ist (vergleiche hierzu auch § 74 Absatz 3 des Bundeskriminalamtgesetzes), bedarf es einer solchen bei den übrigen, eine Benachrichtigungspflicht auslösenden Maßnahmen einheitlich erst nach einem Jahr. Hinsichtlich der Maßnahme nach Absatz 1 Satz 1 Nummer 7 wird auf die obigen Ausführungen unter Absatz 1 verwiesen.

Zur Vereinfachung der Benachrichtigungen und zur Herbeiführung eines einheitlichen Fristlaufs wird in Anlehnung an die Regelung in § 101 Absatz 6 Satz 4 der Strafprozessordnung und des § 74 Absatz 3 Satz 5 des Bundeskriminalamtgesetzes in Satz 2 klargestellt, dass die Frist bei mehreren zeitlich eng zusammenhängenden Maßnahmen grundsätzlich erst dann beginnt, wenn die letzte dieser Maßnahmen beendet wurde.

Zudem sieht Satz 4 auch die Möglichkeit des endgültigen Absehens von der Benachrichtigung in Fällen, die nicht bereits durch Absatz 1 Satz 3 bis 6 abgedeckt sind, nach frühestens fünf Jahren vor. Auch hier ist eine richterliche Zustimmung notwendig. Ungeachtet der Möglichkeit, bei entgegenstehenden überwiegenden Interessen einer betroffenen Person von der Benachrichtigung abzusehen, ist dies nach Satz 4 Nummer 2 auch dann möglich, wenn die Benachrichtigungsvoraussetzungen höchstwahrscheinlich auch zu einem späteren Zeitpunkt nicht mehr eintreten werden und jeweils eine Verwendung gegen die betroffene Person ausgeschlossen ist (vergleiche vorbenanntes Bundesverfassungsgerichtsurteil zum Bundeskriminalamtgesetz vom 20. April 2016, Randnummer 262). Dies wird durch die Löschvorschrift in Satz 5 sichergestellt (§ 45 ist zu beachten).

Die Benachrichtigung, das vorübergehende Absehen von der Benachrichtigung sowie der endgültige Verzicht sind nach § 46d Absatz 1 Satz 1 Nummer 7 zu dokumentieren. Ebenso sind die Protokollierungspflichten nach §§ 46e und 46f zu beachten.

§ 46b (Benachrichtigung über die Speicherung personenbezogener Daten von Kindern und unter Betreuung stehenden Personen)

§ 46b entspricht im Wesentlichen dem bisher geltenden § 36 Absatz 3, orientiert sich an § 75 des Bundeskriminalamtgesetzes und wird sprachlich angepasst. Zusätzlich wird die Norm durch Verweis auf § 46a Absatz 4 dahingehend ergänzt, dass eine weitere Zurückstellung sowie der endgültige Verzicht (nach frühestens fünf Jahren) der richterlichen Zustimmung bedürfen. Im Falle des endgültigen Verzichts sind die gespeicherten Daten nach § 45 Absatz 2 Satz 1 Nummer 4 zu löschen, es sei denn, die Daten dürfen nach § 36 Absatz 2 bis 4 weiterverarbeitet werden.

§ 46c (Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten)

§ 46c dient der Umsetzung von Artikel 31 der Richtlinie (EU) 2016/680 und orientiert sich maßgeblich an der Regelung des § 66 des Bundesdatenschutzgesetzes. Dabei erfolgen insbesondere sprachliche Anpassungen an den allgemeinen und gefahrenabwehrrechtlichen Sprachgebrauch.

Absatz 1 setzt die in Artikel 31 Absatz 1 der Richtlinie (EU) 2016/680 vorgeschriebene Pflicht zur Benachrichtigung einer betroffenen Person über eine Verletzung ihrer personenbezogenen Daten um.

Die Benachrichtigung der betroffenen Person sollte stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müsste die betroffene Person sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder ähnliche Verletzungen des Schutzes von Daten zu treffen (vergleiche Erwägungsgrund 62 der Richtlinie (EU) 2016/680).

In Absatz 2 werden in Anlehnung an § 66 Absatz 2 des Bundesdatenschutzgesetzes Form und Inhalt der Benachrichtigung festgelegt.

Mit Absatz 3 werden die nach Artikel 31 Absatz 5 der Richtlinie (EU) 2016/680 zulässigen Beschränkungen von der Benachrichtigungspflicht festgelegt. Die Regelung orientiert sich überwiegend an § 7 des Landesdatenschutzgesetzes und führt die Gründe auf, die eine Zurückstellung, Einschränkung oder ein Unterbleiben der Benachrichtigung rechtfertigen. Jeder Auskunftsverweigerung muss eine entsprechende Interessenabwägung vorausgehen, bei der auch die Bedeutung der Auskunft für die spätere Geltendmachung weiterer Betroffenenrechte zu berücksichtigen ist. Im Unterschied zu Absatz 4 ist hier insbesondere der zeitliche Moment zu beachten. Die Benachrichtigung darf nur soweit (inhaltlich) und solange (zeitlich) zurückgestellt werden, wie einer der aufgeführten Gründe besteht. Hier ist also zum einen inhaltlich zu trennen, für welche Teile der Verletzung ein Grund nach Absatz 3 vorliegt. Zum anderen ist aber vor allem regelmäßig zu prüfen, ob der Grund, der zunächst zur Zurückstellung geführt hat, noch vorliegt. In der Praxis kann es im Einzelfall auch dazu führen, dass die Zurückstellung solange gerechtfertigt wäre, dass es ein Unterbleiben bedeutet. Dies dürfte vor dem Hintergrund der aufgeführten Gründe aber eher einen Ausnahmefall darstellen.

Absatz 4 hingegen orientiert sich an § 66 Absatz 3 des Bundesdatenschutzgesetzes und führt diejenigen Gründe auf, deren Vorliegen sofort ein Unterbleiben der Benachrichtigung rechtfertigt. Diese sind derart ausgestaltet, dass sie - anders als bei einem der Gründe nach Absatz 3 - auch zukünftig nicht wegfallen können. Daher kommt hier kein vorübergehendes Zurückstellen in Betracht (vergleiche Erwägungsgrund 62 der Richtlinie (EU) 2016/680). Gleichzeitig sind diese Gründe derart umfassend, dass auch inhaltliche Einschränkungen nicht in Betracht kommen.

Absatz 5 dient der Umsetzung von Artikel 31 Absatz 5 der Richtlinie (EU) 2016/680.

Absatz 6 dient dem verfassungsrechtlichen Verbot einer Selbstbezichtigung. Die Regelung kann auf Artikel 83 Absatz 8 der Verordnung (EU) 2016/679 sowie auf Artikel 47 Absatz 4 der Richtlinie (EU) 2016/680 gestützt werden, wonach angemessene Verfahrensgarantien geschaffen werden müssen. Die Motivation zur Benachrichtigung der betroffenen Person bei einer Verletzung des Schutzes personenbezogener Daten soll nicht dadurch verringert werden, dass die somit verfügbar werdenden Verarbeitungsinformationen zur Einleitung eines Straf- oder Ordnungswidrigkeitenverfahrens führen können.

§ 46d (Dokumentationspflichten)

In § 46d werden die bisher in den einzelnen Befugnisnormen des SOG M-V enthaltenen Pflichten zur Dokumentation aufgrund der allgemeinen Gültigkeit und zugunsten der besseren Lesbarkeit der Normen in eine zentrale Norm zusammengefasst. So soll für die Praxis verdeutlicht werden, dass bei jeder Datenverarbeitung entsprechende Dokumentationen zu führen sind. Diese können schriftlich oder elektronisch erfolgen.

Gleichzeitig wird bereits in Absatz 1 klargestellt, dass die Dokumentationspflicht nicht nur für die verantwortliche Stelle gilt, sondern im Falle der Auftragsverarbeitung vom Auftragsverarbeiter ebenso erfüllt werden muss. Die in Satz 1 Nummer 3 erwähnte Kombination meint, dass zwar einzelne Daten in einem Fall nicht personenbezogen sein können, jedoch durch die Kombination aus verschiedenen Daten ein Personenbezug möglich wird.

Das Erfordernis der Uhrzeitdokumentation ist insbesondere bei Maßnahmen der Telekommunikationsüberwachung nach § 33d einschlägig, da nur so nachvollzogen werden kann, ob die Erhebung der Daten innerhalb des angeordneten Zeitraumes erfolgte. In Fällen der Datenübermittlung kommt den Dokumentationspflichten neben der Rechtmäßigkeitskontrolle auch hinsichtlich der Mitteilungspflicht nach § 45 Absatz 5 eine besondere Rolle zu. Nur wenn nachvollziehbar ist, welche Daten an wen, wann und in welchem Umfang übermittelt wurden, ist ersichtlich, wer von nachträglich festgestellten Verpflichtungen zur Berichtigung, Ergänzung, Löschung oder Einschränkung der Verarbeitung betroffen ist. Der Umfang der Dokumentation ist nicht abschließend geregelt und kann durch abweichende Spezialnormen verändert werden.

Absatz 2 erweitert zudem den Umfang der Dokumentationspflicht für verdeckte und eingriffsintensive Maßnahmen, die in § 46f Absatz 2 aufgeführt sind. Auch wenn die erhobenen Daten nicht in automatisierten Verfahren nach § 42 verarbeitet werden, müssen die in den §§ 46e und 46f genannten Inhalte festgehalten werden. Dies ist - sofern technisch nicht anders möglich - durch händische Dokumentation zu gewährleisten. Da nach § 48h Absatz 6 bei den in § 46f Absatz 2 genannten Maßnahmen ebenso wie bei Datenübermittlungen an Drittstaaten und weitere zwischen- und überstaatliche Stellen nach den §§ 39d bis 39h sowie nach der Verordnung (EU) 2016/679 eine regelmäßige datenschutzrechtliche Kontrolle durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz durchzuführen ist, sind die Dokumentationen zu diesen Maßnahmen mindestens bis zum Abschluss dieser Kontrolle aufzubewahren (vergleiche auch Bundesverfassungsgerichtsurteil zum Bundeskriminalamtgesetz vom 20. April 2016, Randnummer 205).

Absatz 3 regelt die Zwecke, zu denen die Dokumentationen verwendet werden dürfen. Entsprechen die Dokumentationen den Protokollierungen in § 46f, dann ist die Regelung in § 46f Absatz 4 Satz 1 zu beachten, andernfalls gilt § 46e Absatz 4 Satz 1.

Die Löschung der Dokumentationen bedarf hier keiner gesonderten Regelung, sondern richtet sich nach § 45, da sie eng mit den Datenverarbeitungsmaßnahmen verbunden sind.

§ 46e (Protokollierungspflichten)

§ 46e dient der Umsetzung von Artikel 25 der Richtlinie (EU) 2016/680 und entspricht weitgehend § 76 des Bundesdatenschutzgesetzes, auf den auch § 81 des Bundeskriminalamtgesetzes zur Protokollierung maßgeblich verweist.

Absatz 1 statuiert eine umfassende Pflicht der verantwortlichen Stelle zur Protokollierung der unter ihrer Verantwortung durchgeführten Datenverarbeitungen.

Absatz 2 enthält konkrete Vorgaben an den Inhalt der Protokolle und Absatz 3 trifft Regelungen zur Form der Protokollierung.

Absatz 4 enthält Verwendungsbeschränkungen, wobei von der durch Artikel 25 Absatz 2 der Richtlinie (EU) 2016/680 eröffneten Möglichkeit, die Protokolldaten über die Datenschutzkontrolle, Eigenüberwachung und Aufrechterhaltung der Datensicherheit hinaus auch im Zusammenhang mit der Verhütung oder Verfolgung von Straftaten zu verwenden, Gebrauch gemacht wird. Soweit sie zur Erstellung der Berichte nach § 48h benötigt werden, dürfen sie ebenfalls verwendet werden. In Absatz 4 wird neben den Verwendungszwecken auch eine allgemeine Löschfrist für die Protokolldaten festgelegt. Abweichungen durch anderweitige gesetzliche Regelungen bleiben unberührt. Letzteres ist etwa im Zusammenhang mit der Protokollierung von Verarbeitungsvorgängen bei verdeckten Maßnahmen nach § 46f Absatz 4 Satz 2 der Fall. Laut den Vorgaben des Bundesverfassungsgerichtes (vergleiche oben benanntes Urteil zum Bundeskriminalamtgesetz vom 20. April 2018, Randnummern 140 bis 143, 354) muss die oder der Landesbeauftragte für den Datenschutz in Fällen einer Datenübermittlung an Drittstaaten und weitere zwischen- und überstaatliche Stellen alle zwei Jahre eine Kontrolle durchführen. Dementsprechend wird die Aufbewahrungsfrist für Protokolldaten, die eine solche Übermittlung betreffen, auf die in § 48b Absatz 6 genannte Frist verlängert.

Mit der Regelung in Absatz 5 wird gewährleistet, dass der oder dem behördlichen Datenschutzbeauftragten und der oder dem Landesbeauftragten für den Datenschutz die Protokolle zum Zweck der Datenschutzkontrolle zur Verfügung stehen.

Absatz 6 verweist auf die mit § 115 Absatz 3 geschaffene Übergangsregelung zu den Protokollierungen.

§ 46f (Protokollierungspflichten bei verdeckten und eingriffsintensiven Maßnahmen)

Die Vorschrift setzt die Anforderungen aus dem Urteil des Bundesverfassungsgerichtes vom 20. April 2016 zum Bundeskriminalamtgesetz (Aktenzeichen 1 BvR 966/09) an eine umfassende, über die „normale“ Protokollierung (§ 46e) hinausgehende Protokollierungspflicht bei verdeckten und sonstigen eingriffsintensiven Maßnahmen um (siehe hierzu Randnummern 140 f). Um eine weitere Harmonisierung der Regelungslage zur Gewährleistung eines problemlosen Datenaustausches auch hinsichtlich der Protokollierung zu bewirken, orientiert sich diese Regelung an § 82 des Bundeskriminalamtgesetzes. Der bei diesen Maßnahmen besondere zu beachtende Umfang der Protokollierung ist in Absatz 1 und in Absatz 2 ergänzend in Abhängigkeit von der Maßnahme aufgeführt.

Nach Absatz 1 Nummer 1 und 2 sind zunächst die Bezeichnung des eingesetzten technischen Mittels und der Zeitpunkt seines Einsatzes zu dokumentieren. Die Vorschrift verlangt keine detaillierte technische Beschreibung des eingesetzten Mittels, sondern lediglich allgemein verständliche Angaben zu seinem Funktionsumfang, die zum Beispiel der betroffenen Person oder einem Gericht die Beurteilung ermöglichen, ob die in der Anordnung der Maßnahme bestimmten Vorgaben hinsichtlich der Art der Maßnahme beachtet worden sind. Anzugeben ist zum Beispiel im Falle einer Online-Durchsuchung nach § 33c in jedem Fall,

- 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 und
- ob nur gespeicherte Daten kopiert oder auch Tastatureingaben protokolliert werden.

Auch wenn die Gewährleistung effektiven Daten- und Rechtsschutzes, der Absatz 1 letztlich dient, keine vollständige technische Dokumentation der Funktionsweise des eingesetzten technischen Mittels erfordert, so wird es sich doch gleichwohl empfehlen, eine Kopie der eingesetzten Software aufzubewahren, damit sich im Zweifelsfall zum Beispiel gerichtlich bestellte Sachverständige davon überzeugen können, ob die Vorgaben der Anordnung tatsächlich beachtet wurden.

Absatz 1 Nummer 3 verlangt eine Protokollierung von Angaben, die die Feststellung der erhobenen Daten ermöglicht. Zu protokollieren sind also nicht die erhobenen Daten selbst, sondern lediglich Metadaten, die zuverlässige Rückschlüsse auf die erhobenen Daten erlauben. Solche Metadaten sind zum Beispiel die in den Dokumenteneigenschaften enthaltenen Angaben (Name der Datei, Versionsnummer, Zeitpunkt der letzten Änderung, Größe der Datei).

Nach Absatz 1 Nummer 4 ist schließlich zu dokumentieren, welche Organisationseinheit die Maßnahme durchführt.

Absatz 2 regelt nach dem Vorbild des § 82 Absatz 2 des Bundeskriminalamtgesetzes, dass zusätzlich zu Absatz 1 die zu den verschiedenen Maßnahmen jeweils aufgezählten Personen und Inhalte zu protokollieren sind. Die Betroffenheit der in Nummer 3 genannten Personen erstreckt sich nicht nur auf diejenigen Personen, deren personenbezogene Daten tatsächlich erhoben wurden, sondern auch auf die Personen, deren Wohnung Ziel der Maßnahme war.

Absatz 3 Satz 1 regelt, wann Nachforschungen zur Identität einer Person, die nicht bekannt ist, geboten sind. Durch die in Satz 2 geforderte Protokollierung der Anzahl der Personen, deren Protokollierung unterblieben ist, soll dem Erfordernis der umfassenden Protokollierung der in Rede stehenden Maßnahmen Genüge getan werden. Zudem können diese Information und daraus zu ziehende Schlüsse für die Auskunftsfähigkeit des Landes im Rahmen seiner Berichtspflichten nach § 48h erforderlich sein.

Absatz 4 Satz 1 enthält eine Zweckbegrenzung für die Nutzung der Protokolldaten auf Benachrichtigungs- und Berichtszwecke sowie Zwecke der Datenschutz- und Rechtmäßigkeitskontrolle. Satz 2 fordert die automatisierte Löschung der Protokolldaten nach Abschluss der Datenschutzkontrolle nach § 48b Absatz 6 durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz, es sei denn, die Aufbewahrung der Protokolldaten ist für Zwecke des Satzes 1 noch erforderlich.

§ 46g (Kennzeichnungspflichten)

Der Grundsatz der hypothetischen Datenneuerhebung lässt sich in den polizeilichen, automatisierten Informationssystemen nur umsetzen, wenn die darin gespeicherten personenbezogenen Daten mit den notwendigen Zusatzinformationen versehen - mithin gekennzeichnet - sind. Hierzu wird die neue Regelung des § 46g zur Kennzeichnung geschaffen.

In Anlehnung an die Vorschrift des § 14 Bundeskriminalamtgesetzes und § 20a des Hessischen Sicherheits- und Ordnungsgesetzes wird so zum einen auch zukünftig die Zusammenarbeit mit den anderen Bundesländern und dem Bund gesichert, zum anderen werden gleichzeitig die bisher in den einzelnen Erhebungsnormen enthaltenen Vorschriften zur Kennzeichnung zugunsten einer besseren Übersichtlichkeit zentriert sowie weitere aufgenommen.

Absatz 1 Satz 1 stellt klar, dass nur im Rahmen der Verarbeitung personenbezogener Daten in automatisierten polizeilichen Verfahren nach § 42 eine Kennzeichnung in Betracht kommt. Da die Teilnahme an polizeilichen Informationssystemen jedoch ausschließlich über automatisierte Systeme erfolgt, hat diese Einschränkung lediglich deklaratorischen Charakter.

Weiterhin sieht Satz 1 vor, dass personenbezogene Daten durch Angabe des Mittels der Erhebung der Daten einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden (Nummer 1), bei Personen, zu denen Grunddaten angelegt wurden, durch die Angabe der Kategorie nach § 25a Absatz 2 (Nummer 2), durch die Angabe der Rechtsgüter, deren Schutz die Erhebung dient (Nummer 3a) oder Straftaten oder Ordnungswidrigkeiten, deren Verfolgung oder Verhütung die Erhebung dient (Nummer 3 b), und durch die Angabe der Stelle, die sie erhoben hat (Nummer 4), zu kennzeichnen sind. Diese umfassende Kennzeichnung schafft die Voraussetzung für eine konsequente Anwendung des Grundsatzes der hypothetischen Datenneuerhebung.

Die folgenden Nummern 5 bis 9 greifen die bisher im SOG M-V in den einzelnen Erhebungsnormen enthaltenen Vorschriften zur Kennzeichnung (siehe zum Beispiel bisher geltende §§ 32a Absatz 5 Satz 2, 34b Absatz 7 Satz 1) auf und ergänzen diese. Nummer 10 trägt dem Umstand Rechnung, dass nach § 39b persönliche Einschätzungen oder Beurteilungen nur an Ordnungsbehörden oder die Polizei übermittelt werden dürfen. Um dieser Einschränkung in der Praxis entsprechen zu können, müssen jene Daten gekennzeichnet werden. Dies ist zwingend im Rahmen der technischen Möglichkeiten zu gewährleisten.

Nach Satz 2 kann die Kennzeichnung auch durch eine Angabe der Rechtsgrundlage der der Datenerhebung zugrundeliegenden Mittel ergänzt werden (vergleiche auch § 20a Absatz 1 Satz 2 des Hessischen Sicherheits- und Ordnungsgesetzes und § 14 Absatz 1 Satz 2 des Bundeskriminalamtgesetzes). Satz 3 schreibt zudem zur Gewährleistung einer späteren Kontrollmöglichkeit vor, dass personenbezogene Daten, die zu einem anderen Zweck als dem, zu dem sie erhoben wurden, weiterverarbeitet werden, ebenfalls entsprechend zu kennzeichnen sind. Dies betrifft insbesondere die Fälle, in denen personenbezogene Daten aus der Strafverfolgung zu Zwecken der Gefahrenabwehr weiterverarbeitet werden sollen. Diese Daten sind dann im polizeilichen Datenverarbeitungssystem entsprechend Satz 1 zu kennzeichnen. Sofern Daten, die zu Zwecken der Gefahrenabwehr erhoben wurden, zu anderen Zwecken weiterverarbeitet werden sollen, sind die Daten insoweit nur hinsichtlich des Umstandes der Zweckänderung ergänzend zu kennzeichnen. Ob und inwieweit die Daten nach der Zweckänderung darüber hinaus zu kennzeichnen sind, richtet sich nicht nach § 46g, sondern nach den eventuell bestehenden Kennzeichnungspflichten anderer Gesetze, die eine Verarbeitung zu diesem geänderten Zweck erlauben.

Zur Vermeidung einer Weiterverarbeitung personenbezogener Daten, die nicht dem Grundsatz der hypothetischen Datenneuerhebung entspricht, bestimmt Absatz 2, dass personenbezogene Daten, die nicht entsprechend den Anforderungen des Absatzes 1 gekennzeichnet sind, solange nicht weiterverarbeitet werden dürfen, bis eine Kennzeichnung entsprechend den Anforderungen des Absatzes 1 erfolgt ist.

Damit der Grundsatz der hypothetischen Datenneuerhebung auch bei der Weiterverarbeitung von Daten bei anderen Stellen beachtet werden kann, regelt Absatz 3, dass die nach Absatz 1 vorzunehmende Kennzeichnung im Falle der Übermittlung der Daten durch die empfangende Stelle aufrechtzuerhalten ist.

Absatz 4 verweist auf § 115, der abweichende Regelungen zu den Kennzeichnungsregelungen in den Absätzen 1 und 2 enthält.

§ 46h (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen)

Mit § 46h wird eine Norm zum Datenschutz durch Technikgestaltung und zu datenschutzfreundlichen Voreinstellungen in das SOG M-V übernommen.

Die Vorschrift entspricht mit ihren Absätzen 1 und 2 den Regelungen des § 71 des Bundesdatenschutzgesetzes und dient der Umsetzung von Artikel 20 der Richtlinie (EU) 2016/680, die generische Anforderungen an die datenschutzfreundliche Gestaltung von Datenverarbeitungssystemen (Privacy by Design) und die Implementierung datenschutzfreundlicher Grundeinstellungen (Privacy by Default) formulieren.

Der Norm liegt der Gedanke zugrunde, dass der Aufwand zur Verfolgung der hier formulierten Ziele und Anforderungen im Sinne eines effizienten Mitteleinsatzes in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen sollte. Zur Konkretisierung und Handhabbarmachung der Vorgaben werden in Absatz 1 Elemente des § 3a des Bundesdatenschutzgesetzes (in der bis zum 24. Mai 2018 geltenden Fassung) aufgenommen.

Die in Absatz 2 angesprochene Anforderung, die automatisierte umfassende Zugänglichmachung personenbezogener Daten zu verhindern, mündet letztlich in die Anforderung, eine solche Zugänglichmachung stets durch menschliches Zutun einer Prüfung zu unterziehen.

Absatz 3 bestimmt, dass die Einhaltung eines genehmigten Zertifizierungsverfahrens im Rahmen des Nachweises der Erfüllung der Anforderungen nach den Absätzen 1 und 2 als ein Umstand berücksichtigt werden kann.

§ 46i (Anforderungen an die Sicherheit der Datenverarbeitung)

Der neu in das SOG M-V eingefügte § 46i bestimmt die Anforderungen an die Sicherheit der Datenverarbeitung. Er dient der Umsetzung von Artikel 29 der Richtlinie (EU) 2016/680 und greift weitgehend die Regelung des § 64 des Bundesdatenschutzgesetzes auf.

Absatz 1 verpflichtet die verantwortliche Stelle und den Auftragsverarbeiter dazu, erforderliche technisch-organisatorische Maßnahmen zu treffen. Gleichzeitig wird klargestellt, dass die Ausgestaltung der Maßnahmen das Ergebnis eines Abwägungsprozesses sein soll, in den insbesondere der Stand der verfügbaren Technik, die entstehenden Kosten, die näheren Umstände der Verarbeitung und die in Aussicht zu nehmende Gefährdung für die Rechtsgüter der betroffenen Person einzustellen sind. Weiterhin wird klarstellend geregelt, dass bei der Festlegung der technisch-organisatorischen Maßnahmen die einschlägigen Standards und Empfehlungen, insbesondere Technische Richtlinien, des Bundesamts für Sicherheit in der Informationstechnik zu berücksichtigen sind.

In Absatz 1 wird der im bisher geltenden § 21 Absatz 1 des Landesdatenschutzgesetzes (in der vor dem 25. Mai 2018 geltenden Fassung) enthaltene Gedanke, wonach die Erforderlichkeit der Maßnahmen daran zu bemessen ist, ob ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht, aufgenommen. Satz 2 bestimmt, dass für den Nachweis der Erfüllung der Sicherheitsanforderungen unter anderem auf genehmigte Verhaltensregeln oder Zertifizierungsverfahren verwiesen werden kann.

In Absatz 2 wird festgelegt, was die in Absatz 1 genannten Maßnahmen umfassen und was sie sicherstellen sollen.

Absatz 3 greift die Vorgaben aus Artikel 29 Absatz 2 der Richtlinie (EU) 2016/680 auf, die weitgehend bereits in den §§ 21 und 22 des Landesdatenschutzgesetzes (in der vor dem 25. Mai 2018 geltenden Fassung) enthalten waren.

Absatz 4 gibt vor, dass Maßnahmen der Datensicherheit regelmäßig auf ihre Wirksamkeit zu untersuchen und zu bewerten sind. Er korrespondiert insoweit auch mit Absatz 1 Satz 2, wonach hinsichtlich der Datensicherheit die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen sind.

§ 46j (Vertrauliche Meldung von Verstößen)

Der neu in das Gesetz aufgenommene § 46j regelt die vertrauliche Meldung von Verstößen. Er setzt Artikel 48 der Richtlinie (EU) 2016/680 um und entspricht § 68 des Bundesdatenschutzgesetzes.

Die verantwortliche Stelle hat im Zusammenhang mit der Meldung von Verstößen sowohl interne Meldungen als auch Hinweise von betroffenen Personen oder sonstigen Dritten in den Blick zu nehmen. Für beides bietet sich als Kontakt- und Beratungsstelle die oder der behördliche Datenschutzbeauftragte an.

§ 46k (Auftragsverarbeitung)

§ 46k wird zur Regelung der Auftragsverarbeitung neu in das Gesetz aufgenommen und dient unter anderem der Umsetzung von Artikel 22 der Richtlinie (EU) 2016/680. Er orientiert sich weitgehend an der Regelung des § 62 des Bundesdatenschutzgesetzes und stellt Anforderungen für den Fall auf, dass die verantwortliche Stelle Auftragsverarbeitungsverhältnisse eingehen will. Bislang fanden sich entsprechende Regelungen im Landesdatenschutzgesetz. Am bisherigen Regelungsansatz, wonach die verantwortliche Stelle für die Datenübermittlung an den Auftragsverarbeiter keiner gesonderten Rechtsgrundlage bedarf, ändert sich nichts.

Absatz 1 entspricht mit wenigen sprachlichen Modifikationen § 62 Absatz 1 des Bundesdatenschutzgesetzes und regelt den bekannten Grundsatz, dass die datenschutzrechtliche Verantwortlichkeit in Auftragsverarbeitungsverhältnissen bei der beauftragenden Stelle bleibt; sie ist somit verantwortliche Stelle im Sinne des Artikels 3 Nummer 8 der Richtlinie (EU) 2016/680 und Artikel 4 Nummer 7 der Verordnung (EU) 2016/680.

Absatz 2 beschreibt die an den Auftragsverarbeiter zu stellenden Anforderungen und setzt insbesondere Artikel 22 Absatz 1 der Richtlinie (EU) 2016/680 um. Die beauftragende Stelle hat den Auftragsverarbeiter sorgfältig auszuwählen und dabei insbesondere die Art der zu verarbeitenden Daten zu berücksichtigen, was vor allem im Bereich der straftatenbezogenen Gefahrenabwehr durch die Polizei, etwa bei verdeckten Maßnahmen, eine besondere Rolle spielt. In Verbindung mit Satz 2 wird somit deutlich, dass die Anforderungen an den Auftragsverarbeiter umso höher sind, je sensibler die zu verarbeitenden Daten sind. Nach Satz 3 kann die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 der Verordnung (EU) 2016/679 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 der Verordnung (EU) 2016/679 durch einen Auftragsverarbeiter als Umstand zur Begründung für dessen Geeignetheit im Sinne des Satzes 2 dienen. Dies entbindet die beauftragende Stelle jedoch nicht von einer grundsätzlichen Prüfung der Geeignetheit des Auftragsverarbeiters, vor allem hinsichtlich seiner Zuverlässigkeit im sicherheitsrelevanten Sinn.

Absatz 3 entspricht § 62 Absatz 3 des Bundesdatenschutzgesetzes und regelt die Voraussetzungen für die Eingehung von Unterauftragsverarbeitungsverhältnissen. Dadurch wird Artikel 22 Absatz 2 der Richtlinie (EU) 2016/680 umgesetzt.

Absatz 4 entspricht im Wesentlichen § 62 Absatz 4 des Bundesdatenschutzgesetzes und trifft Regelungen für den Fall, dass der Auftragsverarbeiter einen weiteren Auftragsverarbeiter (Unterauftragsnehmer) hinzuzieht. Mit dem Verweis auf Absatz 2 wird klargestellt, dass die Anforderungen an die Geeignetheit des weiteren Auftragsverarbeiters dieselben sind wie diejenigen, die für den Auftragsverarbeiter selbst gelten.

Absatz 5 entspricht weitgehend § 62 Absatz 5 des Bundesdatenschutzgesetzes. Dort werden die erforderlichen (Mindest-)Inhalte einer der Auftragsverarbeitung zugrunde liegenden Vereinbarung niedergelegt. Diese Inhalte sind sowohl dem Artikel 22 Absatz 3 der Richtlinie (EU) 2016/680 als auch dem § 4 des Landesdatenschutzgesetzes (in der vor dem 25. Mai 2018 geltenden Fassung) entnommen und in den Regelungskontext eingepasst worden.

In Satz 2 werden Elemente aus Artikel 22 Absatz 3 Satz 2 der Richtlinie (EU) 2016/680und § 4 Absatz 2 Landesdatenschutzgesetz (in der vor dem 25. Mai 2018 geltenden Fassung) aufgenommen.

Absatz 6 trifft in Umsetzung von Artikel 22 Absatz 4 der Richtlinie (EU) 2016/680 Aussagen zur Form der Vereinbarung. Bezüglich der Anforderungen für die Ersetzung der Schriftform durch die elektronische Form wird auf § 3a des Landesverwaltungsverfahrensgesetzes verwiesen. Zusätzlich wird die bereits in § 4 Absatz 2 Satz 3 des Landesdatenschutzgesetzes (in der vor dem 25. Mai 2018 geltenden Fassung) bestehende Vorgabe eingefügt, dass die oder der Landesbeauftragte für den Datenschutz über die Beauftragung zu informieren ist, um der Kontrollaufgabe nachkommen zu können.

Absatz 7 dient der Umsetzung von Artikel 22 Absatz 5 der Richtlinie (EU) 2016/680.

§ 47 (Recht auf Anrufung der oder des Landesbeauftragten für den Datenschutz)

§ 47 dient mangels entsprechender allgemeiner Regelung im neugefassten Landesdatenschutzgesetz der Umsetzung von Artikel 52 Absatz 1 der Richtlinie (EU) 2016/680.

Jede betroffene Person hat damit das Recht, sich mit Beschwerden über die bei verantwortlichen Stellen durchgeführte Verarbeitung personenbezogener Daten an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz zu wenden. Gemäß Erwägungsgrund 85 der Richtlinie (EU) 2016/680 sollte in diesem Zusammenhang jede Aufsichtsbehörde Maßnahmen zur Erleichterung der Einreichung von Beschwerden treffen, wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

Weitere Bestimmungen bezüglich der Tätigkeit der oder des Landesbeauftragten für den Datenschutz in diesem Zusammenhang sind in § 48b Absatz 4 enthalten.

§ 48 (Recht auf Auskunft und Akteneinsicht)

In § 48 ist - wie bisher - das Recht der betroffenen Person auf Auskunft und Akteneinsicht als Spezialnorm zum Auskunftsanspruch aus § 1 des Informationsfreiheitsgesetzes M-V statuiert. Dieses wird zur Umsetzung von Artikel 14 der Richtlinie (EU) 2016/680 erweitert.

So wird in Absatz 1 in Anlehnung an § 57 des Bundesdatenschutzgesetzes der Inhalt der Auskunft dahingehend ergänzt, dass auch die voraussichtliche Dauer der Speicherung der Daten beziehungsweise alternativ die Kriterien für die Festlegung der Speicherdauer (Nummer 4), ein Hinweis auf das Recht nach § 48a (Nummer 5) sowie auf das Recht nach § 47 (Nummer 6) aufgenommen werden. Zudem wird mit Satz 2 das Recht der angefragten Behörde aufgenommen, einen Nachweis der Identität der antragstellenden Person zu verlangen, um missbräuchlichen Antragstellungen entgegenzuwirken.

In Absatz 2 wird die Pflicht zur Beteiligung betroffener Stellen aufgenommen. Sofern diese Stellen im Rahmen ihrer Stellungnahme Gründe darlegen, die darauf hinweisen, dass eine Auskunftserteilung die Aufgabenerfüllung dieser Stellen gefährden könnte, ist der Antrag auf Auskunft abzulehnen. Entsprechend § 57 Absatz 5 des Bundesdatenschutzgesetzes wird zudem festgelegt, dass bei Beteiligung von Verfassungsschutzbehörden des Bundes oder der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes zur Auskunftserteilung eine Zustimmung dieser Stellen vorliegen muss. Die Entscheidung dieser genannten Behörden ist also für die Behörde, bei der der Antrag auf Auskunft vorliegt, bindend; eine eigene Abwägung ist nicht vorzunehmen. Auch in diesen Fällen ist es irrelevant, ob die personenbezogenen Daten von diesen Behörden stammen oder an diese übermittelt wurden. Zweck dieser Regelung ist, dass die betroffene Person nicht über andere Behörden dasjenige erfahren soll, was ihr insbesondere die Sicherheitsbehörden oder Nachrichtendienste nicht direkt mitteilen würden.

Absatz 3 Satz 1 regelt, dass kein Auskunftsanspruch besteht, wenn eine Auskunft bereits erteilt wurde und die gespeicherten personenbezogenen Daten sich nicht geändert haben oder die Auskunft offensichtlich missbräuchlich verlangt wird. So soll neben dem Schutz der personenbezogenen Daten auch der Schutz der verantwortlichen Stelle vor Überlastung durch missbräuchlich gestellte Anträge gewährleistet werden. Satz 2 schreibt durch entsprechenden Verweis die gleichen Gründe für ein Zurückstellen, Einschränken oder Absehen von einer Auskunft vor wie sie nach den §§ 46a bis 46c für eine Benachrichtigung einschlägig sind. Diese dort genannten Gründe sind derart tiefgreifend, dass, wenn schon die aktive Benachrichtigung (noch) nicht erfolgen muss, auch die passive durch eine Auskunft nicht erfolgen darf. Durch Satz 3 wird jedoch klargestellt, dass ansonsten eine Auskunft nach § 48 keinerlei Auswirkungen auf die Benachrichtigungspflichten nach §§ 46a bis 46c hat. Insbesondere dürfen die Benachrichtigungen nicht unterbleiben, nur weil ein Antrag auf Auskunft vorliegt.

Absatz 4 entspricht weitgehend dem bereits im bisher geltenden § 48 Absatz 2 geregelten Recht auf Akteneinsicht. Mit Verweis auf die Voraussetzungen der Absätze 1 bis 3 wird deutlich gemacht, dass für die Einsichtnahme in Akten vor Ort dieselben Voraussetzungen vorliegen müssen wie für eine Einsichtnahme in Daten nach postalischer oder elektronischer Zusendung (Auskunft). Zur Klarstellung wird zudem Satz 2 um einen Verweis auf § 3 Absatz 4 Nummer 2 ergänzt.

Absatz 5 wird zur Umsetzung von Artikel 15 Absatz 3 der Richtlinie (EU) 2016/680 konkretisiert. Im Falle einer Ablehnung des Auskunfts- oder Akteneinsichtsantrages hat die verantwortliche Stelle die Ablehnungsgründe zu dokumentieren und grundsätzlich der betroffenen Person mitzuteilen. Die Mitteilung dieser Gründe kann jedoch in den in Satz 4 genannten Fällen (zunächst ganz oder teilweise) unterbleiben. Auch bei Vorliegen einer der Gründe nach Satz 4 ist die Dokumentation der Gründe der Ablehnung nach Satz 6 der oder dem Landesbeauftragten für den Datenschutz in auswertbarer Weise zur Verfügung zu stellen, soweit nicht das Ministerium für Inneres und Europa im Einzelfall feststellt, dass dadurch die Sicherheit des Landes, eines anderen Bundeslandes oder des Bundes gefährdet würde. Zudem begrenzt Satz 6 den Umfang der Informationen, die die oder der Landesbeauftragte für den Datenschutz der antragstellenden Person im Beschwerdeverfahren geben darf.

Die Ablehnungsgründe nach Absatz 3 sowie die Gründe für das Unterbleiben der Mitteilung der Ablehnungsgründe nach Absatz 4 dürfen nicht dadurch umgangen werden, dass die oder der Landesbeauftragte für den Datenschutz die entsprechenden Informationen im Beschwerdeverfahren preisgibt. Um dies zu vermeiden, bedarf es zuvor einer Zustimmung der verantwortlichen Stelle.

Neben der bereits in Absatz 5 Satz 3 enthaltenen Pflicht, die betroffene Person bei Ablehnung eines Antrages über die Möglichkeit der Beschwerde bei der oder dem Landesbeauftragten für den Datenschutz und der Wahrnehmung ihrer Rechte über diese oder diesen zu informieren, wird in Absatz 6 in Umsetzung von Artikel 15 Absatz 3 der Richtlinie (EU) 2016/680 diese Hinweispflicht auch auf die Fälle einer teilweisen Ablehnung oder verzögerten Bearbeitung des Antrages erweitert. Ein separater Hinweis auf die Möglichkeit der Inanspruchnahme gerichtlichen Rechtschutzes ist in den Fällen, in denen ein Bescheid erlassen wird, entbehrlich, da dieser ohnehin nach § 37 Absatz 6 des Verwaltungsverfahrens-, Zustellungs- und Vollstreckungsgesetzes des Landes Mecklenburg-Vorpommern mit einer Rechtsbehelfsbelehrung zu versehen ist.

Absatz 7 schließt durch Verweis auf § 6 Absatz 5 des Landesdatenschutzgesetzes einen Auskunftsanspruch hinsichtlich Daten, die ausschließlich zu Zwecken der Datensicherung und der Datenschutzkontrolle gespeichert sind, aus.

Absatz 8 regelt bei offensichtlich unbegründeten oder in ungebührlichem Umfang gestellten Anträgen eine Ausnahme von dem Grundsatz der Gebührenfreiheit aus Absatz 1. Soweit nicht ausnahmsweise schon von der Bearbeitung abgesehen werden kann, können Kosten erhoben werden. Hierzu wird eine gesonderte Tarifstelle in der Verordnung über Kosten im Geschäftsbereich des Ministeriums für Inneres und Europa zu schaffen sein. Gemäß Erwägungsgrund Nummer 40 der Richtlinie (EU) 2016/680 kann beispielsweise eine angemessene Gebühr erhoben werden, wenn die betroffene Person ungebührlich und wiederholt Informationen verlangt oder wenn die betroffene Person ihr Recht auf Unterrichtung missbraucht, indem sie zum Beispiel falsche oder irreführende Angaben macht. Alternativ kann in diesen Ausnahmefällen auch ein Tätigwerden verweigert werden. In der Praxis wird im Rahmen der Anhörung gemäß § 28 Absatz 1 des Landesverwaltungsverfahrensgesetzes die Kostenerhebung angekündigt werden müssen.

§ 48a (Recht auf Berichtigung, Ergänzung, Löschung sowie Einschränkung der Verarbeitung)

§ 48a verankert in Anlehnung an § 58 des Bundesdatenschutzgesetzes das Recht der betroffenen Personen auf Berichtigung, Ergänzung, Löschung und Einschränkung der Verarbeitung und setzt damit Artikel 16 der Richtlinie (EU) 2016/680 um.

Damit erhält die betroffene Person nicht nur aufgrund des § 45 ein passives Recht auf Berichtigung, Ergänzung, Löschung und Einschränkung der Verarbeitung, sondern kann nach Absatz 1 aktiv die Prüfung einer Berichtigung, Ergänzung, Löschung und Einschränkung der Verarbeitung einleiten. In Satz 2 wird ein in Erwägungsgrund 47 der Richtlinie (EU) 2016/680 enthaltener Gedanke aufgenommen, wonach zur Vorbeugung massenhafter und nicht erfolgversprechender Anträge klargestellt wird, dass sich die Berichtigung auf die die betroffene Person betreffenden Tatsachen bezieht und nicht etwa auf den Inhalt von Zeugenaussagen. Gleiches gilt etwa für polizeifachliche Bewertungen.

In Satz 3 wird Artikel 16 Absatz 3 Satz 1 Buchstabe a der Richtlinie (EU) 2016/680 umgesetzt. Zwar sieht der Richtlinientext im beschriebenen Fall die Verarbeitungseinschränkung als Alternative zur Löschung vor. Da die Richtlinie allerdings im Fall der Verarbeitung unrichtiger Daten deren Berichtigung, aber nicht deren Löschung vorsieht, wird der in der Richtlinie (EU) 2016/680 beschriebene Sachverhalt systematisch korrekt in Absatz 1 verortet, indem für Fälle, in denen nach Bestreiten der Richtigkeit der Daten deren Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, an die Stelle der Berichtigung eine Verarbeitungseinschränkung tritt. Für das Bestreiten der Richtigkeit der bei der verantwortlichen Stelle verarbeiteten Daten durch die betroffene Person reicht die reine Behauptung der Unrichtigkeit nicht aus. Vielmehr müssen die Zweifel an der Unrichtigkeit durch Beibringung geeigneter Tatsachen belegt werden. Dies dient dem Schutz der fachlichen Arbeit der verantwortlichen Stelle und der Vermeidung unverhältnismäßigen Prüfaufwands. In Umsetzung des Artikels 12 Absatz 5 in Verbindung mit Artikel 16 der Richtlinie (EU) 2016/680 kann die verantwortliche Stelle nach Satz 5 bei begründeten Zweifeln an der Identität des Antragstellers die Bearbeitung seines Anliegens von der Erbringung geeigneter Nachweise abhängig machen. Diese zusätzlichen Informationen dürfen nur für diesen Zweck verarbeitet und nicht länger gespeichert werden als für diesen Zweck notwendig.

Stellt eine betroffene Person einen entsprechenden Antrag, prüft die verantwortliche Stelle diesen nach Maßgabe des § 45. Die betroffene Person ist gemäß Absatz 2 über den weiteren Verfahrensverlauf zu informieren. Eine Ablehnung ist grundsätzlich zu begründen. In den Ausnahmefällen kann die Begründung jedoch inhaltlich begrenzt (soweit), zeitlich aufgeschoben (solange) oder im Ganzen unterlassen werden.

Absatz 3 erklärt § 48 Absatz 6 bis 8 für entsprechend anwendbar. Damit sind auch die Personen, deren Antrag auf Berichtigung, Ergänzung, Löschung oder Einschränkung der Verarbeitung abgelehnt wurde, auf die Möglichkeit der Beschwerde bei der oder dem Landesbeauftragten für den Datenschutz und der Wahrnehmung ihrer Rechte über diesen hinzuweisen. Die Verpflichtung zur Belehrung über die Möglichkeiten der Inanspruchnahme gerichtlichen Rechtschutzes im Rahmen der Bescheidung des Antrages bleibt unberührt (vergleiche Begründung zu § 48 Absatz 6 und 8). Darüber hinaus ist auch hier § 6 Absatz 5 des Landesdatenschutzgesetzes entsprechend anwendbar, sodass Daten, die lediglich zu Zwecken der Datensicherung und der Datenschutzkontrolle gespeichert sind, von dem Recht auf Berichtigung, Ergänzung, Löschung sowie Einschränkung der Verarbeitung ausgenommen sind.

Weiterhin wird mit dem Verweis auf § 48 Absatz 8 auch für das Recht nach § 48a eine Ausnahme der Gebührenfreiheit bei offensichtlich unbegründeten oder in ungebührlichem Umfang gestellten Anträgen geregelt. Auch hier wird in der Praxis im Rahmen der Anhörung gemäß § 28 Absatz 1 des Landesverwaltungsverfahrensgesetzes die Kostenerhebung angekündigt werden müssen.

§ 48b (Aufsicht durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz über die Datenverarbeitung)

§ 48b wird neu in das Gesetz aufgenommen. Die Norm regelt die Aufsicht durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz über die Datenverarbeitung zu Zwecken der Richtlinie (EU) 2016/680. Im Unterschied zur Verordnung (EU) 2016/679 gesteht die Richtlinie den Mitgliedstaaten insbesondere bei der Ausgestaltung der wirksamen Abhilfebefugnisse einen Gestaltungsspielraum zu, indem in Artikel 47 Absatz 2 der Richtlinie (EU) 2016/680 lediglich exemplarisch bestimmte Abhilfebefugnisse genannt werden, ohne hiermit einen zwingenden Umsetzungsbefehl zu verknüpfen.

Absatz 1 legt im Anwendungsbereich der Richtlinie (EU) 2016/680 die der oder dem Landesbeauftragten für den Datenschutz zukommenden Aufgaben und Befugnisse fest und dient damit der normativen Umsetzung der Regelungsaufträge der Artikel 46 und 47 der genannten Richtlinie, wonach die unabhängige Aufsichtsbehörde bestimmte Aufgaben wahrzunehmen hat und ihr wirksame Untersuchungs-, Abhilfe- und Beratungsbefugnisse zustehen müssen.

Absatz 1 beschränkt die Abhilfebefugnisse der oder des Landesbeauftragten für den Datenschutz im Anwendungsbereich der Richtlinie (EU) 2016/680 zunächst auf die Möglichkeit des Ausspruchs der Warnung und Verwarnung im Sinne des Artikels 58 Absatz 2 Buchstabe a und b der Verordnung (EU) 2016/679. Im Unterschied zur Warnung steht bei einer Verwarnung bereits fest, dass ein Verstoß gegen die Bestimmungen der Richtlinie zum Datenschutz bei Polizei und Justiz stattgefunden hat. Darüber hinaus verfügt die oder der Landesbeauftragte für den Datenschutz über die in Artikel 58 Absatz 1 der Verordnung (EU) 2016/679 genannten Untersuchungsbefugnisse sowie die in Artikel 58 Absatz 3 Buchstabe a und b der Verordnung (EU) 2016/679 aufgeführten Beratungsbefugnisse. Eine mit Absatz 1 vergleichbare Regelung sieht auch Artikel 34 Absatz 1 des Bayerischen Datenschutzgesetzes vor.

Um den Regelungsauftrag aus Artikel 47 Absatz 2 der Richtlinie (EU) 2016/680 zu erfüllen, sieht Absatz 2 vor, dass die Aufsichtsbehörde auch weitergehende Maßnahmen anordnen darf, wobei die Löschung von Daten der Sicherheitsbehörden im Anwendungsbereich der Richtlinie (EU) 2016/680 nicht angeordnet werden darf. Im Bereich der Straftatenverhütung sowie der darauf bezogenen Gefahrenabwehr lassen sich uneingeschränkte Letztentscheidungs- und Anordnungsbefugnisse der oder des Landesbeauftragten nicht mit der Sensibilität und Komplexität der entsprechenden Verarbeitungen und dem Bedürfnis nach ständiger Verfügbarkeit rechtmäßig erhobener Daten und Datenverarbeitungsanlagen in Einklang bringen. Dieser Gedanke lässt sich auch dem Erwägungsgrund 82 der Richtlinie (EU) 2016/680 entnehmen, wonach die Befugnisse der Aufsichtsbehörde die speziellen Vorschriften für Strafverfahren, einschließlich der Ermittlung und Verfolgung von Straftaten nicht berühren dürfen. Dabei ist beachtlich, dass Datenverarbeitungsvorgänge, die im Zusammenhang mit der Verhütung von Straftaten stehen, vielfach, aber nicht unbedingt absehbar, in die Ermittlung und Verfolgung von Straftaten übergehen, so etwa nach § 100e Absatz 6 Nummer 3 der Strafprozessordnung bei der Verwendung von Daten aus polizeirechtlichen Maßnahmen zur Strafverfolgung. Selbst im Rahmen von bereits laufenden Strafverfahren können einzelne Datenverarbeitungen noch präventiven Charakter haben, zum Beispiel eine erkennungsdienstliche Maßnahme nach § 81b Alternative 2 der Strafprozessordnung.

Aus der engen Verzahnung von straftatenbezogener Gefahrenabwehr und Strafverfolgung ergibt sich, dass die Befugnisse der Aufsichtsbehörde im Anwendungsbereich der Richtlinie (EU) 2016/680 bereits dann Einschränkungen erfahren müssen, wenn die Datenerhebung zur Verhütung von Straftaten erfolgen muss, da jedwede unbeschränkte Durchgriffbefugnis gleichsam auch die speziellen Vorschriften für Strafverfahren berühren würde.

Insoweit sieht Absatz 2 zunächst ein Stufenverhältnis zu Maßnahmen nach Absatz 1 vor. Ferner dürfen weitergehende Maßnahmen, zum Beispiel die Beschränkung einer Datenverarbeitung auch nach der Ausübung einer Befugnis nach Absatz 1 nur angeordnet werden, wenn dies zur Abwendung einer fortbestehenden wesentlichen Verletzung datenschutzrechtlicher Vorschriften erforderlich ist und die Aufgabenwahrnehmung durch die verantwortliche Stelle dadurch nicht wesentlich beeinträchtigt wird.

In Absatz 3 wird für den Anwendungsbereich der Richtlinie (EU) 2016/680 das nach dem § 32 des Landesdatenschutzgesetzes (in der vor dem 25. Mai 2018 geltenden Fassung) bestehende Beanstandungsrecht in kompakterem Umfang beibehalten.

Unter Berücksichtigung der Befugnisse in den Absätzen 1 und 2 stehen der Aufsichtsbehörde damit hinreichend wirkungsvolle Möglichkeiten zur Verfügung, die als öffentliche Stelle an Recht und Gesetz gebundene verantwortliche Stelle auf aus ihrer Sicht rechtswidrige Verarbeitungen aufmerksam zu machen und ihren Beitrag dazu zu leisten, aus ihrer Sicht rechtswidrigen Zuständen abzuhelfen.

Absatz 4 dient der Umsetzung der Vorgaben nach Artikel 46 Absatz 1 Buchstabe g und Artikel 17 der Richtlinie (EU) 2016/680 und trifft Verfahrensregelungen für Fälle, in denen die oder der Landesbeauftragte für den Datenschutz die Rechte der betroffenen Person für diese wahrnimmt. Gleichsam werden die Anforderungen aus Artikel 52 Absatz 4 und Artikel 53 Absatz 2 und 3 der Richtlinie (EU) 2016/680 umgesetzt.

Absatz 5 stellt im Anwendungsbereich der Richtlinie (EU) 2016/680 klar, dass der Aufsichtsbehörde keine aufsichtlichen Befugnisse für Datenverarbeitungen zustehen, die von einem Gericht angeordnet beziehungsweise auf ihre Rechtmäßigkeit hin überprüft wurden.

Absatz 6 dient der Umsetzung der Anforderungen aus dem Urteil des Bundesverfassungsgerichtes zum Bundeskriminalamtgesetz vom 20. April 2016 (Aktenzeichen 1 BvR 966/09, vergleiche dort Randnummern 141, 266 und 322) im Hinblick auf die aufsichtliche Kontrolle der Wahrnehmung der Verarbeitungsbefugnisse der Sicherheitsbehörden. Es handelt sich insbesondere um die Übernahme von Anforderungen, die das Urteil an die Wirksamkeit der aufsichtlichen Kontrolle stellt.

In Absatz 6 wird mit Satz 1 und 2 angeordnet, dass die oder der Landesbeauftragte für den Datenschutz Kontrollen im Hinblick auf die Verarbeitung bei den in § 46f Absatz 2 genannten Maßnahmen und zu Datenübermittlungen an Drittstaaten und weitere zwischen- und überstaatliche Stellen nach den §§ 39d bis 39h und nach der Verordnung (EU) 2016/679 durchführt. Zudem wird normiert, dass die oder der Landesbeauftragte für den Datenschutz mindestens alle zwei Jahre kontrolliert, wobei die potentielle Arbeitsbelastung der Aufsichtsbehörde insoweit berücksichtigt wird, als dass diese Kontrolle sich auch auf Stichproben beschränken darf.

Die Möglichkeit einer umfassenden Kontrolle bleibt der Aufsichtsbehörde selbstverständlich vorbehalten. Die Kontrolltätigkeit wird durch Vorschriften wie beispielsweise die Art der Protokollierung in § 46e Absatz 3 unterstützt.

Es wird an dieser Stelle darauf hingewiesen, dass mit § 115 Absatz 4 eine Übergangsregelung zu § 48b Absatz 6 getroffen wird.

§ 48c (Zusammenarbeit mit der oder dem Landesbeauftragten für den Datenschutz und deren oder dessen Anhörung)

§ 48c wird als die Zusammenarbeit mit der oder dem Landesbeauftragten für den Datenschutz und deren beziehungsweise dessen Anhörung regelnde Norm neu in das Gesetz eingefügt.

Absatz 1 entspricht bis auf die Bezeichnung der Aufsichtsbehörde und die Einbeziehung des Auftragsverarbeiters dem § 68 des Bundesdatenschutzgesetzes. Er setzt Artikel 26 der Richtlinie (EU) 2016/680 um. Auf den in den genannten Normen vorgesehenen, irreführenden Passus, dass eine Zusammenarbeit „auf Anfrage“ zu erfolgen hat, wird verzichtet. Die hier angesprochene Pflicht der verantwortlichen Stelle zur Zusammenarbeit mit der oder dem Landesbeauftragten für den Datenschutz fasst die ohnehin sich aus anderen Vorschriften ergebenden Kooperationsverpflichtungen und Kooperationsbeziehungen zwischen der verantwortlichen Stelle und der oder dem Landesbeauftragten zusammen.

Die Absätze 2 bis 5 dienen der Umsetzung von Artikel 28 der Richtlinie (EU) 2016/680. Die Vorkonsultation - hier als Anhörung bezeichnet - der oder des Landesbeauftragten für den Datenschutz dient der datenschutzrechtlichen Absicherung in Bezug auf beabsichtigte Verarbeitungen in neu anzulegenden Dateisystemen, die ein erhöhtes Gefährdungspotential für Rechtsgüter der betroffenen Personen in sich bergen. Insofern besteht eine enge inhaltliche Verbindung zum Instrument der Datenschutz-Folgenabschätzung (siehe § 45b).

Prozedural wird diese Verbindung dadurch hergestellt, dass nach Absatz 2 Nummer 1 eine Anhörung durchzuführen ist, wenn im Ergebnis einer Datenschutz-Folgenabschätzung eine erhöhte Gefährdung angenommen wird und die verantwortliche Stelle hierauf nicht mit Maßnahmen zur Gefährdungsminimierung reagiert.

Der Umfang der der oder dem Landesbeauftragten für den Datenschutz vorzulegenden Unterlagen wird in Absatz 3 unter Berücksichtigung der Vorgaben aus Artikel 28 Absatz 4 der Richtlinie (EU) 2016/680 festgelegt.

In Absatz 4 wird wegen der unterschiedlichen Fristen in Artikel 28 Absatz 5 der Richtlinie (EU) 2016/680 und in Artikel 36 Absatz 2 der Verordnung (EU) 2016/679 eine Differenzierung zwischen den jeweiligen Anwendungsbereichen der genannten EU-Vorschriften vorgenommen. Mit Satz 4 wird die Vorschrift in Artikel 36 Absatz 2 Satz 4 der Verordnung (EU) 2016/679 implementiert. Satz 5 stellt im Sinne von Artikel 28 Absatz 5 Satz 1 der Richtlinie (EU) 2016/680 und Artikel 36 Absatz 2 Satz 1 der Verordnung (EU) 2016/679 klar, dass das Anhörungsverfahren die sonstigen Befugnisse der oder des Landesbeauftragten für den Datenschutz unberührt lässt.

Artikel 28 der Richtlinie (EU) 2016/680 knüpft an die Einleitung der Konsultation an, setzt aber nicht voraus, dass diese zwingend abgeschlossen sein muss, bevor personenbezogene Daten entsprechend verarbeitet werden. Zwar wird man im Regelfall den Abschluss der Konsultation im Interesse der Betroffenen abwarten. Im Ausnahmefall können jedoch Abweichungen geboten sein.

Die in Absatz 5 vorgesehene Eilfallregelung trägt solchen operativen und (polizei-) fachlichen Erfordernissen in Abweichung von Absatz 4 Satz 1 Rechnung, soweit die geplante Datenverarbeitung zu Zwecken der Richtlinie (EU) 2016/680 erfolgen soll. Die Nutzung der Eilfallregelung entbindet die verantwortliche Stelle gleichwohl nicht davon, die Empfehlungen der oder des Landesbeauftragten für den Datenschutz nach pflichtgemäßem Ermessen zu prüfen und die Verarbeitung gegebenenfalls daraufhin anzupassen. Weiterhin schmälert die Eilfallregelung nicht die der oder dem Landesbeauftragten für den Datenschutz zur Verfügung stehenden Befugnisse.

Absatz 6 dient der Umsetzung des Artikels 28 Absatz 2 der Richtlinie (EU) 2016/680. Er entspricht weitestgehend der Regelung in § 33 Absatz 2 Satz 3 des Landesdatenschutzgesetzes (in der vor dem 25. Mai 2018 geltenden Fassung). Mit der Einfügung des Wortes „frühestmöglich“ wird klargestellt, dass die oder der Landesbeauftragte für den Datenschutz frühzeitig in das Normsetzungsverfahren einzubinden ist. Dies betrifft insbesondere Gesetzgebungsverfahren während der vorparlamentarischen Phase und polizeiliche Verwaltungsvorschriften, die das Recht auf informationelle Selbstbestimmung berühren.

§ 48d (Benachrichtigung der oder des Landesbeauftragten für den Datenschutz bei Verletzungen des Schutzes personenbezogener Daten)

§ 48d orientiert sich als neu in das SOG M-V aufgenommene Vorschrift an der Regelung des § 65 des Bundesdatenschutzgesetzes und dient der Umsetzung von Artikel 30 der Richtlinie (EU) 2016/680. Die Vorschrift legt den Umfang und die Modalitäten der Meldung von „Verletzungen des Schutzes personenbezogener Daten“ an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz fest.

In Absatz 1 wird die Formulierung „unverzüglich und möglichst innerhalb von 72 Stunden“ zur Meldefrist aus Artikel 30 Absatz 1 der Richtlinie (EU) 2016/680 durch „unverzüglich, spätestens jedoch 72 Stunden“ ersetzt. Da genauere inhaltliche Angaben zur Verletzung nach den jeweiligen Absätzen 4 der genannten Artikel nachgereicht werden können, wird klargestellt, dass die „bloße“ Meldung einer Verletzung nach Bekanntwerden unverzüglich, spätestens nach 72 Stunden erfolgen muss. Die Kombination „unverzüglich und möglichst innerhalb“ ist wegen des Wortverständnisses „unverzüglich“ und des Regelungskontextes nicht stimmig.

In Absatz 2 wird bestimmt, dass die Maßgaben der Absätze 3 und 4 entsprechend auch für die Meldung von Verletzungen durch den Auftragsverarbeiter an die verantwortliche Stelle gelten. Dies geschieht vor dem Hintergrund, dass die entsprechenden Angaben notwendig sind, um seitens der verantwortlichen Stelle das „ob“ und „wie“ einer Meldung an die oder den Landesbeauftragten für den Datenschutz prüfen zu können.

Die Absätze 3 und 4 regeln den Umfang und den Inhalt der Meldung sowie eine Nachreichungspflicht.

Die in Absatz 5 geforderte Dokumentation muss in Qualität und Quantität so beschaffen sein, dass sie der oder dem Landesbeauftragten für den Datenschutz die Überprüfung der Einhaltung der gesetzlichen Vorgaben ermöglicht.

Es wird ergänzend darauf hingeweisen, dass § 65 Absatz 7 des Bundesdatenschutzgesetzes wegen des Regelungszusammenhangs einer Verwertung von Daten im Strafverfahren mangels landesgesetzlicher Gesetzgebungskompetenz nicht übernommen werden konnte.

Absatz 6 bestimmt eine Informationspflicht bei Verletzungen, wenn die betroffenen Daten von einer verantwortlichen Stelle in einem anderen Mitgliedstaat der Europäischen Union übermittelt wurden.

Absatz 7 stellt klar, dass die Meldepflicht an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz andere Meldepflichten, etwa solche an das Bundesamt für Sicherheit in der Informationstechnik als Meldestelle des Bundes für IT-Sicherheitsvorfälle (vergleiche § 4 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik), nicht ausschließt beziehungsweise diesen nicht vorgeht.

In Absatz 8 wird der in § 46c Absatz 6 enthaltene Gedanke überführt, wonach auch bei einer Benachrichtigung der Aufsichtsbehörde die Motivation zu dieser Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten nicht dadurch verringert werden soll, dass die durch die Meldung verfügbar werdenden Informationen zur Verarbeitung zur Einleitung eines Straf- oder Ordnungswidrigkeitenverfahrens führen können.

§ 48e (Bestellung behördlicher Datenschutzbeauftragter)

§ 48e wird ebenfalls neu in das Gesetz aufgenommen und orientiert sich an § 5 des Bundesdatenschutzgesetzes.

Absatz 1 legt zu Nachweiszwecken fest, dass die Bestellung der oder des behördlichen Datenschutzbeauftragten sowie ihrer oder seiner Vertretung schriftlich zu erfolgen hat. Die Absätze 2, 3 und 5 setzen Artikel 32 Absatz 2 bis 4 der Richtlinie (EU) 2016/680 um.

Absatz 4 bestimmt, dass sowohl interne als auch externe Datenschutzbeauftragte zulässig sind. Dies geht über die Vorgaben der Richtlinie (EU) 2016/680 hinaus und ist insoweit bei Stellen, die überwiegend Aufgaben im Sinne der Richtlinie wahrnehmen, insbesondere der Polizei, als absolute Ausnahme anzusehen. Dort soll die oder der behördliche Datenschutzbeauftragte grundsätzlich Bedienstete beziehungsweise Bediensteter der jeweiligen Stelle sein.

§ 48f (Stellung der behördlichen Datenschutzbeauftragten)

Der neu in das SOG M-V aufgenommene § 48f orientiert sich an § 6 des Bundesdatenschutzgesetzes.

Absatz 1 Satz 1 Nummer 1 und 2 setzt Artikel 33 der Richtlinie (EU) 2016/680 um.

Die Pflicht zur Einbindung der oder des behördlichen Datenschutzbeauftragten aus Nummer 1 bedeutet nicht, dass diese oder dieser bei jedem Einzelvorgang, bei dem personenbezogene Daten verarbeitet werden sollen, einzubinden ist. Vielmehr muss anhand der Umstände des Einzelfalls, insbesondere der Grundsätzlichkeit der mit ihm verbundenen Fragen abgewogen werden, ob eine Einbindung zum Schutz der personenbezogenen Daten geboten ist. Bei dieser Einschätzung ist insbesondere auf die unterstützende und beratende Funktion der oder des behördlichen Datenschutzbeauftragten (vergleiche Erwägungsgrundes 63 der Richtlinie (EU) 2016/680) abzustellen.

Absatz 1 Satz 1 Nummer 3 schreibt die Weisungsfreiheit der oder des behördlichen Datenschutzbeauftragten im Rahmen der Erfüllung ihrer oder seiner Aufgaben vor. Mit Satz 2 und 3 wird festgeschrieben, dass sie oder er unmittelbar der Leitung der Behörde berichtet und sie oder er wegen der Erfüllung ihrer oder seiner Aufgaben nicht abberufen oder benachteiligt werden darf. Dies geht über die Vorgaben der Richtlinie (EU) 2016/680 hinaus.

Bei dem besonderen Abberufungs- und Kündigungsschutz des Datenschutzbeauftragten in Absatz 2 handelt es sich um eine arbeitsrechtliche Regelung, die in das Gesetz implementiert wird. Die Gesetzgebungskompetenz besteht nach Artikel 72 Absatz 1, 74 Absatz 1 Nummer 12 des Grundgesetzes für das Land, da der Bund eine entsprechende Regelung in § 6 des Bundesdatenschutzgesetzes lediglich für den Bereich der Bundesverwaltung erlassen hat. Durch Absatz 2 soll die Stellung der oder des behördlichen Datenschutzbeauftragten gestärkt werden, indem die Möglichkeiten einer Abberufung stark eingeschränkt werden. Dies war bislang auch nach § 20 Absatz 2 des Landesdatenschutzgesetzes (in der vor dem 25. Mai 2018 geltenden Fassung) der Fall. Eine ordentliche Kündigung der oder des behördlichen Datenschutzbeauftragten ist aufgrund des sonst jedenfalls für interne Datenschutzbeauftragte entstehenden Konflikts in Bezug auf ihre Aufgabenwahrnehmung unzulässig.

Die oder der behördliche Datenschutzbeauftragte kann von ihrem oder seinem Amt aus den Gründen des § 626 des Bürgerlichen Gesetzbuches (BGB) abberufen werden, ohne gekündigt zu werden oder aber ihr oder ihm kann nach Maßgabe des § 626 BGB gekündigt werden. Die Abberufung selbst unterliegt keiner Formvorgabe, im Falle der Beendigung des Arbeitsverhältnisses ist indes auch § 623 BGB zu beachten.

Bestellung und Abberufung der oder des behördlichen Datenschutzbeauftragten haben sowohl eine datenschutzrechtliche als auch eine arbeitsrechtliche Komponente. Der Verweis auf § 626 BGB ist daher nur unter Berücksichtigung der Stellung der oder des behördlichen Datenschutzbeauftragten zu lesen. Wichtig sind diejenigen Gründe, die mit der Funktion der oder des Beauftragten zusammenhängen und die eine weitere Ausübung der Funktion unmöglich machen oder diese gefährden.

Absatz 3 Satz 1 legt fest, dass die oder der behördliche Datenschutzbeauftragte direkter Ansprechpartner für die Beschäftigten der betreffenden Behörde ist. Entsprechendes gilt nach Satz 2 für betroffene Personen. Dies geht über die Vorgaben der Richtlinie (EU) 2016/680 hinaus.

Satz 3 regelt die grundsätzliche Verschwiegenheitspflicht der oder des behördlichen Datenschutzbeauftragten. Die Verletzung von Privatgeheimnissen durch die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten ist gemäß § 203 Absatz 2a des Strafgesetzbuches strafbewehrt.

Das Zeugnisverweigerungsrecht in Absatz 4 sichert die Verschwiegenheitspflicht nach Absatz 3 Satz 3 ab. Die Regelung geht über die Vorgaben der Richtlinie (EU) 2016/680 hinaus.

§ 48g (Aufgaben der behördlichen Datenschutzbeauftragten)

Mit § 48g wird eine Regelung zu den Aufgaben behördlicher Datenschutzbeauftragter im Gesetz neu aufgenommen.

Um die Aufgaben der oder des behördlichen Datenschutzbeauftragten der Ordnungsbehörden und der Polizei für alle Verarbeitungszwecke einheitlich auszugestalten, werden mit Absatz 1 die in Artikel 39 der Verordnung (EU) 2016/679 ausdrücklich genannten Aufgaben auch für den Bereich der Richtlinie (EU) 2016/680 festgeschrieben und gleichzeitig unter Nutzung der Öffnungsklausel aus Artikel 39 Absatz 1 der Verordnung (EU) 2016/679 um zusätzliche Aufgaben ergänzt. Gemäß Artikel 33 Absatz 1 der Richtlinie (EU) 2016/680 ist die oder der behördliche Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden. Sie oder er unterstützt die verantwortliche Stelle und die Beschäftigten, die personenbezogene Daten verarbeiten, indem sie diese Personen über die Einhaltung ihrer jeweiligen Datenschutzpflichten unterrichtet und berät. Sie oder er ist hierbei gegenüber der Behörde unabhängig (vergleiche Erwägungsgrund 63 der Richtlinie (EU) 2016/680).

Die Absätze 2 bis 4 setzen die Artikel 32 bis 34 der Richtlinie (EU) 2016/680 um, indem die spezifischen Bestimmungen zu den Artikeln 37 bis 39 der Verordnung (EU) 2016/679 als allgemein geltende Vorschriften normiert werden. Absatz 2 bestimmt die frühzeitige Einbindung für den Fall des Verzeichnisses aller Verarbeitungstätigkeiten. Um ihrer Überwachungsfunktion nachkommen zu können, müssen die behördlichen Datenschutzbeauftragten Einsicht nehmen und gegebenenfalls Hinweise geben können. Absatz 3 stellt klar, dass die oder der behördliche Datenschutzbeauftragte weitere Aufgaben und Pflichten wahrnehmen kann, sofern diese nicht zu einem Interessenkonflikt führen. Gleichsam wird verhindert, dass der oder dem behördlichen Datenschutzbeauftragten durch arbeitsorganisatorische Maßnahmen die Aufgabenwahrnehmung erschwert oder unmöglich gemacht wird.

§ 48h (Parlamentarische Kontrolle, Unterrichtung der Öffentlichkeit)

Bisher obliegt dem Ministerium für Inneres und Europa gemäß dem aktuell geltenden § 34 Absatz 7 SOG M-V die Pflicht, dem SOG-Gremium mindestens einmal jährlich über Anlass und Dauer der Einsätze technischer Mittel

- zur Erhebung personenbezogener Daten aus Vertrauensverhältnissen im Sinne der §§ 53, 53a der Strafprozessordnung (siehe bisheriger § 33 Absatz 6 SOG M-V),
- ausschließlich zum Schutz der bei einem polizeilichen Einsatz tätigen Personen (siehe bisher geltender § 34 Absatz 4 SOG M-V),
- zur Erhebung personenbezogener Daten in oder aus Wohnungen (siehe bisher geltender § 34b Absatz 9 SOG M-V) und
- zur Überwachung und Aufzeichnung der Telekommunikation (siehe bisher geltender § 34a Absatz 9 SOG M-V)

zu berichten. Das Justizministerium ist zudem verpflichtet, das Gremium über die nach § 100c der Strafprozessordnung erfolgten Maßnahmen in Mecklenburg-Vorpommern (akustische Wohnraumüberwachung) zu unterrichten.

Neben der ausführlichen Berichtspflicht gegenüber dem sogenannten SOG-Gremium sieht § 34 Absatz 7 Satz 6 SOG M-V in der derzeit geltenden Fassung auch eine jährliche Unterrichtung des Landtages über die Anzahl der vorstehend aufgezählten Einsätze technischer Mittel vor.

Unter Beachtung der Vorgaben des Bundesverfassungsgerichtes in seiner Entscheidung zum Bundeskriminalamtgesetz vom 20. April 2016 (Aktenzeichen 1 BvR 966/09) reicht diese Regelungslage nicht mehr aus. So führt das Bundesverfassungsgericht unter anderem unter der Randnummer 143 aus:

„Da sich die Durchführung von heimlichen Überwachungsmaßnahmen der Wahrnehmung der Betroffenen und der Öffentlichkeit entzieht und dem auch Benachrichtigungspflichten oder Auskunftsrechte mit der Möglichkeit anschließenden subjektiven Rechtsschutzes nur begrenzt entgegenwirken können, sind hinsichtlich der Wahrnehmung dieser Befugnisse regelmäßige Berichte des Bundeskriminalamts gegenüber Parlament und Öffentlichkeit gesetzlich sicherzustellen. Sie sind erforderlich und müssen hinreichend gehaltvoll sein, um eine öffentliche Diskussion über Art und Ausmaß der auf diese Befugnisse gestützten Datenerhebung, einschließlich der Handhabung der Benachrichtigungspflichten und Löschungspflichten, zu ermöglichen und diese einer demokratischen Kontrolle und Überprüfung zu unterwerfen (vgl. BVerfGE 133, 277 <372 Rn. 221 f.>).“

Weiterhin führt es unter der Randnummer 268 aus:

„Schließlich fehlt es für eine verhältnismäßige Ausgestaltung der angegriffenen Überwachungsbefugnisse auch an Berichtspflichten gegenüber Parlament und Öffentlichkeit (vgl. BVerfGE 133, 277 <372 Rn. 221 f.>). Weder sieht das Gesetz Berichte darüber vor, in welchem Umfang von den Befugnissen aus Anlass welcher Art von Verdachtslagen Gebrauch gemacht wurde, noch darüber, wieweit die Betroffenen hierüber benachrichtigt wurden. Da sich die Wahrnehmung der in Frage stehenden Befugnisse sowohl dem Betroffenen als auch der Öffentlichkeit weitgehend entzieht, sind solche Berichte zur Ermöglichung einer öffentlichen Diskussion und demokratischen Kontrolle in regelmäßigen Abständen verfassungsrechtlich geboten […].“

Zusätzlich verweist das Bundesverfassungsgericht in der benannten Entscheidung in Bezug auf die Übermittlung von Daten ins Ausland unter der Randnummer 340 auf das Erfordernis von Berichtspflichten. Es führt unter der Randnummer 354 zu den Befugnissen zur Datenübermittlung im internationalen Bereich aus:

„*Im Übrigen genügen die Übermittlungsregelungen des § 14 Abs. 1 BKAG insoweit nicht den verfassungsrechtlichen Anforderungen, als es an […] der Anordnung von Berichtspflichten zur Übermittlungspraxis fehlt […].“*

Aus diesen Gründen wird mit § 48h nun eine zentrale und wesentlich erweiterte Norm zur parlamentarischen Kontrolle und zur Unterrichtung der Öffentlichkeit über bestimmte Maßnahmen nach dem Gesetz aufgenommen, wobei an dem bisherigen Verfahren des Berichts durch die fachaufsichtlich zuständigen Ministerien gegenüber einem Gremium des Landtages und der anschließenden Unterrichtung des Landtages grundsätzlich festgehalten werden soll.

In Absatz 1 Satz 1 wird das Ministerium für Inneres und Europa zu einem Bericht gegenüber dem SOG-Gremium über folgende durchgeführte Maßnahmen verpflichtet:

Zu berichten ist nach Satz 1 Nummer 1 über alle Einsätze besonderer Mittel der Datenerhebung nach § 33 Absatz 1. Umfasst sind damit alle Einätze der dort in den Nummern 1 bis 4 aufgeführten besonderen Mittel der Datenerhebung, insbesondere auch der Einsatz von verdeckt Ermittelnden und Vertrauenspersonen. Diese Berichtspflicht ist neu im Gesetz verankert und dient der Umsetzung der oben angeführten verfassungsgerichtlichen Vorgaben.

Auch über den Einsatz technischer Mittel in Wohnungen nach § 33b ist nach Satz 1 Nummer 2 zu berichten. Soweit die Maßnahme nach § 33b Absatz 9 als Personenschutzmaßnahme erfolgt ist, greift die Berichtspflicht jedoch nur dann, wenn die erhobenen Daten gemäß § 36 weiterverarbeitet wurden. Diese Berichtspflicht nach Nummer 2 wird nicht neu in das Gesetz aufgenommen. Maßnahmen der Wohnraumüberwachung sind nach dem bisher geltenden § 34b bereits berichtspflichtig. Auch der Einsatz technischer Mittel zur Eigensicherung bei einem Einsatz in Wohnungen unterliegt nach dem bisher geltenden § 34 Absatz 4 nur dann einer Berichtspflicht, wenn die Daten verwertet werden sollten.

Satz 1 Nummer 3 unterstellt die neu in das Gesetz aufgenommene Maßnahme des verdeckten Zugriffs auf informationstechnische Systeme nach § 33c (Online-Durchsuchung) einer Berichtspflicht.

Mit Satz 1 Nummer 4 werden Eingriffe in den Telekommunikationsbereich nach §§ 33d (und damit einschließlich der Befugnis zur Quellen-TKÜ), 33e (Auskunft über Nutzungsdaten), 33f (Identifizierung und Lokalisierung von Mobilfunkkarten/-endgeräten) und 33g (Unterbrechung oder Verhinderung der Telekommunikation) einer Berichtspflicht unterworfen. Bereits nach dem bisher geltenden § 34a waren Eingriffe in den Telekommunikationsbereich berichtspflichtig. Aufgrund der Neuregelung der Quellen-TKÜ und der neu aufgenommenen Befugnis zur Auskunft über Nutzungsdaten und dem damit verbundenen Eingriff ist diese Berichtspflicht konsequenterweise auch auf diese neuen Maßnahmen zu erstrecken.

Neu aufgenommen wird mit den Nummern 5 und 6 des Satzes 1 eine Berichtspflicht zur Rasterfahndung nach § 44 und zur elektronischen Aufenthaltsüberwachung nach § 67a. Gerade bei der Nutzung dieser Eingriffsmaßnahmen erscheint eine Information des SOG-Gremiums, des Landtages und auch der Öffentlichkeit angezeigt.

Mit Satz 1 Nummer 7 werden Datenübermittlungen einer Berichtspflicht unterstellt, soweit es sich um Datenübermittlungen an Drittstaaten und weitere zwischen- und überstaatliche Stellen handelt. Soweit also personenbezogene Daten an Drittstaaten und weitere zwischen- und überstaatliche Stellen durch die Polizei- oder Ordnungsbehörden oder deren Auftragsverarbeiter übermittelt werden, sind diese Datenübermittlungen - sowohl im Anwendungsbereich der Richtlinie als auch nach der Verordnung (EU) 2016/679 -berichtspflichtig. Datenübermittlungen im innerstaatlichen Bereich (§ 39b) und Übermittlungen an Mitgliedstaaten und Organisationen der Europäischen Union (§ 39c) sind nicht berichtspflichtig. Die Berichtspflicht zu den benannten Datenübermittlungen setzt ebenfalls die Entscheidung des Bundesverfassungsgerichtes vom 20. April 2016 um (siehe Randnummern 340 und 354). Während nach Satz 1 Nummer 1 bis 6 ausschließlich Maßnahmen der Polizei einer Berichtspflicht unterliegen, sind hier sowohl Ordnungsbehörden als auch die Polizei berichtspflichtig. Auch § 88 des Bundeskriminalamtgesetzes sieht eine Berichtspflicht über Datenübermittlungen nach § 27 des Bundeskriminalamtgesetzes vor.

Der Bericht nach Satz 1 bezieht sich auf ein Kalenderjahr und ist bis zum 31. Dezember des darauf folgenden Jahres abzugeben. Die bisher geltende „jährliche Berichtspflicht“ wird durch diese Vorgabe in Satz 2 präzisiert. Im Bericht ist nach Satz 3 zukünftig darzustellen, in welchem Umfang von den Befugnissen aus Anlass welcher Art von Gefahrenlagen Gebrauch gemacht wurde und in welchem Umfang die Benachrichtigung der betroffenen Personen erfolgt ist. Damit werden die oben angeführten Vorgaben des Bundesverfassungsgerichtes vollumfänglich umgesetzt. § 88 des Bundeskriminalamtgesetzes weist ebenfalls diesen Umfang der Berichtspflicht auf.

Die derzeit in § 34 Absatz 7 enthaltene Berichtspflicht des Justizministeriums wird in Absatz 1 Satz 4 übernommen. Unter Beachtung von Satz 2 hat es dem Gremium aber zukünftig entsprechend den Vorgaben in § 101b Absatz 4 der Strafprozessordnung über die durchgeführten Maßnahmen nach § 100c der Strafprozessordnung, die von einem Gericht in Mecklenburg-Vorpommern angeordnet worden sind, zu berichten. Somit wird der Bericht der von den Ländern gegenüber dem Bundesamt für Justiz über Maßnahmen nach § 100c der Strafprozessordnung abzugeben ist, mit der bestehenden landesrechtlichen Berichtspflicht zu diesen Maßnahmen harmonisiert und vereinheitlicht.

Mit Absatz 2 werden die Regelungen aus dem bisher geltenden § 34 Absatz 7 zur Bildung des SOG-Gremiums beibehalten. Wie bisher auch besteht es aus fünf Mitgliedern und wird vom Landtag gewählt. Die Zusammensetzung regelt sich nach dem Stärkeverhältnis der Fraktionen und das Gremium gibt sich eine Geschäftsordnung.

Die Unterrichtung des Landtages wird in Absatz 3 geregelt. Die Unterrichtung hat auf der Grundlage des Berichts nach Absatz 1 über die Anzahl der Maßnahmen nach Absatz 1 Satz 1 und Satz 3 zu erfolgen. Damit ist umgehend nach dem erfolgten Bericht gegenüber dem SOG-Gremium das Notwendige durch das Ministerium für Inneres und Europa und durch das Justizministerium für eine Unterrichtung des Landtages durch die Landesregierung zu veranlassen.

Die Unterrichtung muss zukünftig auch die zusätzliche Angabe enthalten, in welchem Umfang eine Benachrichtigung erfolgt ist. Die Unterrichtung erfolgt damit wesentlich umfassender als bisher und setzt die oben angeführte Vorgabe des Bundesverfassungsgerichtes um.

Im Gesetz festgelegt wird mit Absatz 4, dass sowohl das Ministerium für Inneres und Europa als auch das Justizministerium zur Information der Öffentlichkeit die erfolgte Unterrichtung an den Landtag auf ihrer Internetseite veröffentlichen müssen. Die Veröffentlichung hat umgehend nach Unterrichtung des Landtages zu erfolgen. Mit Absatz 4 wird ebenfalls die oben angeführte Vorgabe des Bundesverfassungsgerichtes umgesetzt.

Aufgrund der Vielzahl der Maßnahmen, zu denen ein Bericht abzugeben ist beziehungsweise eine Unterrichtung zu erfolgen hat, und in Anbetracht der Organisation der Landespolizei, wonach mehrere Behörden die in Absatz 1 genannten Maßnahmen durchführen oder bestimmte Maßnahmen - wie zum Beispiel die der angeordneten Telekommunikationsüberwachung - zentral über das Landeskriminalamt umgesetzt werden, bedarf es wie auch bisher schon näherer Vorschriften zur Zusammenstellung der Informationen und Unterlagen und auch deren Prüfung. Von der Berichtspflicht sind nun auch die Ordnungsbehörden betroffen, soweit Fälle der Datenübermittlung nach Absatz 1 Satz 1 Nummer 7 vorliegen. Auch hier gilt es wegen der Vielzahl der im Land zuständigen Ordnungsbehörden ein Verfahren festzulegen, damit das Ministerium für Inneres und Europa seinen Berichts- und Unterrichtungspflichten nachkommen kann. Vor diesem Hintergrund wird in Absatz 5 vorgesehen, dass zur Durchführung der Berichtspflichten, die dem Ministerium für Inneres und Europa obliegen, eine Verwaltungsvorschrift durch dieses Ministerium zu erlassen ist.

Zur Anwendung des § 48h bedarf es einer Vorbereitung und Umsetzung in der Praxis, sodass mit § 115 Absatz 5 eine Übergangsregelung geschaffen wird.

§ 49 (Straftaten von erheblicher Bedeutung)

Der bisher geltende § 49 (Katalog der Straftaten von erheblicher Bedeutung) wird übernommen und um folgende Straftatbestände ergänzt:

In Nummer 2 werden zunächst § 89c Absatz 1 bis 4 (Terrorismusfinanzierung) und die §§ 129a und b (Bildung terroristischer Vereinigungen) der Strafprozessordnung aufgenommen, die auch im Katalog des § 100a Absatz 2 der Strafprozessordnung aufgeführt sind, um den entsprechenden terroristischen Aktivitäten und Unterstützungshandlungen bereits im Bereich der Gefahrenabwehr begegnen zu können. Diese sind teilweise schon von Nummer 1 als Verbrechen abgedeckt, allerdings sind die Teile der Normen, die erhebliche Vergehen darstellen zur konsequenten Bekämpfung des Terrorismus ebenfalls einzubeziehen. Ebenfalls werden in Nummer 2 die Straftatbestände der §§ 184b Absatz 1 und 2 (Verbreitung, Erwerb und Besitz kinderpornographischer Schriften) und 184c Absatz 2 (Verbreitung, Erwerb und Besitz jugendpornographischer Schriften) aufgenommen, da diese ebenfalls als erheblich anzusehen sind. Sie sind auch in § 100a Absatz 2 der Strafprozessordnung enthalten. Die Taten sind in der Regel die Produkte vorheriger Missbrauchshandlungen, aus denen Gewinn erzielt werden soll, der wiederum Anreiz für weitere Taten gibt.

Auch hier müssen der Polizei zur Straftatenverhütung die erforderlichen Maßnahmen zur Verfügung stehen. Zudem erfolgt eine Aufnahme des § 303b Absatz 4 des Strafgesetzbuches (Computersabotage in einem besonders schweren Fall). Die dort genannten Handlungen sind im besonderen Maße aufgrund ihrer Begehungsweise, der Höhe des Schadens oder wegen der besonderen Bedeutung der geschädigten Rechtsgüter als erhebliche Straftaten anzusehen, wofür auch der Strafrahmen von 6 Monaten bis zu 10 Jahren Freiheitsstrafe spricht. Aufgrund der großen Bedeutung von Datenverarbeitungssystemen in der zunehmend multimedialen Gesellschaft müssen die besonderen Mittel der Gefahrenabwehr, die an den Katalog der erheblichen Straftaten anknüpfen, zur Verhütung solcher Straftaten Anwendung finden.

Nummer 3a wird um den Straftatbestand der Geldwäsche nach § 261 des Strafgesetzbuches ergänzt.
Nummer 3d wird um den ebenfalls in § 100a Absatz 2 der Strafprozessordnung befindlichen § 96 Absatz 2 des Aufenthaltsgesetzes (Einschleusen von Ausländern) erweitert, um konsequent gegen Schleuserkriminalität vorgehen zu können.

§ 49a (Grundsatz)

Mit § 49a wird zur Klarstellung die neue Regelung in das Gesetz aufgenommen, dass die Vorschriften des Abschnittes 3 anzuwenden sind, soweit nach Abschnitt 4 personenbezogene Daten verarbeitet werden und dort nichts Abweichendes bestimmt ist.

Diese Klarstellung ist erforderlich, da auch im Abschnitt 4 Maßnahmen normiert werden, die mit einer Verarbeitung personenbezogener Daten einhergehen (beispielweise §§ 52a, 52b, 67a, 67b). Auch bei diesen Maßnahmen müssen die Vorschriften zur Datenverarbeitung, die im 3. Abschnitt normiert und dort nicht speziell für dort normierte Befugnisse gelten, zur Anwendung gelangen. Damit wird sichergestellt, dass beispielsweise Normen wie § 26a zum Schutz des Kernbereiches privater Lebensgestaltung, § 26b zum Schutz von zeugnisverweigerungsberechtigten Personen oder auch der in § 36 verankerte Grundsatz der hypothetischen Datenneuerhebung auch bei im Abschnitt 4 verorteten Maßnahmen, bei denen personenbezogene Daten erhoben werden, zu beachten sind, soweit der Abschnitt 4 selbst nicht etwas Abweichendes bestimmt.

§ 50 (Vorladung)

Die bisherigen Absätze 1 bis 4 gelten unverändert fort und die Absätze 5 und 6 werden unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 51 (Verfahren bei der Vorführung)

§ 51 wird mit der Änderung übernommen, dass der in Absatz 3 enthaltene Verweis auf § 56 nun nicht mehr nur auf dessen Absätze 2 und 5, sondern vollumfänglich erfolgt. Durch die entsprechende Anwendung des § 56 gelangen nur diejenigen Vorschriften zur Anwendung, die sich auf den Fall der Vorführung übertragen lassen.

§ 52 (Platzverweisung und Wegweisung)

Die Überschrift wird um das Wort Wegweisung ergänzt und der bisher geltende Absatz 1 wird unverändert übernommen.

In Absatz 2 Satz 1 wird die sprachliche Gleichstellung vollzogen und es wird durch die Einfügung eines Klammerzusatzes ausdrücklich definiert, wer mit Blick auf die Regelung im neuen Absatz 3 gefährdete Personen sind. Dies sind demzufolge die Bewohner der von einer Wegweisung oder einem Betretungsverbot betroffenen Wohnung, von denen eine gegenwärtige Gefahr für Leib, Leben oder Freiheit abzuwenden ist. Darüber hinaus wird die Regelung dahingehend präzisiert, dass das Betretungsverbot durch die Einsatzleitung angeordnet werden kann. In diesem Fall informiert sie die Leitung der zuständigen Polizeibehörde über die Anordnung. Die schriftliche Anordnung hat die Vorgaben in § 52a Absatz 3 zu erfüllen und es wird zusätzlich bestimmt, dass Widerspruch und Anfechtungsklage gegen die Anordnung keine aufschiebende Wirkung entfalten. Im Übrigen werden die Regelungen des bisherigen § 52 Absatz 2 übernommen. Lediglich die geregelte gerichtliche Information im Falle einer Entscheidung nach dem Gewaltschutzgesetz an die „Polizei“ wird noch bestimmter gefasst, indem das Gericht die örtlich zuständige Polizeidienststelle unverzüglich über seine Entscheidung zu unterrichten hat. Diese unverzügliche Information stellt sicher, dass die Polizei damit Kenntnis davon erlangt, dass von ihr verfügte Maßnahmen mit dem Tag der Wirksamkeit der Entscheidung des Gerichtes beendet sind und damit eine etwaige Durchsetzung polizeilich verfügter Maßnahmen nicht mehr zulässig ist.

Der derzeit geltende Absatz 3 zur Anordnung von Aufenthalts- und Betretungsverboten wird aus § 52 herausgelöst und in die gesonderte Norm § 52a überführt und dort der übrigen Regelungssystematik, insbesondere der zur Aufenthaltsanordnung in § 67b, angepasst. Absatz 3 enthält in Bezug auf Maßnahmen, die nach Absatz 2 Satz 1 (Wegweisung) oder Satz 2 (Betretungsverbot) getroffen wurden, nun eine ausdrückliche und damit spezielle Datenübermittlungsvorschrift. So darf die Polizei personenbezogene Daten der in Absatz 2 benannten gefährdeten Personen an die zuständige und vom Ministerium für Soziales, Integration und Gleichstellung anerkannte Interventionsstelle übermitteln. Diese Übermittlungsbefugnis gilt jedoch nicht für Fälle, in denen ausschließlich gefährdete Personen betroffen sind, die das 18. Lebensjahr noch nicht vollendet haben, da die anerkannten Interventionsstellen hier keine Legitimation für eine beratende Tätigkeit besitzen.

Diese gesetzlich normierte Übermittlungsbefugnis ist letztlich nicht neu. Bisher konnte die Polizei personenbezogene Daten der nach Absatz 2 gefährdeten Personen auch schon an Interventionsstellen übermitteln. Denn diese gelten nach der Verwaltungsvorschrift der Parlamentarischen Staatssekretärin für Frauen und Gleichstellung zur „Anerkennung von Interventionsstellen gegen häusliche Gewalt und Stalking in Mecklenburg-Vorpommern“ vom 3. Februar 2010 (siehe Amtsblatt M-V 2010, Seite 58) als „Stellen außerhalb der öffentlichen Verwaltung“ im Sinne des bisher geltenden § 41 Absatz 1 des SOG M-V und damit als an der Gefahrenabwehr beteiligte Stellen. Neu ist also „lediglich“, dass die Befugnis der Polizei zur Datenübermittlung an anerkannte Interventionsstellen bei Maßnahmen, die nach Absatz 2 Satz 1 (Wegweisung) und Satz 2 (Betretungsverbot) getroffen wurden, nun ausdrücklich gesetzlich und damit für die Zukunft datenschutzrechtlich sicher verankert wird.

Hinzuweisen ist insbesondere darauf, dass die aus datenschutzrechtlicher Sicht für die Datenübermittlung in Betracht zu ziehende Lösungsmöglichkeit einer Einwilligungserklärung, bei deren Abgabe die gefährdete Person in der Lage sein sollte, die Folgen der Abgabe ihrer Erklärung in vollem Umfang zu überschauen, ihre Grenzen in den in § 52 Absatz 2 geregelten Fällen der Wegweisung oder des angeordneten Betretungsverbots findet. Aufgrund der psychischen Ausnahmesituation, in der sich die gefährdete Person bei Vorliegen einer gegenwärtigen Gefahr gerade im Zusammenhang mit häuslicher Gewalt befindet, ist ihr die Abgabe einer Einwilligungserklärung zur Datenübermittlung nicht zumutbar. Die nun normierte Datenübermittlung durch die Polizei an die Interventionsstellen hat in den besonderen Fällen der Wegweisung und des Betretungsverbots, die gerade deshalb erfolgen, weil dann eine akute Gefahrsituation für Leib, Leben oder Freiheit der gefährdeten Person besteht, eine entlastende Wirkung für diese gefährdete Person.

Zudem wird durch die Beschränkung der Norm auf die vom Ministerium für Soziales, Integration und Gleichstellung anerkannte Interventionsstellen sichergestellt, dass Datenübermittlungen nach Absatz 3 durch die Polizei an nicht anerkannte Beratungsstellen ausscheiden.

Des Weiteren wird in Absatz 3 eine Verwendungsbeschränkung normiert. So darf die anerkannte Interventionsstelle die ihr übermittelten personenbezogenen Daten ausschließlich dazu verwenden, den gefährdeten Personen unverzüglich Beratung zum Schutz ihrer Rechtsgüter anzubieten. Soweit eine gefährdete Person die Beratung ablehnt, muss die Interventionsstelle die übermittelten Daten unverzüglich löschen. Im Übrigen wird bestimmt, dass die übermittelten Daten nach Abschluss der Beratungstätigkeit durch die Interventionsstelle zu löschen sind.

§ 52a (Aufenthalts- und Betretungsverbot)

Mit § 52a wird der bisherige § 52 Absatz 3 als längerfristige Maßnahme gegenüber dem Platzverweis und der Wegweisung nach § 52 Absatz 1 und 2 in eine gesonderte Norm überführt. Die materiellen Anordnungsvoraussetzungen bleiben grundlegend bestehen.

Absatz 1 übernimmt den Wortlaut des bisherigen § 52 Absatz 3 Satz 1 und 2 weitgehend, wobei mit der Nennung der Ordnungsbehörden und der Polizei klargestellt werden soll, dass Aufenthalts- und Betretungsverbote von beiden Gefahrenabwehrbehörden angeordnet werden dürfen. Es besteht somit trotz der Ausrichtung der Norm auf die Verhütung von Straftaten keine vorrangige Zuständigkeit der Polizei. Davon ist der Gesetzgeber bei der Schaffung der bisherigen Vorschrift in § 52 Absatz 3 offenbar auch ausgegangen, da er die Befugnis ausdrücklich für Ordnungsbehörden und Polizei geschaffen hat und dabei als Hauptanwendungsfälle die Verhinderung gewalttätiger Veranstaltungen und die Bekämpfung der offenen Drogenszene benannt hat (vergleiche hierzu Landtagsdrucksache 3/2049, Seite 35; anders zur vergleichbaren Rechtslage in Niedersachsen Oberverwaltungsgericht Lüneburg, Beschluss vom 16. Januar 2014 - 11 ME 313/13 –; dagegen wiederum Vahle in Deutsche Verwaltungspraxis 2015, Seite 125, 126). Die Regelung einer parallelen Zuständigkeit rechtfertigt sich vor allem mit Blick auf den Bezug der Vorschrift zum Gemeindegebiet, das ordnungsrechtlich den örtlichen Ordnungsbehörden zugewiesen ist. In Absatz 1 wird ferner in Abgrenzung zur speziellen Regelung der Aufenthaltsanordnung in § 67b klargestellt, dass eine solche Anordnung nach § 67b der in § 52a geregelten Anordnung vorgeht, wenn die zu verhütende Straftat eine solche nach § 67c ist.

Nach Absatz 2 darf die Maßnahme nur von der Leitung der zuständigen Ordnungsbehörde einschließlich der ständigen Vertretung im Amt, angeordnet werden. Entsprechendes gilt für eine polizeiliche Anordnung, wobei durch die Behördenleitung auch besonders beauftragte Beamtinnen und Beamte mit der Anordnungskompetenz versehen werden können. Dies trägt dem Umstand Rechnung, dass in der Praxis wegen der Sachnähe Aufenthalts- und Betretungsverbote, vor allem gegenüber gewaltbereiten Fußballfans, von einer der Polizeibehörde untergeordneten Dienststelle, etwa einer Polizeiinspektion, angeordnet werden. Absatz 2 trifft daher - im Gegensatz zu dem bisher geltenden § 52 Absatz 3 - eine klare Regelung zur Anordnungskompetenz. Sie wird jedoch - wie zum Beispiel auch im geltenden und unverändert in dieses Gesetz übernommenen § 67b Absatz 2 - als behördliche und nicht als richterliche Kompetenz ausgestaltet. Zwar ist insbesondere das Grundrecht auf Freizügigkeit durch ein Aufenthalts- oder Betretungsverbot betroffen, jedoch liegt hier keine Freiheitsentziehung im Sinne des Artikel 104 Absatz 1 und 2 des Grundgesetzes, sondern lediglich eine Freiheitsbeschränkung vor. Da bei freiheitsbeschränkenden Maßnahmen eine richterliche Anordnung verfassungsrechtlich nicht zwingend geboten ist, wird eine solche – unter zusätzlicher Beachtung des Normgefüges des Gesetzes - in § 52a nicht aufgenommen. Damit wird auch die Justiz nicht unnötig beansprucht. Zudem ist darauf hinzuweisen, dass bei einer Verlängerung des Aufenthalts- oder Betretungsverbots über drei Monate hinaus und damit unter Berücksichtigung des zeitlichen Ausmaßes einer solchen Maßnahme, eine richterliche Anordnung in Absatz 5 normiert ist. Ein solches „gestuftes“ Anordnungsverfahren findet sich auch in § 52b oder in § 67b wieder (siehe ergänzend zur Frage der Anordnungskompetenz auch die Begründung zu § 67b Absatz 2 in der Drucksache des Landtages Mecklenburg-Vorpommern 7/1320neu).

Zudem wird bestimmt, dass Widerspruch und Anfechtungsklage gegen die Anordnung keine aufschiebende Wirkung haben, um eine sofortige Vollziehbarkeit der Anordnung zur Straftatenverhütung zu gewährleisten.

Absatz 3 regelt die Form und den Inhalt der Anordnung. Absatz 4 übernimmt die Sätze 3 und 4 des bisherigen § 52 Absatz 3.

Mit Absatz 5 Satz 1 wird die bisherige Höchstdauer der Anordnung von zehn Wochen auf drei Monate erhöht. Dies erfolgt mit Blick auf die unlängst neu in das Gesetz aufgenommene Regelung einer Aufenthaltsanordnung in § 67b und damit zur Harmonisierung der gesetzlichen Bestimmungen. Da es sich um eine Höchstfrist handelt, ist in jedem Anordnungsfall durch Vornahme einer Einzelfallprüfung zu entscheiden, inwieweit diese Höchstfrist auszuschöpfen ist. Mit Blick auf die neu normierte Höchstdauer der Anordnung erhöhen sich aus Gründen der Verhältnismäßigkeit (siehe auch § 15) die Anforderungen an die Anordnungsbefugnis sowie die Form und den Inhalt der Anordnung. Absatz 5 sieht entsprechend § 67b Absatz 4 vor, dass es zur Verlängerung der Maßnahme einer gerichtlichen Anordnung auf Antrag der Leitung der zuständigen Ordnungs- oder Polizeibehörde bedarf. Hinsichtlich der polizeilichen Anordnung liegt die Anordnungskompetenz damit abweichend von Absatz 2 ausschließlich bei der Leitung der Polizeibehörde, einschließlich der ständigen Vertretung im Amt. Das Gericht trifft hier unabhängig von den Gründen der vorherigen behördlichen Anordnung eine eigenständige neue Entscheidung in der Sache.

Nach Absatz 6 haben sich die jeweils örtlich zuständigen Ordnungs- und Polizeibehörden gegenseitig unverzüglich über ein nach dieser Vorschrift angeordnetes Aufenthalts- und Betretungsverbot zu unterrichten. Um ein solches Verbot vollumfänglich kontrollieren zu können, bedarf es einer umfassenden Information, insbesondere der Polizei, die bei Feststellung entsprechender Verstöße weitere Maßnahmen, zum Beispiel die Gewahrsamnahme, durchführen kann. Zudem bedarf es einer solchen Information, um einen gegebenenfalls bestehenden Geltungsvorrang polizeilicher Anordnungen im Rahmen von Maßnahmen zur Abwehr terroristischen Gefahren nach § 67b Absatz 5 Satz 2 aufzuzeigen.

§ 52b (Meldeauflage)

Bei der Meldeauflage handelt es sich um eine in der Praxis der Sicherheitsbehörden bewährte Maßnahme, um Straftaten zu verhindern. In Mecklenburg-Vorpommern werden Meldeauflagen erlassen, um die Begehung von Straftaten bei sportlichen, kulturellen und gesellschaftlichen Veranstaltungen, insbesondere im Zusammenhang mit Fußballgroßveranstaltungen, zu verhindern. Dabei können Meldeauflagen bisher sowohl von den Ordnungsbehörden nach Übermittlung der Gefahrenlage durch die Polizei als auch durch diese selbst angeordnet werden.

Nach gegenwärtiger Rechtsprechung sind Meldeauflagen auf der Grundlage der Generalklauseln der Polizeigesetze der Länder zulässig, um im Einzelfall Gefahren für die öffentliche Sicherheit oder Ordnung abzuwehren (vergleiche Urteil des Bundesverwaltungsgerichtes vom 25. Juli 2007 - Aktenzeichen 6 C 39.06; auch Verwaltungsgerichtshof Mannheim im Urteil vom 18. Mai 2017 - 1 S 1193/16 - DÖV 2017, 783). In der fachlichen Literatur wird der Rückgriff auf die Generalklausel in allen Fällen einer Meldeauflage jedoch diskutiert. Das Problem wird in der Eingriffsqualität der Meldeauflage im Vergleich zu geregelten Aufenthaltsverboten und Betretungsverboten gesehen. So kann die Meldeauflage im Einzelfall eingreifender sein als Aufenthaltsverbote (vergleiche hierzu auch Schucht NVwZ 2011, 709, 713). In einem aktuellen Urteil des Verwaltungsgerichtes Freiburg vom 15. April 2016 (Aktenzeichen 4 K 143/15) wird unter der Randnummer 59 ausgeführt:

„Sofern es, wie im baden-württembergischen Recht, an einer spezialgesetzlichen Grundlage für den Erlass einer Meldeauflage fehlt, wird in der Rechtsprechung die Anwendung der polizeilichen Generalklausel als Grundlage für eine Meldeauflage ausdrücklich für zulässig erachtet […]. Dem schließt sich die Kammer für den hier vorliegenden Fall an, auch wenn aus ihrer Sicht eine spezialgesetzliche Regelung etwa mit Blick auf die Frage der materiellen Voraussetzungen für ihren Erlass, der Bestimmung einer möglichen zeitlichen Höchstfrist derartiger Maßnahmen (wie etwa in § 27a Abs. 2 Satz 3 PolG erfolgt) oder der ausdrücklichen Festlegung der örtlichen Zuständigkeit für den Erlass der Meldeauflage durchaus wünschenswert wäre oder bei einer weiteren Verfestigung der Meldeauflage als polizeiliche Standardmaßnahme gar geboten sein könnte (vgl. zu dem früher ebenfalls auf §§ 1, 3 PolG gestützten Platzverweis etwa VG Stuttgart, Beschluss vom 17.05.2001 - 5 K 1912/01 -, juris, oder zu der so gen. offenen Observation u.a. Urteil der Kammer vom 14.02.2013 - 4 K 1115/12 -, juris).“

Für Aufenthaltsverbote beziehungsweise Aufenthaltsanordnungen haben teilweise andere Länder, aber auch Mecklenburg-Vorpommern gesonderte Rechtsgrundlagen geschaffen (vergleiche vorstehender § 52a sowie bereits geltender § 67b). Mit Blick auf die Regelungssystematik des SOG M-V und zur Herstellung von Rechtssicherheit sollen mit der neuen Ermächtigungsnorm die Voraussetzungen der Meldeauflage konkretisiert werden. Auch die Anwendbarkeit der Maßnahme für den Bereich der Abwehr terroristischer Straftaten bei Vorliegen der Voraussetzungen des § 67a Absatz 1 lassen eine Regelung notwendig erscheinen (vergleiche Bundesverwaltungsgericht a. a. O. Randnummer 34, juris). Zur Herstellung von Rechtssicherheit wurde von Rheinland-Pfalz ebenfalls eine Regelung in § 12a des Polizei- und Ordnungsbehördengesetzes geschaffen. Hessen verfügt mit § 30a des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung über eine Norm zur Meldeauflage. Auch in Bayern wurde mit Artikel 16 Absatz 2 Satz 2 des Gesetzes über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei eine Regelung zur Meldeauflage geschaffen. Auch das Land Niedersachsen plant eine Regelung zur Meldeauflage (siehe Drucksache 18/850 des Niedersächsischen Landtages, Seite 4, geplanter § 16a).

Nach Absatz 1 ist nunmehr ausschließlich die Polizei zum Erlass von Meldeauflagen gegenüber einer Person befugt, 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, an bestimmten Tagen zu bestimmten Zeiten bei einer bestimmten Polizeidienststelle zu erscheinen. Dadurch soll verhindert werden, dass die Verantwortlichen an gewalttätigen Auseinandersetzungen am Veranstaltungsort teilnehmen. Nicht maßgeblich ist dabei, 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 Absatz 1 des Grundgesetzes und in das Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes ein. Zudem wird die verantwortliche Person regelmäßig in ihrer Freizügigkeit gemäß Artikel 11 Absatz 1 des Grundgesetzes eingeschränkt. Meldeauflagen sind deshalb nur gerechtfertigt, wenn Tatsachen die Annahme der Begehung von Straftaten rechtfertigen. 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. Da es sich jedoch nur um eine Freiheitsbeschränkung und nicht um eine Freiheitsentziehung im Sinne des Artikels 104 Absatz 1 und 2 des Grundgesetzes handelt, ist es verfassungsrechtlich nicht geboten, die erstmalige Anordnung unter einen Richtervorbehalt zu stellen (siehe hierzu ergänzend auch die Ausführungen zu § 52a Absatz 2). Ein Richtervorbehalt wird – wie auch in den §§ 52a und 67b – für den Fall der Anordnungsverlängerung in Absatz 5 normiert.

Da die Tatsachen zum Erlass einer Meldeauflage grundsätzlich auf polizeilichen Erkenntnissen beruhen, zum Beispiel solchen aus der in das polizeiliche Informationssystem einbezogenen Verbunddatei „Gewalttäter Sport“, in der Täterinnen und Täter gespeichert werden, die durch Gewaltstraftaten im Zusammenhang mit sportlichen Ereignissen in Erscheinung getreten sind, sollen künftig Meldeauflagen nur von der Polizei angeordnet werden.

Hinzu kommt, dass sich die betroffenen Personen ohnehin auf einer Polizeidienststelle zu melden haben, da in der Praxis die Meldepflicht oftmals an Wochenenden zu erfüllen ist und eine Kontrolle der betroffenen Personen insoweit durch die Polizei erfolgt.

Nach Satz 2 können Meldeauflagen auch unter den Voraussetzungen des § 67a Absatz 1 zur Verhütung terroristischer Straftaten angeordnet werden. Die Meldeauflage kann damit gleichsam als flankierende Maßnahme zur Kontrolle von angeordneten Aufenthaltsverboten nach § 67b dienen.

Satz 3 gibt der Polizei aus Gründen der Verhältnismäßigkeit die Möglichkeit, mit Zustimmung der betroffenen Person auch eine inländische Polizeidienststelle außerhalb des Wohnsitzes oder ständigen Aufenthaltsortes der betroffenen Person zu bestimmen, sofern damit der Zweck der Meldeauflage oder anderer in diesem Zusammenhang angeordneter Maßnahmen nicht gefährdet wird. Innerhalb der Grenzen der Amtshilfe kann sich die Polizeidienststelle auch außerhalb Mecklenburg-Vorpommerns befinden. Damit kann der betroffenen Person zum Beispiel ermöglicht werden, zu verreisen, wenn sich die Annahme einer Straftatenbegehung auf ein lokal begrenztes Ereignis bezieht und die Erfüllung der Meldepflicht an anderer Stelle gleich geeignet ist, die Begehung solcher Straftaten zu verhindern. Eine Verpflichtung der Polizei, einem Wunsch der betroffenen Person hinsichtlich der Bestimmung der Polizeidienststelle nachzukommen, besteht grundsätzlich nicht. Die Polizei hat dies jedoch im Rahmen ihres Ermessens zu berücksichtigen.

Die Absätze 2 bis 5 regeln weitgehend entsprechend der Vorschrift zu Aufenthalts- und Betretungsverboten die Anordnungsbefugnis, das Verfahren und die Höchstdauer der Maßnahme.

In Absatz 4 wird ausdrücklich darauf verwiesen, dass die Meldeauflage keine unzumutbaren Auswirkungen auf die Lebensführung der betroffenen Person haben darf, wobei jedoch insbesondere die Art und Schwere der zu verhütenden Straftat besonders zu berücksichtigen sind. Die Norm ermöglicht zwar grundsätzlich auch, der betroffenen Person eine engmaschige Meldepflicht aufzuerlegen, allerdings dürfte es in der Regel nicht erforderlich sein, mehr als zwei Meldungen an den jeweiligen Tagen anzuordnen.

Die in Absatz 5 festgelegte Frist von 3 Monaten erlaubt der Polizei auch eine längerfristige Anordnung, etwa wenn sich aus dem Spielplan für Fußballveranstaltungen eine Reihe von Risikospielen ergibt und die vorliegenden Erkenntnisse die Gefahr begründen, dass die betroffene Person bei jedem dieser Spiele Straftaten begehen könnte. Für den besonderen Bereich der polizeilichen Abwehr terroristischer Gefahren entspricht die Höchstfrist den Fristen in der Regelung zur elektronischen Aufenthaltsüberwachung nach § 67a und der zur Aufenthaltsanordnung nach § 67b. Im Falle der gerichtlichen Anordnung bei Verlängerung der Maßnahme trifft hier das Gericht unabhängig von den Gründen der vorherigen behördlichen Anordnung eine eigenständige neue Entscheidung in der Sache.

Absatz 6 trifft in Anlehnung an § 67b Absatz 5 eine Vorrangregelung für eine Meldeauflage, die der Verhütung einer terroristischen Straftat dient. Diese geht anderweitigen Meldeauflagen, aber auch Aufenthaltsanordnungen außerhalb der Verhütung terroristischen Straftaten (siehe § 52a) vor, wenn diese ihr entgegenstehen. Die verdrängten Maßnahmen leben jedoch im Falle des Ablaufs der Meldeauflage nach Absatz 1 Satz 2 wieder auf, sofern sie nicht bereits beendet sind.

§ 53 (Durchsuchung von Personen und Verfahren)

Die Bezeichnung des § 53 wird geändert, da zum einen der Absatz 4 zur Untersuchung von Personen aus der Regelung herausgelöst und mit § 54 als gesonderte Norm verortet wird. Das bisher in § 54 geregelte Verfahren bei der Durchsuchung von Personen wird nun vollständig in § 53 integriert. Damit wird in § 53 eine Norm geschaffen, die die Durchsuchung von Personen und auch das diesbezügliche Verfahren in einer Norm zusammenfasst.

In Absatz 1 Nummer 1 erfolgt eine sprachliche Anpassung zur Harmonisierung der Regelungslage durch die Aufnahme der klarstellenden Formulierung „die Annahme rechtfertigen“. Im Übrigen wird der bisher geltende Absatz 1 unverändert übernommen.

Die bisherigen Absätze 2 und 3 werden beibehalten, wobei in Absatz 3 die sprachliche Gleichstellung vollzogen wird.

Der bisherige Regelungsinhalt von Absatz 4 wird neu in § 54 verortet.

Die Absätze 4 und 5 entsprechen - ungeachtet der vollzogenen sprachlichen Gleichstellung - inhaltlich vollständig den aus § 54 herausgelösten Verfahrensregelungen bei Durchsuchungen von Personen. Zusätzlich wird bestimmt, dass bei berechtigtem Interesse dem Wunsch der zu durchsuchenden Person, die Durchsuchung einer Person oder einer Ärztin oder einem Arzt bestimmten Geschlechts zu übertragen, entsprochen werden soll. Die zu durchsuchende Person ist auf diese Regelung hinzuweisen. Damit wird den individuellen Befindlichkeiten der zu durchsuchenden Person Rechnung getragen, für die im Einzelfall die Durchführung der Durchsuchung durch eine Person des von ihr bestimmten Geschlechts am wenigsten schamverletzend ist. Das Wahlrecht hinsichtlich des Geschlechts der Durchsuchenden gilt zudem nur bei berechtigtem Interesse. Ein solches Interesse kann zum Beispiel vorliegen, wenn die Person zum Personenstand „divers“ zählt (siehe hierzu auch Entscheidung des Bundesverfassungsgerichtes vom 10. Oktober 2017 - 1 BvR 2019/16). Aufgrund der ergänzten Regelung ist in der übernommenen Verfahrensregelung aus § 54 Absatz 2 Satz 2 nunmehr zu bestimmen, dass Satz 1 und 2 nicht gelten, wenn die sofortige Durchsuchung zum Schutz gegen eine im einzelnen Falle bevorstehende Gefahr für Leib oder Leben erforderlich ist.

§ 54 (Untersuchung von Personen und Verfahren)

Durch die Überführung der bisherigen Regelungen in § 54 in die Absätze 4 und 5 des § 53 enthält § 54 zukünftig die Befugnis zur Untersuchung von Personen, die vorher in § 53 Absatz 4 verortet war.

In Absatz 1 und Absatz 4 werden die Regelung aus dem bisher geltenden § 53 Absatz 4 übernommen und sprachlich an die im Gesetz enthaltenen Begrifflichkeiten angepasst. Es wird zudem die sprachliche Gleichstellung vollzogen. Eine Erweiterung der Befugnis erfolgt durch die Änderungen nicht. Jedoch wird zusätzlich bestimmt, dass bei der Untersuchung, die ausschließlich durch eine Ärztin oder einen Arzt durchgeführt werden darf, die Regelungen in § 53 Absatz 5 Satz 2 (Wahlrecht hinsichtlich des Geschlechts der untersuchenden Person; siehe Begründung zu § 53 Absatz 5) und § 53 Absatz 5 Satz 3 (Eilfallregelung) insoweit entsprechend gelten. Anzumerken ist, dass die bisher in der Befugnisnorm enthaltenen Festlegungen zur gerichtlichen Zuständigkeit und zum Verfahren aufgrund des eingefügten § 25b entbehrlich sind.

Neu aufgenommen werden in die Untersuchungsbefugnis die Absätze 2 und 3. In ihnen wird das Anordnungsverfahren konkreter ausgestaltet. Die Maßnahme bedarf - wie bisher auch - der richterlichen Anordnung außer in Fällen von Gefahr im Verzug. Es wird - wie in anderen Anordnungsnormen des Gesetzes - nun zusätzlich gesetzlich bestimmt, dass der Antrag an das Gericht von der Leitung der zuständigen Polizeibehörde oder von der Behördenleitung besonders beauftragte Beamtinnen oder Beamte zu stellen ist. Es wird der Inhalt des Antrages festgelegt und für den Fall von Gefahr im Verzug bestimmt, dass § 25b hinsichtlich der gerichtlichen Zuständigkeit und des Verfahrens gilt. Damit wird klargestellt, dass sich das Verfahren nicht nach den Vorschriften über die allgemeine Verwaltungsgerichtsbarkeit richtet, wenn die betroffene Person vor erfolgter Einholung einer richterlichen Entscheidung durch die anordnende Behörde den Rechtsweg beschreitet. Es wird zudem festgelegt, dass eine richterliche Entscheidung unverzüglich nachzuholen ist. Die Einschränkung des Absatzes 2 Satz 2 Nummer 1 („soweit möglich“) resultiert aus dem Umstand, dass in der Praxis zum Beispiel keine Anschrift der Person bekannt sein kann.

Dass die Polizei eine nachträgliche richterliche Entscheidung herbeiführen muss, wenn sie die Maßnahme wegen Gefahr im Verzug selbst angeordnet hat, wird im Gesetz vor folgendem Hintergrund neu verankert:

Das Landesverfassungsgericht Sachsen-Anhalt hat in seinem Urteil vom 11. November 2014, Aktenzeichen: LVG 9/13, einzelne Regelungen des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt als verfassungswidrig beanstandet. Gegenstand des Verfahrens waren verschiedene Vorschriften, die im Jahr 2013 mit dem Vierten Änderungsgesetz geändert oder neu in das Gesetz eingefügt worden waren. Dies betraf unter anderem auch die Regelung zur Untersuchung von Personen (vergleiche § 41 Absatz 6 des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt in der im Jahr 2013 geltenden Fassung). Diese Regelung war mit § 53 Absatz 4 des Sicherheits- und Ordnungsgesetzes des Landes Mecklenburg-Vorpommern vergleichbar. Das Landesverfassungsgericht Sachsen-Anhalt entschied, dass die normierte Ermächtigung zur Anordnung von Untersuchungspflichten gegenüber Personen, durch die möglicherweise ein besonders gefährlicher Krankheitserreger auf andere Personen übertragen wurde, grundsätzlich mit der Verfassung vereinbar sei. Verfassungswidrig aus Gründen der Verhältnismäßigkeit sei jedoch die in der Regelung vorgesehene Ausnahme vom Richtervorbehalt. Die alleinige Entscheidungsbefugnis der Polizei bei „Gefahr im Verzuge“ wird nach Auffassung des Landesverfassungsgericht Sachsen-Anhalt „*der Bedeutung des Grundrechtseingriffs nicht gerecht, der zumindest eine zwingende nachträglich richterliche Prüfung erforderlich macht, …*“ (vergleiche Seite 39 Nummer 2.6.4. a. a. O.).

Die Angaben, die die schriftliche Anordnung enthalten muss, sind in Absatz 3 festgelegt. Im Eilfall darf die Anordnung ausnahmsweise nachträglich dokumentiert werden, wenn die Zeit, die eine schriftliche Anordnung erfordert, mit Blick auf die bestehende Gefahr nicht mehr abgewartet werden kann.

Absatz 4 entspricht inhaltlich der Regelung im letzten Satz des bisherigen § 53 Absatz 4.

§ 55 (Gewahrsam von Personen)

§ 55 wird mit folgenden Änderungen übernommen:

In Absatz 1 Nummer 5 wird eine Regelungserweiterung vorgenommen. Danach kann eine Person - zusätzlich zu dem bisher aufgeführten Fall des § 52 - auch in Gewahrsam genommen werden, wenn dies unerlässlich ist, um eine Maßnahme nach § 52a durchzusetzen. Die Regelung ist insofern neu, als dass in den § 52a nicht nur die Regelungslage aus dem derzeit geltenden § 52 Absatz 3 übernommen und geändert wird, sondern in § 52a insgesamt neue Regelungen zur Anordnung von Aufenthalts- und Betretungsverboten geschaffen werden. Darüber hinaus werden in die Nummer 5 auch die §§ 52b, 67a und 67b aufgenommen. Damit können Personen in Gewahrsam genommen werden, soweit es zur Durchsetzung der Anordnung einer Meldeauflage (§ 52b) oder auch zur Durchsetzung der am 5. April 2018 in Kraft getretenen Maßnahmen der elektronischen Aufenthaltsüberwachung (§ 67a) und Aufenthaltsanordnung (§ 67b) unerlässlich ist.

Im Übrigen wird die Regelungslage in Absatz 1 beibehalten.

Der bisher geltende Absatz 2 wird unverändert übernommen.

Die Regelung in Absatz 3 wird übernommen und ergänzt. So wird die Regelung auch auf Personen erstreckt, die aus dem Vollzug von einer Jugendstrafe entwichen sind oder sich sonst ohne Erlaubnis außerhalb der Jugendanstalt oder Jugendarrestanstalt aufhalten. Die bisher erfolgte Bezugnahme auf die §§ 129 bis 138 des Strafvollzugsgesetzes ist durch die Bezugnahme auf die §§ 63, 64 oder 66 des Strafgesetzbuches zu ersetzen. Damit werden die Fälle der Unterbringung in einem psychiatrischen Krankenhaus (§ 63), der Unterbringung in einer Entziehungsanstalt (§ 64) und der Unterbringung in der Sicherungsverwahrung (§ 66) erfasst.

Die bisher geltenden Absätze 4 und 5 werden inhaltlich unverändert übernommen. In Absatz 4 wird ausschließlich die sprachliche Gleichstellung vollzogen.

§ 56 (Verfahren bei amtlichem Gewahrsam)

Die bisher geltenden Absätze 1 bis 4 werden inhaltlich unverändert übernommen. In Absatz 2 wird ausschließlich die sprachliche Gleichstellung vollzogen und in Absatz 3 wird die getrennte Unterbringung nicht mehr auf Männer und Frauen bezogen, sondern geschlechtsneutral formuliert.

Die Übernahme der Absätzen 5 und 6 erfolgt mit folgenden Änderungen:

In Absatz 5 wird der bisherige Satz 1 dahingehend präzisiert, dass die Polizei, die eine Person in Gewahrsam nimmt, die richterliche Entscheidung über die Zulässigkeit und Fortdauer des Gewahrsams unter Angabe des Namens der betroffenen Person und deren Anschrift, der beabsichtigten Gewahrsamsdauer, des Sachverhalts und der Begründung unverzüglich herbeizuführen hat. Die Regelung wird daher präzisiert und an andere Regelungen im Gesetz, die eine richterliche Entscheidung vorsehen, angepasst. Die Ausnahmeregelung in Satz 2 wird inhaltlich unverändert übernommen.

Satz 3 wird übernommen und ebenfalls präzisiert. Bestimmt wird, dass die richterliche Entscheidung schriftlich zu erheben hat und sie die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift, die Art und höchstzulässige Dauer des Gewahrsams und auch die Gründe zu enthalten hat. Die Einschränkung „soweit möglich“ resultiert aus dem Umstand, dass in der Praxis zum Beispiel keine Anschrift der Person bekannt sein kann.

Die bisher geltende Regelung, dass der Gewahrsam im Falle des § 55 Absatz 1 Nummer 2 zehn Tage und in den übrigen Fällen drei Tage nicht überschreiten darf, soweit gesetzlich nichts anderes bestimmt, bleibt unverändert bestehen. Dem Vorgehen in einigen anderen Bundesländer den Präventivgewahrsam auf mehrere Wochen oder Monate auszudehnen, wird nicht gefolgt.

Mit Absatz 5 Satz 4 wird in Abweichung von § 25b die Zuständigkeit für die gerichtliche Entscheidung neu bestimmt. Es wird nunmehr aus polizeipraktischen Gründen das Amtsgericht, in dessen Bezirk der Gewahrsam vollzogen wird, für zuständig erklärt.

Absatz 5 Satz 5 bestimmt nach wie vor, dass für das Verfahren die Vorschriften über das Verfahren in Freiheitsentziehungssachen nach dem Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend gelten. Satz 5 weicht damit ebenfalls von § 25b ab und stellt zu diesem eine Sonderregelung dar.

Mit Absatz 5 Satz 6 bis 9 werden Regelungen für den Fall neu in das Gesetz aufgenommen, dass eine Anhörung der vom Gewahrsam betroffenen Person durch das Gericht beispielsweise aufgrund übermäßigem Alkohol- oder Drogenkonsums nicht möglich ist. Liegt so ein Fall vor, wird die richterliche Entscheidung mit Erlass wirksam und bedarf hierzu nicht der Bekanntgabe an die in Gewahrsam genommene Person. Dauert die Freiheitsentziehung länger als bis zum Ende des Tages nach dem Ergreifen, ist in den Fällen, in denen keine Anhörung erfolgte, unverzüglich eine erneute richterliche Entscheidung herbeizuführen. Ist eine Anhörung hierbei nicht möglich, hat sich das Gericht einen persönlichen Eindruck von der in Gewahrsam genommenen Person zu verschaffen.

Mit Satz 10 erfolgt aufgrund bestehender Unsicherheiten in der gerichtlichen Praxis zudem die Klarstellung, dass für die Gerichtskosten soweit nichts anderes bestimmt ist, die Vorschriften über die Kostenerhebung in der Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend gelten.

In Absatz 6 wird der Gesetzesanwender nun zusätzlich auf den Vollstreckungsplan des Landes Mecklenburg-Vorpommern verwiesen, da dieser die zuständige Justizvollzugsanstalt für den Vollzug des Gewahrsams nach § 55 Absatz 1 im Wege der Amtshilfe bestimmt. Die Bezugnahme auf die genannten Regelungen des Gesetzes über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung (Strafvollzugsgesetz des Bundes) bleiben auch nach dem Inkrafttreten des Strafvollzugsgesetzes Mecklenburg-Vorpommern weiter anwendbar. Denn ausweislich der amtlichen Begründung zum Strafvollzugsgesetz Mecklenburg-Vorpommern heißt es zum Anwendungsbereich in § 1 (vergleiche Seite 68 der Drucksache 6/1337):

„Die Gesetzgebungsbefugnis für den Strafvollzug liegt seit dem 1. September 2006 bei den Ländern. Das Strafvollzugsgesetz M-V bezieht auch den Strafarrest ein, der in Anstalten vollzogen wird. Für den Vollzug von Ordnungs-, Sicherungs-, Zwangs- und Erzwingungshaft hat weiterhin der Bund die Gesetzgebungszuständigkeit, sodass die §§ 97, 109 bis 121 und 171 bis 175 des Strafvollzugsgesetzes des Bundes fortgelten.“

Auch wenn in dieser Aufzählung § 178 Absatz 3 des Strafvollzugsgesetzes des Bundes nicht ausdrücklich genannt ist, gilt auch diese Norm in Ermangelung ländereigener Gesetzgebungskompetenz für die Ordnungs-, Sicherungs-, Zwangs- und Erzwingungshaft ebenfalls entsprechend weiter.

Für das „Gesetz über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung“ des Bundes wird aber die amtliche Kurzbezeichnung „Strafvollzugsgesetz“ in Absatz 6 übernommen.

§ 57 (Durchsuchung von Sachen)

Der bisher geltende Absatz 1 Satz 1 bedarf aufgrund der neu aufgenommenen speziellen Durchsuchungsbefugnisse in den §§ 33c Absatz 5, 33d Absatz 3 Satz 3 und 35 Absatz 2 Satz 2 Nummer 2 einer Anpassung, indem diese gesondert geregelten Durchsuchungsbefugnisse dort aufgeführt werden. Eine inhaltliche Änderung wird dadurch nicht bewirkt.

Zudem erfolgt in den Nummern 2, 3 und 5 eine sprachliche Anpassung zur Harmonisierung der Regelungslage durch die Aufnahme der klarstellenden Formulierung „die Annahme rechtfertigen“.

In Anlehnung an § 110 Absatz 3 der Strafprozessordnung (siehe hierzu auch die Begründung in der Drucksache des Deutschen Bundestages 16/5846, Seite 63) wird in Absatz 2 zum Zwecke der Gefahrenabwehr eine ausdrückliche, rechtsklare Regelung geschaffen, dass die Befugnis zur Durchsuchung von Sachen in § 57 Absatz 1 auch die Durchsuchung von Datenbeständen erfasst.

Zum einen wird klargestellt, dass sich eine vom Grundsatz her offene Durchsuchungsmaßnahme unter den Voraussetzungen nach Absatz 1 auch auf elektronische Speichermedien beziehen darf. Zum anderen wird der Zugriff auch auf vom primären Durchsuchungsobjekt aus verfügbare, aber dort selbst nicht unmittelbar gespeicherte Daten geregelt. Die Maßnahme darf jedoch nur durchgeführt werden, wenn die Erfüllung der Aufgabe nach diesem Gesetz auf andere Weise aussichtslos oder wesentlich erschwert wäre. Entsprechend dem Stand der Technik ist damit auch der Zugriff auf von der benutzten Endeinrichtung der betroffenen Person entfernte Speicherorte zulässig. Dies wird deshalb so geregelt, weil es keinen Unterschied machen kann, ob sich die zu durchsuchenden Inhalte auf lokalen oder über Netzwerkverbindungen, etwa auf einer serverbasierten Cloud, erreichbaren Speichermedien befinden. Das Bundesverfassungsgericht hat in seiner Entscheidung zum Bundeskriminalamtgesetz vom 20. April 2016 den Zugriff auf vernetzte fremde Computer (etwa in Form von Cloud-Diensten) als grundsätzlich zulässig erachtet (vergleiche hierzu Randnummern 209 f im Zusammenhang mit der Online-Durchsuchung nach dem bisher geltenden § 20k des Bundeskriminalamtgesetzes).

In Abgrenzung zu einfachen Sichtungen auf der Grundlage etwa des § 27 einerseits und einer Online-Durchsuchung nach § 33c andererseits, handelt es sich bei Durchsuchungsmaßnahmen nach dem neuen § 57 Absatz 2 in Verbindung mit Absatz 1 vom Grundsatz her um offene Maßnahmen, die – anders als Maßnahmen nach § 33c – ohne verdeckte technische Infiltration erfolgen.

Satz 2 stellt klar, dass die Durchsuchungsmaßnahme auch durchgeführt werden darf, wenn Dritte unvermeidbar betroffen sind. Satz 3 bringt zum Ausdruck, dass sich eine weitere Verarbeitung personenbezogener Daten, die über die im Rahmen der Durchsuchung erfolgte bloße Kenntnisnahme hinausgeht, nach gesonderten Vorschriften richtet, wobei je nach Lage des Falls etwa die ebenfalls nunmehr speziell geregelte Sicherstellung personenbezogener Daten nach § 61 Absatz 1 oder eine Datenerhebung nach § 27ff in Betracht kommen kann. Letztlich sind die bezeichneten Abgrenzungen stets nach den Umständen des Einzelfalls zu treffen. Die anderweitigen, je nach den Umständen des Einzelfalles einschlägigen Regelungen hinsichtlich der Datenverarbeitung im SOG M-V - wie insbesondere der Eingriff in informationstechnische Systeme nach § 33c oder Telekommunikationsüberwachungen nach § 33d - bleiben von der klarstellenden Regelung in § 57 Absatz 2 unberührt.

§ 58 (Verfahren bei der Durchsuchung von Sachen)

§ 58 wird unter Vollzug der sprachlichen Gleichstellung übernommen und dahingehend angepasst, dass die Worte „vor Ort“ eingefügt werden und die Regelung in zwei Absätze aufgeteilt wird. Aufgrund des in § 57 neu eingefügten Absatzes 2 wird damit klargestellt, dass ein Anwesenheitsrecht der betroffenen Person nur dann besteht, wenn Sachen noch vor Ort, also im Verfügungsbereich der betroffenen Person durchsucht werden. Werden Speichermedien sichergestellt und (gegebenenfalls unter Verwendung spezieller Techniken) erst bei der Polizei oder beauftragten Drittunternehmen umfassend durchsucht, kann ein Anwesenheitsrecht selbstredend nicht bestehen.

Die nach dem bisherigen § 58 Satz 2 nur auf Verlangen zu erteilende Bescheinigung über die erfolgte Durchsuchung wird im neuen Absatz 2 nunmehr so ausgestaltet, dass der Gewahrsamsinhaberin oder dem Gewahrsamsinhaber eine Bescheinigung über die Durchsuchung und ihren Grund zu erteilen ist. Nur im Falle ihrer oder seiner Anwesenheit erfolgt die Erteilung der Bescheinigung nur dann, wenn sie oder er es verlangt. Durch diese neue Regelungslage wird gewährleistet, dass die Gewahrsamsinhaberin oder der Gewahrsamsinhaber in Fällen, in denen sie oder er bei der Durchsuchung abwesend ist - wie etwa vorstehend ausgeführt - von der Durchsuchung Kenntnis erlangt. Die Regelung in Absatz 2 gilt unabhängig davon, ob die Durchsuchung vor Ort oder etwa zum Beispiel in einer Polizeidienststelle erfolgt.

§ 59 (Betreten und Durchsuchung von Räumen)

Absatz 1 wird unter Vollzug der sprachlichen Gleichstellung und Absatz 2 wird unverändert übernommen.

Der bisher geltende Absatz 3 wird dahingehend angepasst, dass die bislang in Absatz 6 enthaltene Bestimmung, dass die Durchsuchung ausschließlich Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte vornehmen dürfen, direkt in Absatz 3 übernommen wird.

Zudem erfolgt eine sprachliche Anpassung in Nummer 1 und 2 zur Harmonisierung der Regelungslage durch die Aufnahme der klarstellenden Formulierung „die Annahme rechtfertigen“.

Ebenso wie in Absatz 3 wird in den Absatz 4 Satz 1 direkt die bisher in Absatz 6 enthaltene Bestimmung, dass die Durchsuchung ausschließlich Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte vornehmen dürfen, übernommen. Zusätzlich wird unter Beachtung der Entscheidung des Bundesverfassungsgerichtes vom 12. März 2019 - Aktenzeichen 2 BvR 675/14 - der zur Bestimmung der Nachtzeit in Klammern enthaltene Verweis auf § 104 Absatz 3 der Strafprozessordnung durch die konkrete Bestimmung der Nachtzeit (umfasst die Stunden von 21 bis 6 Uhr) ersetzt. Zudem erfolgt eine sprachliche Anpassung in Satz 2 Nummer 2 durch die Aufnahme der klarstellenden Formulierung „die Annahme rechtfertigen“.

Die bisher geltende Regelung in Absatz 5 Satz 1 zur richterlichen Anordnung von Durchsuchungen von Wohn- und Geschäftsräumen - außer bei Gefahr im Verzug -wird beibehalten. Es wird jedoch zusätzlich bestimmt, dass der Antrag an das Gericht durch die Leitung der zuständigen Polizeibehörde oder eine von ihr besonders beauftragte Beamtin oder einen von ihr besonders beauftragten Beamten zu stellen ist. Mit Satz 2 wird - wie auch in anderen Regelungen - festgelegt, welche Angaben der Antrag zu enthalten hat. Die Einschränkung der Nummer 1 „soweit möglich“ resultiert aus dem Umstand, dass in der Praxis zum Beispiel keine Wohnanschrift einer Person bekannt sein kann.

Soweit eine Anordnung durch die Polizei im Eilfall erfolgte, wird bestimmt, dass § 25b entsprechend gilt. Damit wird klargestellt, dass sich das Verfahren nicht nach den Vorschriften über die allgemeine Verwaltungsgerichtsbarkeit richtet, wenn die betroffene Person vor erfolgter Einholung einer richterlichen Entscheidung durch die anordnende Behörde den Rechtsweg beschreitet. Es wird darüber hinaus festgelegt, dass die richterliche Entscheidung in Fällen polizeilicher Anordnung unverzüglich nachzuholen ist. Diese Bestimmung ist neu und wird aufgrund der von der Durchsuchung betroffenen besonders sensiblen Bereiche in das Gesetz aufgenommen.

Der bisherige Absatz 6 konnte aufgrund der direkten Aufnahme der Regelung in den Absätzen 3 und 4 entfallen. In Absatz 6 Satz 1 und 2 wird aber neu aufgenommen, welche Angaben die schriftliche Anordnung nach Absatz 5 zu enthalten hat. Für Eilfälle wird ausnahmsweise die nachträgliche Dokumentation der Anordnung zugelassen. Satz 3 und 4 bestimmt abweichend von § 25b die gerichtliche Zuständigkeit. Für die Anordnung ist das Amtsgericht zuständig, in dessen Bezirk die zu durchsuchenden Räume liegen; für das Verfahren ist § 25b jedoch anzuwenden.

§ 60 (Verfahren bei der Durchsuchung von Räumen)

Der bisher geltende § 60 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 61 (Sicherstellung von Sachen)

Der bisher geltende § 61 wird mit folgenden Anpassungen und Ergänzungen übernommen:

Absatz 1 wird unter Vollzug der sprachlichen Gleichstellung vollumfänglich übernommen und um Regelungen zur Sicherstellung von Daten ergänzt.

Klargestellt wird mit den nach Satz 2 aufgenommenen Bestimmungen, dass die Sicherstellungsbefugnis nach Satz 1 auch für Daten auf einem elektronischen Speichermedium und für Daten auf von diesem räumlich getrennten Speichermedien, soweit auf sie vom elektronischen Speichermedium aus zugegriffen werden kann, gilt (vergleiche hierzu auch Ausführungen zu § 57). Es wird zudem mit Satz 3 zugelassen, dass der weitere Zugriff auf Daten ausgeschlossen werden kann, wenn andernfalls die Abwehr der Gefahr, der Schutz vor Verlust oder die Verhinderung der Verwendung aussichtslos oder wesentlich erschwert wäre.

Damit können unter Beachtung der Voraussetzungen in Satz 1 zukünftig etwa die Sicherstellung und die Entziehung von Zugangsdaten außerhalb eines laufenden Telekommunikationsvorgangs erfolgen (und damit gegenüber § 33c und § 33d Absatz 3 erleichterten Voraussetzungen). Auch Sicherstellungen von Daten, die sich an von der benutzten Endeinrichtung der betroffenen Person entfernten Speicherorten - wie etwa auf einer serverbasierten Cloud - befinden, wären zulässig. Eine derartige Sicherstellung erfolgt entsprechend der Konzeption der Sicherstellung im SOG M-V als grundsätzlich offene Maßnahme, sodass die betroffene Person Kenntnis von der Sicherstellungmaßnahme erhält (siehe § 62; vergleiche auch die Ausführungen zur grundsätzlich offenen Maßnahme der Durchsuchung von Datenbeständen in § 57 Absatz 2 gegenüber dem verdeckten Zugriff auf informationstechnische Systeme nach § 33c).

Zudem wird mit Satz 4 bestimmt, dass die sicherstellende Behörde die richterliche Bestätigung der Rechtmäßigkeit der Maßnahmen nach Satz 2 und 3 unverzüglich zu beantragen hat. Zusätzlich wird festgelegt, dass § 25b entsprechend gilt. Damit wird klargestellt, dass sich das Verfahren nicht nach den Vorschriften über die allgemeine Verwaltungsgerichtsbarkeit richtet, wenn die betroffene Person vor erfolgter Einholung einer richterlichen Entscheidung durch die anordnende Behörde den Rechtsweg beschreitet.

Ferner bestimmt Satz 5, dass Daten, die nach den §§ 26a und 26b nicht weiter verarbeitet werden dürfen oder für die Aufgabenerfüllung nicht mehr erforderlich sind, zu löschen sind. Die Pflicht gilt aber nicht für Daten, die zusammen mit dem Datenträger sichergestellt wurden, auf dem sie gespeichert sind. Im Übrigen wird insbesondere auf die Geltung der Regelungen zur Dokumentation (§ 46d), Protokollierung (§ 46e), Kennzeichnung (46g) und zur Sicherheit der Datenverarbeitung (§ 46i) verwiesen, die nach § 49a entsprechend anwendbar sind. Satz 6 bestimmt, dass die Regelungen in Absatz 3 und in den §§ 62, 63, 64 Absatz 4 hinsichtlich der Herausgabe, des Verfahrens, der Verwahrung und der Vernichtung unter Berücksichtigung der unkörperlichen Natur von Daten entsprechend gelten.

Absatz 2 wird neu in § 61 eingefügt. Danach erhält die Polizei die ausdrückliche Befugnis, Forderungen oder andere Vermögensrechte bis zu einer Dauer von sechs Monaten sicherzustellen, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass diese zur Begehung einer Straftat von erheblicher Bedeutung nach den § 49 oder einer terroristischen Straftat nach § 67c verwendet werden sollen. Im Rahmen dieser Befugnis kann die Polizei unbare Vermögenrechte wie Forderungen, elektronisches Geld und digitale Zahlungsmittel (beispielsweise Bitcoins) sicherstellen.

Die Aufnahme des Absatzes 2 erfolgt aufgrund einer Entscheidung des Bayerischen Verwaltungsgerichtshofs (siehe Urteil vom 23. Februar 2016 - 10 BV 14.2353). Dieser hat zum Fall eines zunächst als Bargeld nach der Strafprozessordnung sichergestellten, dann in die Landesjustizkasse eingezahlten und damit seit diesem Zeitpunkt nur noch als Buchgeld in Form eines Auszahlungsanspruchs fortbestehenden Geldbetrags entschieden, dass eine auf Sachen als körperliche Gegenstände bezogene Sicherstellung nicht in Betracht kommt. Rechtsvergleichend ist sowohl in § 33 Absatz 2 des Polizeigesetzes des Landes Baden-Württemberg als auch in Artikel 25 Absatz 2 des Gesetzes über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei bereits die Möglichkeit der Sicherstellung von Forderungen oder anderen Vermögensrechten durch Pfändung entsprechend den Vorschriften der Zivilprozessordnung enthalten. Auch das Land Niedersachsen plant eine Regelung zur Sicherstellung von Forderungen und anderen Vermögensrechten (siehe Drucksache 18/850 des Niedersächsischen Landtages, Seite 7, geplanter § 29a). Aufgrund des bestehenden rechtspraktischen Bedürfnisses der präventiv-polizeilichen Sicherstellung auch unbarer Vermögenswerte gilt es, eine explizite und zugleich den aktuellen Stand von Wirtschaft und Technik (insbesondere im Hinblick auf sogenannter Kryptowährungen) abbildende, zukunftsoffene Sicherstellungsregelung im SOG M-V zu schaffen.

Dem Landesgesetzgeber steht hierzu auch die entsprechende Gesetzgebungskompetenz zu. Es handelt sich um einen Unterfall der präventiv-polizeilichen Sicherstellung zur Gefahrenabwehr. Die Sicherstellung nach § 61 Absatz 1 ist unabhängig von einem strafrechtlichen Anfangsverdacht. Sie ist aufgrund der festgelegten Dauer von sechs Monaten nur von vorläufiger Natur. Sie ist zudem zwingend zu beenden, wenn die Gefahr entfallen ist. Kann eine Freigabe nach sechs Monaten nicht erfolgen, ohne dass die Voraussetzungen der Sicherstellung erneut eintreten, kann die Sicherstellung mit gerichtlicher Zustimmung um jeweils weitere sechs Monate verlängert werden (vergleiche hierzu weiter die Ausführungen zu Absatz 3).

Die normierte Sicherstellung in Absatz 2 darf auf Antrag der Leitung der Polizeibehörde durch Pfändung durch das Amtsgericht, in dessen Bezirk die Inhaberin oder der Inhaber der Forderungen oder Vermögensrechte ihren oder seinen Wohnsitz oder ständigen Aufenthalt hat, bewirkt werden. Die Vorschriften der Zivilprozessordnung über die Zwangsvollstreckung in Forderungen und andere Vermögensrechte werden für entsprechend anwendbar erklärt. Insbesondere aufgrund der Geltung der Formvorschriften der Zivilprozessordnung wird auch gewährleistet, dass die von der Maßnahme betroffenen Personen über den Umfang und die Gründe der Sicherstellung in Kenntnis gesetzt werden.

Absatz 3 übernimmt die Regelungen im bisher geltenden § 61 Absatz 2 unter Vollzug der sprachlichen Gleichstellung. Ihnen wird zusätzlich eine Bestimmung zur Herausgabe von sichergestellten Forderungen oder anderen Vermögensrechten angefügt. Soweit eine Herausgabe von sichergestellten Forderungen oder anderen Vermögensrechte ausgeschlossen ist, weil dadurch erneut die Voraussetzungen für eine Sicherstellung eintreten würden, kann deren Sicherstellung um jeweils weitere sechs Monate verlängert werden. Über die Verlängerung entscheidet auf Antrag der Leitung der Polizeibehörde, der insbesondere die Gründe für die Verlängerung enthalten muss, das Amtsgericht, in dessen Bezirk die Inhaberin oder der Inhaber ihren oder seinen Wohnsitz oder ständigen Aufenthalt hat. Die Zuständigkeit des Amtsgerichtes weicht somit von § 25b ab und stellt damit eine Sonderreglung dar. Auf diese Weise wird gewährleistet, dass eine Verlängerung der Sicherstellung über sechs Monate hinaus durch ein Gericht geprüft wird und so auf einer gerichtlichen Entscheidung beruht. Die Polizei selbst darf diese Entscheidung über die Verlängerung nicht treffen. Für das Verfahren ist § 25b jedoch zu beachten.

Hat das Amtsgericht entschieden, dass eine Verlängerung der Sicherstellung der Forderungen oder Vermögensrechte zulässig ist, so wird die Sicherstellung - wie in Absatz 2 bestimmt - durch Pfändung durch das Amtsgericht, in dessen Bezirk die Inhaberin oder der Inhaber der Forderungen oder Vermögensrechte ihren oder seinen Wohnsitz oder ständigen Aufenthalt hat, bewirkt. Die Vorschriften der Zivilprozessordnung über die Zwangsvollstreckung in Forderungen und andere Vermögensrechte sind gemäß Absatz 2 entsprechend anwendbar.

In den neuen Absatz 4 wird die Regelung des bisher geltenden Absatzes 3 unverändert übernommen.

§ 62 (Verfahren bei der Sicherstellung von Sachen)

Der bisher geltende § 62 wird - mit Ausnahme des Absatzes 4 Satz 2 - unter Vollzug der sprachlichen Gleichstellung übernommen.

In Absatz 4 Satz 2 bedürfen die Verweise zum Verfahren vor dem Amtsgericht zur Abnahme der eidesstattlichen Versicherung in die Normen der Zivilprozessordung einer Anpassung. In diesem Zusammenhang ist darauf hinzuweisen, dass die in § 25b enthalten Regelungen zur Zuständigkeit und zum gerichtlichen Verfahren damit nicht gelten.

§ 63 (Amtliche Verwahrung)

Der bisher geltende § 63 wird unter Vollzug der sprachlichen Gleichstellung und durch Änderung des Wortes „Dritten“ durch „Andere“, um einen Bezug zum dem in § 3 Absatz 4 definierten Dritten zu vermeiden, übernommen. Eine inhaltliche Änderung ist damit nicht verbunden.

§ 64 (Verwertung, Vernichtung)

Die bisher geltenden Absätze 1 und 2 werden unter Vollzug der sprachlichen Gleichstellung übernommen. In Absatz 2 wird aufgrund der Änderungen in § 61 zusätzlich bestimmt, dass bei der Verwertung von Datenträgern - soweit eine solche überhaupt in Betracht zu ziehen ist - sicherzustellen ist, dass zuvor personenbezogene Daten dem Stand der Technik entsprechend gelöscht wurden.

Der bisher geltende Absatz 3 wird ebenfalls übernommen. Er bedarf jedoch der Ergänzung. Denn bisher ist nicht geregelt, dass der Erlös aus einer Verwertung an die berechtigte Person herauszugeben ist. Diese Regelungslücke wird nun ergänzt. Darüber hinaus wird für den Fall, dass eine berechtigte Person nicht vorhanden oder nicht zu ermitteln ist, bestimmt, dass der Erlös in diesen Fällen nach den Vorschriften des Bürgerlichen Gesetzbuchs zu hinterlegen ist. Normiert wird auch, dass der Anspruch auf Herausgabe des Erlöses drei Jahre nach Ablauf des Jahres, in dem die Sache verwertet worden ist, erlischt. Ferner wird nun in Absatz 3 geregelt, dass die Kosten der Verwertung aus dem Erlös gedeckt werden können. Die in Absatz 3 erfolgten Ergänzungen weisen teilweise auch andere Landesgesetze (vergleiche etwa § 29 des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung, § 46 des Polizeigesetzes des Landes Nordrhein-Westfalen oder auch § 25 des Polizei- und Ordnungsbehördengesetzes des Landes Rheinland-Pfalz) auf.

Der bisher geltende Absatz 4 wird unverändert übernommen.

§ 65 (Verfahren bei der Wegnahme einer Person)

Der bisher geltende § 65 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 66 (Verfahren bei der Zwangsräumung)

§ 66 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 67 (Übertragung des Eigentums)

Der bisher geltende § 67 wird unter Vollziehung der sprachlichen Gleichstellung und Änderung des Wortes „Dritter“ in „Anderer“, um einen Bezug zum dem in § 3 Absatz 4 definierten Dritten zu vermeiden, übernommen. Eine inhaltliche Änderung ist damit nicht verbunden.

§ 67a (Elektronische Aufenthaltsüberwachung)

Der bisher geltende § 67a wird mit folgenden Änderungen in den Absätzen 1, 4, 5 und 7 übernommen:

Die Änderung des Begriffes „bestimmte Tatsachen“ in „Tatsachen“ in Absatz 1 erfolgt mit Blick auf den möglichst einheitlichen Sprachgebrauch des Gesetzes. Eine Änderung der Voraussetzungen ist damit nicht verbunden.

Die im bisher geltenden Absatz 4 enthaltenen Sätze 2 bis 4, die die Protokollierung und die Verwendung der Protokolldaten bestimmen, sind aufgrund der neu geschaffenen Protokollierungsnormen in den §§ 46e und 46f durch einen Verweis auf diese neuen Normen zu ersetzen. Der bisher geltende Satz 6 wird präziser gefasst und der darin zur Protokollierung enthaltene Verweis auf die Sätze 3 und 4 mit Blick auf die vorgenommenen Änderungen im Absatz 4 angepasst.

Absatz 5 wird mit der zusätzlichen Bestimmung übernommen, dass in den Fällen, in denen die Polizeibehörde die Maßnahme der elektronischen Aufenthaltsüberwachung wegen Gefahr im Verzug zunächst selbst gegen die betroffene Person anordnet, § 25b gilt. Da es sich hier um eine gegenüber der betroffenen Person offene polizeiliche Maßnahme handelt, wird so klargestellt, dass sich das Verfahren nicht nach den Vorschriften über die allgemeine Verwaltungsgerichtsbarkeit richtet, wenn die betroffene Person vor erfolgter Einholung einer richterlichen Entscheidung durch die anordnende Behörde den Rechtsweg beschreitet.

In Absatz 7 ist die Bestimmung zum gerichtlichen Verfahren aufgrund der Geltung des § 25b entbehrlich.

§ 67b (Aufenthaltsanordnung)

Der bisher geltende § 67b wird mit folgenden Änderungen übernommen:

Die Änderung des Begriffes „bestimmte Tatsachen“ in „Tatsachen“ in Absatz 1 erfolgt mit Blick auf den möglichst einheitlichen Sprachgebrauch des Gesetzes. Eine Änderung der Voraussetzungen ist damit nicht verbunden.

In Absatz 4 ist die Bestimmung zum gerichtlichen Verfahren aufgrund des neu eingefügten § 25b entbehrlich und wird daher gestrichen.

Absatz 5 Satz 2 wird angepasst, da das bisher in § 52 geregelte Aufenthalts- und Betretungsverbot nun in die neu aufgenommene Befugnis für die Anordnung eines Aufenthalts- und Betretungsverbots in § 52a integriert wird. Es wird nunmehr bestimmt, dass eine Aufenthaltsanordnung nach § 67b Absatz 1 einem Aufenthalts- und Betretungsverbot nach § 52a vorgeht, soweit sie sich entgegenstehen.

Aufgrund der neu aufgenommenen Befugnis zur Anordnung von Meldeauflagen in § 52b ist dieser Vorrang der Aufenthaltsanordnung nach § 67b Absatz 1 auch in Bezug auf eine nach § 52b Absatz 1 Satz 1 angeordnete Meldeauflage zu bestimmen. Dies erfolgt mit dem neuen Satz 3.

§ 67c (Terroristische Straftat)

Keine Änderung.

§ 67d (Strafvorschrift)

Keine Änderung.

§ 68 (Grundsatz)

Keine Änderung.

§ 69 (Verantwortlichkeit für das Verhalten von Personen)

Der bisher geltende § 69 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 70 (Verantwortlichkeit für Sachen)

Der bisher geltende § 70 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 70a (Unmittelbare Ausführung einer Maßnahme)

Der bisher geltende § 70a wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 71 (Inanspruchnahme des Nichtstörers)

Der bisher geltende § 71 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 72 (Entschädigungsanspruch des Nichtstörers

Der bisher geltende § 72 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 73 (Entschädigungsanspruch Unbeteiligter)

Der bisher geltende § 73 wird unter Vollzug der sprachlichen Gleichstellung übernommen. Zudem wird das Wort „Dritte“ in der Bezeichnung des § 73 und in der Regelung durch „Unbeteiligte“ ersetzt, um einen Bezug zum dem in § 3 Absatz 4 definierten Dritten zu vermeiden. Eine inhaltliche Änderung ist damit nicht verbunden.

§ 74 (Art, Inhalt und Umfang der Entschädigungsleistung)

Der bisher geltende § 74 wird unter Vollzug der sprachlichen Gleichstellung übernommen und in Absatz 3 wird das Wort „Dritte“ durch „Andere“ ersetzt, um einen Bezug zum dem in § 3 Absatz 4 definierten Dritten zu vermeiden. Eine inhaltliche Änderung ist damit nicht verbunden.

§ 75 (Entschädigungspflichtiger Rückgriff)

Der bisher geltende § 75 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 76 (Schadensersatzansprüche und Entschädigung aus der Verarbeitung von Daten)

Die bisherige Regelung in § 76 zu Schadensersatzansprüchen aus der Verarbeitung personenbezogener Daten wird neu gefasst. Die Neuregelung setzt Artikel 56 der Richtlinie (EU) 2016/680 um und orientiert sich an § 83 des Bundesdatenschutzgesetzes. Der Regelungsgehalt der Vorschrift entspricht zudem weitgehend dem § 27 des Landesdatenschutzgesetzes (in der vor dem 25. Mai 2018 geltenden Fassung), wobei jedoch eine Haftungsbeschränkung nach dessen Absätzen 3 und 4 nicht mehr den nunmehrigen europarechtlichen Vorgaben entspricht. Es bleibt wie bisher dabei, dass bei der automatisierten Verarbeitung eine verschuldensunabhängige Gefährdungshaftung der verantwortlichen Stelle beziehungsweise ihres Rechtsträgers besteht, während bei der nicht automatisierten Verarbeitung eine Exkulpationsmöglichkeit geregelt ist.

Eine umfassende einheitliche Regelung für alle Verarbeitungszwecke der Sicherheitsbehörden nach diesem Gesetz ist wegen der Abweichungen der Umsetzungsvoraussetzungen der Richtlinie (EU) 2016/680 vom Regelungsgehalt der Verordnung (EU) 2016/679 nicht möglich. Dies gilt insbesondere für die unterschiedlichen Vorgaben zur (direkten) Haftung des Auftragsverarbeiters. Soweit die Datenverarbeitung in den Anwendungsbereich der Verordnung (EU) 2016/679 fällt, gelten somit die Vorschriften zum Schadensersatz in deren Artikel 82. Dies schließt jedoch nicht aus, dass ein Auftragsverarbeiter - wie es Absatz 7 vorsieht - aus anderen Vorschriften schadensersatzpflichtig oder dem haftenden Verantwortlichen gegenüber selbst regresspflichtig ist.

§ 77 (Rechtsweg)

Keine Änderung.

§ 78 (Einschränkung von Grundrechten)

§ 78 wird übernommen und um das Recht auf Versammlungsfreiheit (Artikel 8 Absatz 1 des Grundgesetzes) als einschränkbares Grundrecht ergänzt. Diese Ergänzung erfolgt vor folgendem Hintergrund:

Das Bundesverfassungsgericht hat sich in seiner Entscheidung vom 18. Dezember 2018 - Aktenzeichen 1 BvR 2795/09 - (veröffentlicht vom Bundesverfassungsgericht mit seiner Pressemitteilung Nummer 9/2019 vom 5. Februar 2019) unter anderem mit der Ermächtigung zu automatisierten Kfz-Kennzeichenkontrollen an polizeilichen Kontrollstellen zur Verhinderung von versammlungsrechtlichen Straftaten oder zum Schutz von Versammlungen befasst. Es führt hierzu unter der Randnummer 62 aus:

„*Die Regelung der Identitätsfeststellung an polizeilichen Kontrollstellen zur Verhütung von versammlungsrechtlichen Straftaten sowie der Unterstützung solcher Kontrollen durch eine automatisierte Kennzeichenkontrolle setzt materiell voraus, dass konkrete Hinweise auf erhebliche Straftaten in Bezug auf eine konkrete Versammlung vorliegen und in örtlichem Bezug hierzu eine polizeiliche Kontrollstelle eingerichtet wurde.*

Da die Vorschrift folglich dazu ermächtigt, den Zugang zu Versammlungen zu kontrollieren, liegt in ihr ein Eingriff in Art. 8 Abs. 1 GG (vgl. BVerfG, Beschluss des Ersten Senats vom selben Tag - 1 BvR 142/15 -, Rn. 136). Ein solcher Eingriff unterliegt nach Art. 19 Abs. 1 Satz 2 GG in formeller Hinsicht dem Zitiergebot, dem das Hessische Gesetz über die öffentliche Sicherheit und Ordnung nicht genügt (vgl. § 10 HSOG, der Art. 8 GG nicht aufführt)."

Auch § 29 Absatz 1 Satz 2 sieht die Möglichkeit von Identitätsfeststellungen an polizeilichen Kontrollstellen zur Verhütung von versammlungsrechtlichen Straftaten vor. Auf diese Norm wird in der Befugnis zur Kfz-Kennzeichenerfassung und zum Kennzeichenabgleich (§ 43a) Bezug genommen, sodass im Land Mecklenburg-Vorpommern ebenfalls die Möglichkeit der Erfassung und des Abgleichs von Kennzeichen auch an einer polizeilichen Kontrollstelle, die den Zugang zu einer Versammlung kontrolliert, besteht (vergleiche hierzu Regelung in § 43a Absatz 1 Satz 1 Nummer 2). Da das Bundesverfassungsgericht darin einen (gerechtfertigten) Eingriff in Artikel 8 Absatz 1 des Grundgesetzes erblickt und damit einen Eingriff in das Recht auf Versammlungsfreiheit feststellt, ist insoweit das in Artikel 19 Absatz 1 Satz 2 des Grundgesetzes enthaltene Zitiergebot zu beachten. Das Recht auf Versammlungsfreiheit ist daher zusätzlich in § 78 als einschränkbares Grundrecht aufzunehmen. Auch andere Bundesländer haben in ihren Polizeigesetzen - schon vor der angeführten Entscheidung des Bundesverfassungsgerichtes - das Recht auf Versammlungsfreiheit als einschränkbares Grundrecht aufgenommen.

§ 79 (Grundsatz)

Keine Änderung.

§ 80 (Zulässigkeit des Vollzugs von Verwaltungsakten)

Keine Änderung.

§ 81 (Sofortiger Vollzug)

Der bisher geltende § 81 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 82 (Vollzugsbehörden)

Keine Änderung.

§ 82a (Vollzugshilfe)

Keine Änderung.

§ 82b Verfahren)

Keine Änderung.

§ 82c (Vollzugshilfe bei Freiheitsentziehung)

Der bisher geltende § 82c wird mit der Änderung übernommen, dass der in Absatz 3 enthaltene Verweis auf § 56 nun nicht mehr nur auf dessen Absätze 2 und 5, sondern vollumfänglich erfolgt. Durch die entsprechende Anwendung des § 56 gelangen nur diejenigen Vorschriften zur Anwendung, die sich auf den Fall der Vollzugshilfe bei Freiheitsentziehung übertragen lassen.

§ 83 (Pflichtige Person)

Der bisher geltende § 83 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 84 (Vollzug gegen den Rechtsnachfolger)

Keine Änderung.

§ 85 (Vollzug gegen Träger der öffentlichen Verwaltung)

Keine Änderung.

§ 86 (Zwangsmittel)

Keine Änderung.

§ 87 (Androhung von Zwangsmitteln)

Der bisher geltende § 87 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 88 (Zwangsgeld)

Der bisher geltende § 88 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 89 (Ersatzvornahme)

Der bisher geltende § 89 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 90 (Unmittelbarer Zwang)

Der bisher geltende § 90 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

.

§ 91 (Ersatzzwangshaft

Der bisher geltende § 91 wird unter Abänderung des Verweises in Absatz 2 übernommen. Zur Vollstreckung der Ersatzzwangshaft wird nun nicht mehr auf die §§ 904 bis 910 der Zivilprozessordnung, sondern auf die §§ 802g Absatz 1 Satz 2 und 3 sowie Absatz 2, 802h und 802i der Zivilprozessordnung verwiesen.

§ 92 (Einstellung des Vollzugs)

Der bisher geltende § 92 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 93 (Abgabe einer Erklärung)

Der bisher geltende § 93 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 94 (Anwendung der Vollzugsvorschriften aufgrund bundesrechtlicher Ermächtigungen)

Keine Änderung.

§ 95 (Anwendung der Vollzugsvorschriften auf öffentlich-rechtliche Verträge)

Der bisher geltende § 95 wird unter Aktualisierung der in Satz 1 genannten Gesetzesbezeichnung (jetzt Landesverwaltungsverfahrensgesetz) übernommen.

§ 96 (Sonstige Anwendung der Vollzugsvorschriften)

Keine Änderung.

§ 97 (Maßnahmen gegen Tiere)

Keine Änderung.

§ 98 (Einschränkung von Grundrechten)

Keine Änderung.

§ 99 (Rechtsbehelfe)

Keine Änderung.

§ 100 (aufgehoben)

Die Beibehaltung des bereits aufgehobenen und damit inhaltsleeren § 100 erfolgt zur Vermeidung einer kompletten Regelungsverschiebung.

§ 101 (Rechtliche Grundlagen)

Keine Änderung.

§ 102 (Begriffsbestimmung)

Keine Änderung.

§ 103 (Vollzugsbeamtinnen und Vollzugsbeamte)

Der bisher geltende § 103 wird unter Vollzug der sprachlichen Gleichstellung übernommen. In Absatz 2 Nummer 2 wird zudem zur Klarstellung das Wort „Verordnung“ durch das Wort „Rechtsverordnung“ ersetzt.

Die Regelung des Absatzes 3, nach der Vollzugsbeamtinnen und Vollzugsbeamte der Ämter und amtsfreien Gemeinden der Bestätigung durch die Kreisordnungsbehörde bedürfen, wird bewusst nicht geändert. Die neu im Gesetz aufgenommen großen kreisangehörigen Städte müssen damit kein Bestätigungsverfahren durchführen.

§ 104 (Handeln auf Anordnung)

Der bisher geltende § 104 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 105 (Hilfeleistung für Verletzte)

Keine Änderung.

§ 106 (Fesselung von Personen)

Keine Änderung.

§ 107 (Zum Gebrauch von Schusswaffen Berechtigte)

Der bisher geltende § 107 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 108 (Allgemeine Vorschriften für den Schusswaffengebrauch)

Keine Änderung.

§ 109 (Schusswaffengebrauch gegen Personen)

Die bisher geltende Regelung des § 109 wird mit folgenden Ergänzungen und Anpassungen in den Absätzen 1 und 2 übernommen

Absatz 1 bedarf einer Ergänzung. Die Mehrheit der Bundesländer verfügt in ihren Polizeigesetzen über eine spezielle Ermächtigungsnorm für die Abgabe eines Schusses gegen Personen, der mit an Sicherheit grenzender Wahrscheinlichkeit tödlich wirken wird. Die Absicht, die mit einem solchen Schuss verfolgt wird, ist, jede weitere Handlung, Reaktion oder auch nur Reflexe einer der für die gesetzlich beschriebene Gefahr verantwortlichen Person zu verhindern.

Dieser sogenannte „finale Rettungsschuss“ ist derzeit in 13 Bundesländern ausdrücklich gesetzlich geregelt.[1]

Der Gesetzgeber des Landes Mecklenburg-Vorpommern hat sich im Jahr 1992 gegen eine explizite Regelung des finalen Rettungsschusses entschieden. Im Gesetzentwurf der Landesregierung für ein Sicherheits- und Ordnungsgesetz - Drucksache 1/1612 des Landtages Mecklenburg-Vorpommern - war ursprünglich eine Textfassung zu § 109 Absatz 1 enthalten, die den finalen Rettungsschuss enthielt (siehe Seite 49 der vorgenannten Drucksache). Der Regelungsteil zum finalen Rettungsschuss wurde aber im weiteren Gesetzgebungsverfahren gestrichen. Der Beschlussempfehlung und dem Bericht des Innenausschusses des Landtages Mecklenburg-Vorpommern zum Gesetzentwurf der Landesregierung - Drucksache 1/2002 vom 25. Juni 1992 - lässt sich auf Seite 77 unter anderem folgende Begründung für die Streichung entnehmen:

„[…] Es besteht rechtspolitisch kein Bedürfnis, das Töten eines Menschen durch Staatsorgane positiv gesetzlich festzuschreiben. Die Regelungen des StGB sind - wie die Regelungen in den meisten der alten Bundesländer zeigen - ausreichend. § 32 oder § 34 StGB rechtfertigen jeden tödlich wirkenden Schuss, der nach § 109 Abs. 1 Satz 2 des Entwurfs zulässig wäre. Für den Polizeibeamten vor Ort tritt mit der Regelung des Entwurfs keine Verbesserung ein. […]“

Diese seinerzeitige Argumentation zum Rückgriff auf die §§ 32 und 34 des Strafgesetzbuches ist in der polizeifachlichen Literatur seit Jahren jedoch äußerst umstritten.

[1] Laut Lisken/Denninger, Handbuch des Polizeirechts, Verlag C.H. Beck, 6. Auflage, 2018, Teil E Rn 970: Baden-Württemberg (§ 54 Absatz 2 des Polizeigesetzes), Bayern (Artikel 66 Absatz 2 Satz 2 des Polizeiaufgabengesetzes), Brandenburg (§ 66 Absatz 2 Satz 2 des Brandenburgischen Polizeigesetzes), Hessen (§ 60 Absatz 2 Satz 2 des Hessischen Polizeigesetzes), Niedersachsens (§ 76 Absatz 2 Satz 2 des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung), Rheinland-Pfalz (§ 63 Absatz 2 Satz 2 des Polizei- und Ordnungsbehördengesetzes), Saarland (§ 57 Absatz 1 Satz 2 des Saarländischen Polizeigesetzes), Sachsen (§ 34 Absatz 2 des Polizeigesetzes des Freistaates Sachsen), Sachsen-Anhalt (§ 65 Absatz 2 Satz 2 des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt), Thüringen (§ 64 Absatz 2 Satz 2 des Polizeiaufgabengesetzes), Bremen (§ 46 Absatz 2 Satz 2 des Bremischen Polizeigesetzes), Hamburg (§ 25 Absatz 2 des Gesetzes zum Schutz der öffentlichen Sicherheit und Ordnung), Nordrhein-Westfalen (§ 63 Absatz 2 Satz 2 des Polizeigesetzes des Landes Nordrhein-Westfalen).

Artikel 2 der Europäischen Menschenrechtskonvention (EMRK) schützt das Recht eines jedes Menschen auf Leben. Eine Tötung wird aber nicht als Verletzung dieses Artikels betrachtet, wenn sie durch eine Gewaltanwendung verursacht wird, die unter bestimmten Voraussetzungen unbedingt erforderlich ist. Der Europäische Gerichtshof für Menschenrechte (EGMR) hat sich mit der Möglichkeit des Einsatzes tödlicher Gewalt durch die Polizei vor dem Hintergrund des bestehenden Artikels 2 EMRK unter anderem in seinem Urteil vom 20. Dezember 2004, Rechtssache 50385/99, beschäftigt. Er führt in der rechtlichen Beurteilung unter Nummer 3 aus[2]:

„[…] Wie schon der Text des Art. 2 EMRK zeigt, kann der Einsatz tödlicher Gewalt durch Polizisten unter Umständen gerechtfertigt sein. Art. 2 EMRK gewährt jedoch keine unbeschränkte Vollmacht. Unregulierte und willkürliche Handlungen staatlicher Organe sind mit einem wirksamen Schutz der Menschenrechte nicht vereinbar. Polizeioperationen müssen daher nicht nur im innerstaatlichen Recht vorgesehen sein, auch ihre Durchführung muss im Rahmen eines Systems wirksamer Sicherungen gegen Willkür und Machtmissbrauch ausreichend geregelt sein. […]“

Artikel 2 EMRK steht mithin einem finalen Rettungsschuss nicht entgegen, soweit das innerstaatliche Recht diesen vorsieht.

Das Grundrecht auf Leben und körperliche Unversehrtheit ergibt sich aus Artikel 2 Absatz 2 Satz 1 des Grundgesetzes. In das Recht darf gemäß Artikel 2 Absatz 2 Satz 3 des Grundgesetzes nur aufgrund eines Gesetzes eingegriffen werden. Somit obliegt es dem zuständigen Gesetzgeber, die Entscheidung für oder gegen ein in Grundrechte eingreifendes Handeln des Staates zu treffen.

Eine solche, den Anforderungen des Gesetzesvorbehalts genügende Ermächtigungsgrundlage könnte - mit Blick auf die seinerzeitigen Ausführungen in der oben genannten Beschlussempfehlung aus dem Jahr 1992 - § 32 oder § 34 des Strafgesetzbuches darstellen. Dieses wird jedoch in einschlägiger polizeirechtlicher Literatur vielfach abgelehnt. Einerseits wird argumentiert, dass so die Gefahr bestehe, durch Rückgriffe auf Notrechte, die als Jedermanns-Recht für das Bürger-Bürger-Verhältnis geschaffen wurden, bestehende verfahrens- und kompetenzrechtliche Einschränkungen im differenzierten System öffentlich-rechtlicher Eingriffsermächtigungen im Staat-Bürger-Verhältnis zu umgehen. Anderseits wird angeführt, dass dem Bundesgesetzgeber schon die Kompetenz zur Regelung präventiv-polizeilicher Eingriffsbefugnisse nicht zustehe. Demzufolge sei der Rückgriff auf Vorschriften im Strafgesetzbuch und damit im Bundesrecht für einen aus Gründen der Gefahrenabwehr abzugebenden finalen Rettungsschuss nicht zulässig. § 32 (Notwehr) beziehungsweise § 34 (Rechtfertigender Notstand) des Strafgesetzbuches sollen im Zusammenhang mit einem finalen Rettungsschuss tatsächlich nur herangezogen werden können, wenn es um die strafrechtlichen Rechtfertigungsgründe geht, also um die Frage der Strafbarkeit der handelnden Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten, die einen nicht gesetzlich geregelten finalen Rettungsschuss abgegeben haben. Denn die Beamtinnen und Beamten dürften im Vergleich zum nichthoheitlichen Handeln des Bürgers nicht schlechter gestellt werden.

[2] Deutscher Text abgerufen im Internet unter der Adresse: https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20041220_AUSL000_000BSW50385_9900000_000

In Anbetracht dieser vorstehenden Argumentation wird in der Literatur folglich die Auffassung vertreten, dass die Ermächtigung für die Abgabe eines „finalen Rettungsschusses“ durch die Polizei nicht aus dem Strafrecht entnommen werden kann; vielmehr muss sich die Zulässigkeit eines solchen Schusses aus dem Polizeirecht der Länder ergeben. Darüber hinaus wird zudem vielfach angeführt, dass die in den Polizeigesetzen enthaltene Formulierung, Personen durch den Schusswaffengebrauch „angriffs- oder fluchtunfähig“ machen zu können, mit Blick auf den tiefsten Grundrechtseingriff gegen einen Menschen nicht so weitgehend ausgelegt werden dürfe, dass darunter im Ernstfall auch der finale Rettungsschuss falle[3].

Diese bestehende rechtliche Diskussion ist auch den Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten im Land bekannt. Der Gesetzgeber ist daher - gerade auch unter Berücksichtigung der neuen Herausforderungen, die an die Polizei gestellt werden (zum Beispiel im Zusammenanhang mit der Abwehr von terroristischen Gefahrenlagen) - gefordert, der Polizei ein klares Regelungswerk an die Hand zu geben. Eine eindeutige gesetzliche Ermächtigung zum finalen Rettungsschuss bedeutet letztlich Handlungssicherheit für die im Rahmen der Gefahrenabwehr handelnden Beamtinnen und Beamten in schwierigen Situationen.

Vor diesem Hintergrund wird nun auch im § 109, der den Schusswaffengebrauch gegen Personen bestimmt, eine ausdrückliche Regelung zum sogenannten finalen Rettungsschuss unter eng begrenzten Voraussetzungen getroffen. Er ist seitens der Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten nur zulässig, wenn er das einzige Mittel zur Abwehr einer gegenwärtigen Lebensgefahr oder der gegenwärtigen Gefahr einer schwerwiegenden Verletzung der körperlichen Unversehrtheit ist. Die Formulierung der Regelung stimmt mit der Formulierung, die bereits in § 41 Absatz 2 Satz 2 des Musterentwurfs eines einheitlichen Polizeigesetzes des Bundes und der Länder aus den Jahren 1976/77 enthalten ist, überein. Sie wurde von der Mehrheit der Bundesländer in ihre Polizeigesetze übernommen und stellt eindeutig klar, dass der finale Rettungsschuss nur das allerletzte Mittel polizeilicher Zwangsanwendung sein darf und damit alle anderen Zwangsmittel Vorrang haben.

Die Übernahme des bisher geltenden Absatzes 2 erfolgt mit sprachlichen Anpassungen. In Nummer 3 Buchstabe b und Nummer 4 Buchstabe b werden die Wörter „dafür bestehen“ durch die Wörter „die Annahme rechtfertigen“ ersetzt.

§ 110 (Schusswaffengebrauch gegen Personen in einer Menschenmenge)

Der bisher geltende § 110 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 111 (Warnung)

Keine Änderung.

---

[3] Vergleiche zur Diskussionslage unter anderem:
- Lisken/Denninger, Handbuch des Polizeirechts, Verlag C.H. Beck, 6. Auflage, 2018, Teil E Randnummern 970 ff
- Tegtmeyer/Vahle, Polizeigesetz Nordrhein-Westfalen - PolG NRW - 10. Auflage, § 63 Randnummer 7
- Schmidbauer/Steiner, Bayerisches Polizeiaufgabengesetz und Polizeiorganisationsgesetz - Kommentar, Verlag C. H. Beck, 2. Auflage, Artikel 66 Randnummern 18 ff
- Prof. Dr. Clemens Arzt „Europäische Menschenrechtskonvention und polizeilicher Todesschuss“ veröffentlicht in DÖV - März 2007 - Heft 6, Seite 230

(Alle vorgenannten Quellen mit weiteren Nachweisen.)

§ 112 (Verwaltungsvorschriften über die Anwendung unmittelbaren Zwangs)

Die bisher geltende Regelung des § 112 wird unter Anpassung der Regelungsüberschrift und unter Aktualisierung der Bezeichnung des Innenressorts übernommen.

§ 113 (Einschränkung von Grundrechten)

Keine Änderung.

§ 114 (Kosten, Ermächtigung zum Erlass von Rechtsverordnungen)

Die Überschrift der Norm wird klarer gefasst und die bisherigen Regelungen in § 114 Absatz 1 werden unverändert übernommen.

Die Regelung des bisher geltenden Absatzes 2 wird angepasst. Zum einen wird in der Ermächtigung der obersten Landesbehörden zum Erlass von Rechtsverordnungen in ihrem jeweiligen Zuständigkeitsbereich ausdrücklich bestimmt, dass die Rechtsverordnungen nach § 2 des Landesverwaltungskostengesetzes zu erlassen sind. § 2 Absatz 2 des Landesverwaltungskostengesetzes enthält zudem bereits die Regelung, dass Kostenverordnungen der jeweils fachlich zuständigen obersten Landesbehörden im Einvernehmen mit dem Ministerium für Inneres und Europa und dem Finanzministerium zu erlassen sind. Damit kann diese im bisherigen § 114 Absatz 2 enthaltene Regelung entfallen.

Zusätzlich wird geregelt, dass neben den einzelnen Amtshandlungen, für die Verwaltungsgebühren erhoben werden, und den Gebührensätzen auch die Entstehung der Gebührenschuld sowie Art und Umfang der zu erstattenden Auslagen geregelt werden können. Es bleibt bei der Regelung, dass das Landesverwaltungskostengesetz gilt, wenn das SOG M-V keine abweichenden Vorschriften enthält. In dem dieser Regelung nachfolgenden Satz wird aber jetzt ausdrücklich festgelegt, dass die im Rahmen der Ermächtigung nach Satz 1 erlassenen Rechtsverordnungen von den §§ 10, 11 Absatz 1, 13 Absatz 1, 15 Absatz 1 und 2 sowie von dem § 16 des Landesverwaltungskostengesetzes abweichende Regelungen treffen können. Diese Änderung des Absatzes 2 orientiert sich an der seinerzeit in § 100 des SOG M-V enthaltenen Kostenregelung (vergleiche hierzu unter anderem Landtagsdrucksache 1/2002 Seite 50). Durch die klarere Formulierung der Abweichungsmöglichkeiten wird die derzeit zu verzeichnende inhaltliche Regelungslage in den bestehenden Kostenverordnungen der obersten Landesbehörden, die bereits solche abweichenden Regelungen enthalten, rechtssicherer abgebildet.

Die bisher geltende Regelung in Absatz 3 wird unter Vollzug der sprachlichen Gleichstellung übernommen.

§ 115 (Ausnahme- und Übergangsvorschriften)

Die bisher in § 115 enthaltene Übergangsvorschrift bezogen auf Dateien und Datensammlungen, die vor dem Inkrafttreten des Ersten Gesetzes zur Änderung des SOG M-V errichtet wurden, entfällt in Ermangelung eines heutigen Anwendungsbereichs.

In § 115 werden jedoch Ausnahme- und Übergangsregelungen aufgrund der neu geschaffenen Normen
- zur Datenkennzeichnung (§ 46g),
- zur Protokollierung (§§ 46e und 46f),
- zur bestehenden Prüfpflicht der oder des Landesbeauftragten für den Datenschutz in § 48b Absatz 6 und
- zur Neuregelung der Berichtspflichten in § 48h

erforderlich. Diese neuen gesetzlichen Regelungen bringen erhebliche Ausweitungen mit sich, sodass Ausnahme- und Übergangsvorschriften zu schaffen sind, die einen Übergang in die neuen Strukturen möglichst ohne Reibungsverluste ermöglichen.

Mit Absatz 1 wird eine grundsätzliche Ausnahme von den in § 46g Absatz 1 und 2 enthaltenen Kennzeichnungspflichten bestimmt, wenn die Kennzeichnung nach dem Stand der Technik nicht oder noch nicht vollständig wie normiert umgesetzt werden kann oder tatsächlich nicht möglich ist. Mit der ausnahmsweisen Regelung wird erreicht, dass in diesen Fällen Daten auch ohne Kennzeichnung weiterverarbeitet, insbesondere auch übermittelt werden dürfen und so die Erfüllung der Aufgabe der Gefahrenabwehr nicht in Ermangelung einer nicht umsetzbaren Kennzeichnung gefährdet wird.

Absatz 2 bestimmt eine Ausnahme vom im § 46g Absatz 2 enthaltenen Weiterverarbeitungs- und Übermittlungsverbot von nicht gekennzeichneten Daten. Die Regelung erfolgt in Anlehnung an § 91 des Bundeskriminalamtgesetzes. Sie bestimmt, dass eine Weiterverarbeitung oder Übermittlung personenbezogener Daten auch nach den Bestimmungen der für die Daten bis zum Tag des Inkrafttretens des überarbeiteten SOG M-V jeweils geltenden Verfahrensbeschreibung (in ihrer bis dahin geltenden Fassung) zulässig ist. Die Regelung gilt für personenbezogene Daten, die bis zum Tag des Inkrafttretens des überarbeiten SOG M-V keine Kennzeichnung nach § 46g Absatz 1 aufweisen und auch für personenbezogene Daten, die ab dem Inkrafttreten des neugefassten SOG M-V gespeichert werden, soweit deren Kennzeichnung tatsächlich nicht möglich ist oder solange deren Kennzeichnung nach dem Stand der Technik nicht möglich ist.

Im Ergebnis bewirkt die Vorschrift zum einen eine Fortgeltung der bisherigen Verfahrensbeschreibungen für Altdatenbestände. Die Vorschrift bezieht sich einerseits auf Datenbestände, die bereits vor Inkrafttreten des künftigen SOG M-V nach den für sie jeweils geltenden Rechtsvorschriften erhoben worden sind. Da eine vollständige technische Umsetzung von § 46g Absatz 1 nur sukzessive erfolgen kann und sich über einen längeren Zeitraum erstrecken wird, bezieht sich die Vorschrift aber anderseits auch auf künftig (nach dem Inkrafttreten) zu erhebende Datenbestände, soweit oder solange bei diesen im Zeitpunkt der Erhebung eine Kennzeichnung aus technischen oder tatsächlichen Gründen nicht möglich ist.

Durch diese Vorschrift wird auch eine ressourcenaufwändige Nachkennzeichnung der Altdatenbestände vermieden. Die Möglichkeit, die „Altdaten“ durch eine nachträgliche Kennzeichnung entsprechend den Vorgaben von § 46e zu kennzeichnen, bleibt unberührt.

Mit den Vorschriften in Absatz 2 wird demnach ein rechtssicherer Weg geschaffen, um auch nicht gekennzeichnete Altdatenbestände weiterverarbeiten zu dürfen und so die Funktionsfähigkeit der Gefahrenabwehrbehörden nicht zu beeinträchtigen. Die Altdatenbestände unterliegen Aussonderungsprüffristen und Löschpflichten, sodass sich ihr Bestand - und damit auch das Anwendungsfeld der hier in Absatz 2 geschaffenen Ausnahmevorschrift - sukzessive reduzieren und in der weiteren Zukunft auslaufen wird.

Absatz 3 enthält eine Übergangsregelung von der normierten Protokollierungspflicht in § 46e. Auf die entsprechende Ermächtigung in Artikel 63 Absatz 2 der Richtlinie (EU) 2016/680, Protokollierungspflichten im Ausnahmefall erst später nachzukommen, wird verwiesen (siehe zusätzlich unter anderem auch den Erwägungsgrund 96 der Richtlinie). Protokollierungen müssen nach § 46e bei vor dem 6. Mai 2016 eingerichteten, automatisierten Verfahren erst bis zum 6. Mai 2023 erfolgen, wenn andernfalls ein unverhältnismäßiger Aufwand entstünde. Die Ausnahme gilt ausdrücklich nicht für Protokollierungen bei verdeckten und eingriffsintensiven Maßnahmen nach § 46f und bei der Übermittlung personenbezogener Daten an Drittstaaten und weitere zwischen- und überstaatliche Stellen nach den §§ 39d bis 39h sowie nach der Verordnung (EU) 2016/679; zu diesen Maßnahmen sind die Protokollierungspflichten nach den §§ 46e und 46f zu erfüllen.

Ferner wird bestimmt, dass die Anwendung der Übergangsregelung zur Protokollierung zu begründen, zu dokumentieren und dem Ministerium für Inneres und Europa mitzuteilen ist. Die oder der Landesbeauftragte für den Datenschutz ist über das betroffene automatisierte Verfahren und die Gründe für die Anwendung der in Absatz 3 Satz 1 normierten Übergangsregelung zur Protokollierungspflicht zu unterrichten. Diese Unterrichtungspflicht ist mit Blick auf die bestehenden Kontrollrechte und Kontrollpflichten geboten.

Mit Absatz 4 wird der erstmalige Beginn der Frist für die in § 48b Absatz 6 festgelegte im Abstand von längstens zwei Jahren zumindest stichprobenartige Kontrolle
- zu den in § 46f Absatz 2 genannten Maßnahmen und
- zu den Datenübermittlungen an Drittstaaten und weitere zwischen- und überstaatliche Stellen nach den §§ 39d bis 39h sowie nach der Verordnung (EU) 2016/679

durch die oder den Landesbeauftragten für den Datenschutz auf den 1. Januar 2020 festgelegt. Hierdurch erhält auch die oder der Landesbeauftragte für den Datenschutz, der aufgrund des EU-Datenschutzpakets einen wesentlichen Aufgabenzuwachs zu verzeichnen hat, die Möglichkeit, sich auf die mit diesem Gesetz vorgesehene Aufgabenerweiterung vorzubereiten. Nur so vermag er eine Kontrolle auch tatsächlich auszuüben.

Absatz 5 legt das erste berichtspflichtige Kalenderjahr mit dem Jahr 2020 fest. Folglich ist im Jahr 2021 den neuen Berichtspflichtenregelungen in § 48h zu allen dort genannten Maßnahmen vollständig nachzukommen. Diese zeitliche Verschiebung in der Anwendung der Regelung des § 48h ermöglicht es, die notwendige Zeit für den Erlass der Verwaltungsvorschrift nach § 48h Absatz 5 und für eine Umsetzung der Verfahrens- und Informationswege, die für die Erfüllung der Berichtspflichten notwendig sind (insbesondere innerhalb der Landespolizei), zu erhalten.

Für den Bericht im Jahr 2020 für das Jahr 2019 wird bestimmt, dass den bisher geltenden Berichtspflichten nachzukommen ist. Demnach obliegt dem Ministerium für Inneres und Europa die Pflicht, dem SOG-Gremium im Übergangszeitraum - wie bisher auch - mindestens einmal jährlich über Anlass und Dauer der Einsätze technischer Mittel

- zur Erhebung personenbezogener Daten aus Vertrauensverhältnissen im Sinne der §§ 53, 53a der Strafprozessordnung (siehe bisheriger § 33 Absatz 6 SOG M-V),
- ausschließlich zum Schutz der bei einem polizeilichen Einsatz tätigen Personen soweit richterlich überprüfungsbedürftig (siehe bisher geltender § 34 Absatz 4 SOG M-V),
- zur Erhebung personenbezogener Daten in oder aus Wohnungen (siehe bisher geltender § 34b Absatz 9 SOG M-V) und
- zur Überwachung und Aufzeichnung der Telekommunikation (siehe bisher geltender § 34a Absatz 9 SOG M-V)

zu berichten. Das Justizministerium berichtet - wie bisher - über die nach § 100c der Strafprozessordnung erfolgten Maßnahmen in Mecklenburg-Vorpommern (akustische Wohnraumüberwachung). Zudem hat auch die jährliche Unterrichtung des Landtages über die Anzahl der vorstehend aufgezählten Einsätze technischer Mittel zu erfolgen.

§ 116 (Evaluierungspflicht)

Mit der Regelung wird die Landesregierung verpflichtet, die im SOG M-V vorgenommenen Änderungen bis zum 31. Dezember 2024 zu evaluieren und dem Landtag über das Evaluierungsergebnis zu berichten. Besonderes Augenmerk ist bei der Evaluierung auf die neu aufgenommenen Befugnisse (siehe hierzu I. Allgemeine Begründung unter der Überschrift „Ergänzung des SOG M-V um neue Befugnisnormen und klarstellende Regelungen“) zu legen.

Zu Artikel 2 (Änderung des Brandschutz- und Hilfeleistungsgesetzes M-V)

In den §§ 14 Absatz 2 Satz 3, 17 Absatz 2 Satz 1 und in § 32 Absatz 1 und 2 wird jeweils die Bezeichnung des Innenressorts von „Ministerium für Inneres und Sport“ in „Ministerium für Inneres und Europa“ geändert.

Im § 28 des Brandschutz- und Hilfeleistungsgesetzes sind datenschutzrechtliche Bestimmungen enthalten. Die Änderung des § 28 Absatz 1 ist erforderlich, weil die Verordnung (EU) 2016/679 ab dem 25. Mai 2018 als unmittelbar anwendbares Recht gilt und durch die dort eingeräumten Öffnungsklauseln Regelungen in den datenschutzrechtlichen Bestimmungen der Länder zulässig sind. Zudem wird die Verweisung auf das Landesdatenschutzgesetz beibehalten.

Die Regelungen zur Datenverarbeitung in den Absätzen 2 bis 6 können nach den Maßgaben des Artikels 6 Absatz 1 Buchstabe e, Absatz 2 und 3 der Verordnung (EU) 2016/679 beibehalten werden.

In Bezug auf die bestehende Regelung in Absatz 6 ist aber besonders darauf hinzuweisen, dass bei einer Datenerhebung bei den Diensteanbietern die Informationspflichten gemäß Artikel 14 der Verordnung (EU) 2016/679 mit den ergänzenden Vorschriften in § 5 des Landesdatenschutzgesetzes zu beachten sind.

Zu Artikel 3 (Änderung des Landeskatastrophenschutzgesetzes)

In den §§ 3 Absatz 1 Nummer 1, 5 Absatz 4, 6 Absatz 1, 15 Absatz 5 Satz 7, 24a Satz 2, 25 Absatz 5 Satz 2 und in § 33 wird jeweils die Bezeichnung des Innenressorts von „Ministerium für Inneres und Sport“ in „Ministerium für Inneres und Europa“ geändert.

Im Abschnitt 6 „Datenschutz“ werden zudem folgende Anpassungen vorgenommen:

Die Änderung des § 35 ist erforderlich, weil die Verordnung (EU) 2016/679 ab dem 25. Mai 2018 als unmittelbar anwendbares Recht gilt und durch die dort eingeräumten Öffnungsklauseln Regelungen in den datenschutzrechtlichen Bestimmungen der Länder zulässig sind.

Die Regelungen zur Datenverarbeitung in den §§ 35 bis 37 können nach den Maßgaben des Artikels 6 Absatz 1 Buchstabe e, Absatz 2 und 3 der Verordnung (EU) 2016/679 beibehalten werden.

In § 38 wird in Absatz 1 die Verantwortungsregelung beim Abruf auf Ersuchen gestrichen, da die ersuchte Stelle verantwortliche Stelle im Sinne der Verordnung (EU) 2016/679 bleibt. Die bisherige Regelung zur Zweckänderung bleibt neben § 4 Absatz 2 des Landesdatenschutzgesetzes nach den Maßgaben des Artikels 6 Absatz 1 Buchstabe e, Absatz 2 und 3 der Verordnung (EU) 2016/679 bestehen. Absatz 2 wird gestrichen.

Zu Artikel 4 (Einschränkung von Grundrechten)

Mit Artikel 4 wird dem verfassungsrechtlichen Zitiergebot gemäß Artikel 19 Absatz 1 Satz 2 des Grundgesetzes Rechnung getragen.

Zu Artikel 5 (Inkrafttreten, Außerkrafttreten)

Artikel 5 regelt das Inkrafttreten des Gesetzes am Tag nach der Verkündung. Gleichzeitig wird bestimmt, dass durch die in Artikel 1 bestimmte Neufassung des Sicherheits- und Ordnungsgesetzes dessen bisher geltende Fassung außer Kraft tritt.