Begründung

A. Allgemeiner Teil

1. Am 5. Mai 2016 ist die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU L 119 vom 4.5.2016, S. 89, berichtigt durch ABl. EU L 127 vom 23.5.2018, S. 9) in Kraft getreten. Mit dieser Richtlinie, die in nationales Recht umzusetzen ist, soll der Datenverkehr auf EU-Ebene zwischen jenen Behörden erleichtert werden, die für die Verhütung, Verfolgung sowie Vollstreckung von Straftaten zuständig sind. Gleichzeitig soll in diesen Bereichen ein hohes Schutzniveau für personenbezogene Daten gewährleistet und eine Harmonisierung der Vorschriften innerhalb der Europäischen Union erreicht werden.

Ferner ist 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 (ABl. EU L 119 vom 4.5.2016, S. 1, berichtigt durch ABl. EU L 127 vom 23.5.2018, S. 2 ff.) seit 25. Mai 2018 unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union. Mit ihr soll ein verbindliches Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten in allen Mitgliedstaaten geschaffen werden, das auch alle öffentlichen Stellen zu beachten haben, soweit sie personenbezogene Daten im Anwendungsbereich der Verordnung (EU) 2016/679 verarbeiten. Dabei schließen sich die Anwendungsbereiche der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2016/679 gegenseitig aus. Das neue Landesdatenschutzgesetz (LDSG) trifft künftig ausschließlich im Anwendungsbereich der Verordnung (EU) 2016/679 und nur noch an den Stellen ergänzende Regelungen, an denen die Verordnung (EU) 2016/679 entsprechende Öffnungsklauseln für die nationalen Gesetzgeber vorgesehen hat. Daher enthält das LDSG kein umfassendes Regelwerk mehr, das für den polizeilichen Datenschutz herangezogen werden kann.

Mit dem vorliegenden Gesetzentwurf soll die Richtlinie (EU) 2016/680 für den polizeilichen Bereich umgesetzt werden. Hierzu werden das Polizeigesetz für Baden-Württemberg (PolG) und die Verordnung des Innenministeriums zur Durchführung des Polizeigesetzes (DVOPolG) an die Anforderungen der Richtlinie (EU) 2016/680 angepasst bzw. um die erforderlichen Neuregelungen ergänzt. Aufgrund der unterschiedlichen Anwendungsbereiche zwischen der Richtlinie (EU) 2016/680 einerseits und der Verordnung (EU) 2016/679 andererseits muss das PolG in diesem Zusammenhang auch um allgemeine datenschutzrechtliche Regelungen ergänzt werden, die bisher im LDSG enthalten waren.

Aufgrund des erheblichen Änderungs- und Ergänzungsbedarfs wird das PolG insgesamt neu gefasst und die bisher geltende Fassung aufgehoben.

Die wesentlichen Neuerungen im PolG betreffen im Einzelnen folgende Themenbereiche:

- Personenbezogene Daten unterliegen künftig bei ihrer weiteren Verarbeitung einer engen Zweckbindung.

- Die Vorschriften zur Übermittlung von Daten ins nichteuropäische Ausland werden richtlinienkonform neu gestaltet.

- Besondere Kategorien personenbezogener Daten wie etwa politische Meinungen, religiöse Überzeugungen oder Daten zur sexuellen Orientierung werden künftig unter einen besonderen Schutz gestellt.

- Ferner enthalten die neuen Regelungen umfassende Protokollierungspflichten sowie weitere Pflichten der Polizei, die der Transparenz und der Ermöglichung einer aufsichtlichen Kontrolle dienen.

- Betroffenen Personen wird konkreter als nach bisheriger Rechtslage das Recht auf Auskunft, auf Berichtigung, Löschung oder Einschränkung der Verarbeitung ihrer Daten sowie das Recht gewährt, sich an die Aufsichtsbehörde

für den Datenschutz zu wenden.

- Der Aufsichtsbehörde für den Datenschutz werden wirksame Untersuchungs-, Beratungs- und Abhilfebefugnisse sowie das Recht eingeräumt, eine Datenverarbeitung der Polizei gerichtlich überprüfen zu lassen, um eine aufsichtliche Kontrolle sicherzustellen.

2. Mit den Änderungen der Regelungen zu den verdeckten Eingriffsbefugnissen (§§ 48 bis 56 PolG) wird vor allem die Entscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtgesetz (BVerfG vom 20. April 2016 - 1 BvR 966/09, 1 BvR 1140/09 [Verweise auf das Bundesverfassungsgericht ohne nähere Angaben beziehen sich im folgenden Text nur auf diese Entscheidung]) umgesetzt und werden die vergleichbaren Vorschriften des PolG entsprechend angepasst. Gleichzeitig werden die diesbezüglichen Anforderungen an die weitere Nutzung und Übermittlung erhobener Daten entsprechend berücksichtigt. Für die inhaltliche Telekommunikationsüberwachung (TKÜ) und die Quellen-TKÜ wurden die Vorgaben des Bundesverfassungsgerichts im Rahmen der Polizeigesetz-Novelle 2017 bereits vollständig umgesetzt.

Das Bundesverfassungsgericht hat in diesem Zusammenhang entschieden, dass die Befugnisse des Bundeskriminalamts zum Einsatz von heimlichen Überwachungsmaßnahmen zur Terrorabwehr zwar im Grundsatz mit den Grundrechten vereinbar sind, ihre derzeitige Ausgestaltung jedoch in verschiedener Hinsicht nicht dem Verhältnismäßigkeitsgrundsatz genügt. Es hat geurteilt, dass bei solchen Maßnahmen, die tief in das Privatleben Betroffener hineinreichen, besondere Anforderungen an den Verhältnismäßigkeitsgrundsatz zu stellen sind. Insbesondere verlangen die Befugnisse besondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung sowie einen Schutz von Berufsgeheimnisträgern, unterliegen Anforderungen an Transparenz, individuellen Rechtsschutz und datenschutzaufsichtliche Kontrolle und müssen von Löschungspflichten bezüglich der erhobenen Daten flankiert sein.

In seiner Entscheidung hat das Bundesverfassungsgericht zudem grundsätzliche Ausführungen zum polizeilichen Datenschutz gemacht. Es hat die bisherige Rechtsprechung zu den einzelnen verdeckten Ermittlungsbefugnissen zusammengeführt,

sie in übergreifende Prinzipien systematisiert, die verfassungsrechtlichen Anforderungen an Zweckbindung und Zweckänderung von Daten fortentwickelt und erstmals Aussagen zur Übermittlung von Daten an öffentliche Stellen im Ausland getroffen. Es hat insbesondere ausgeführt, dass sich die Anforderungen an die Nutzung und Übermittlung staatlich erhobener Daten nach den Grundsätzen der Zweckbindung und Zweckänderung richten und sich die Verhältnismäßigkeitsanforderungen für eine solche Zweckänderung am Grundsatz der hypothetischen Datenneuerhebung zu orientieren haben. Auch die Übermittlung von Daten an öffentliche Stellen im Ausland unterliegt diesen verfassungsrechtlichen Grundsätzen der Zweckbindung und Zweckänderung.

Die Übergangsregelungen in § 85 des bisherigen PolG können aufgrund der jetzt vorgenommenen Änderungen gestrichen werden.

Die bisherige Regelung des § 23a PolG a.F., die gebündelt besondere Bestimmungen über polizeiliche Maßnahmen mit Bezug zur Telekommunikation enthielt, wird in diesem Zusammenhang aus Gründen der Übersichtlichkeit hinsichtlich der einzelnen dort enthaltenen Maßnahmen aufgeteilt. Die Bestandsdatenauskunft ist künftig in § 52 geregelt, die Erhebung von Telekommunikationsverkehrsdaten und Nutzungsdaten in § 53 und der Einsatz des sog. IMSI-Catchers sowie die Befugnis zur Unterbrechung oder Verhinderung von Telekommunikationsverbindungen in § 55. Die bislang schon in einer eigenen Vorschrift geregelte inhaltliche Überwachung der Telekommunikation findet sich künftig in § 54.

3. Gesetzgeberischer Handlungsbedarf besteht auch im Zusammenhang mit öffentlichen Großveranstaltungen, die ein besonderes Gefährdungsrisiko aufweisen. Zum einen stehen öffentliche Veranstaltungen und Ansammlungen im Fokus des internationalen Terrorismus. Anschläge wie das Massaker im Bataclan-Theater und die Selbstmordattentate am Stade de France im November 2015 in Paris, das Selbstmordattentat im Mai 2017 bei einem Popkonzert in Manchester, der Anschlag auf die Feierlichkeiten zum französischen Nationalfeiertag 2016 in Nizza oder im selben Jahr auf den Berliner Weihnachtsmarkt sind nur einige schreckliche Beispiele dafür. Darüber hinaus sind Weihnachtsmärkte, Volksfeste, Konzerte oder Sportveranstaltungen mit ihrer Anziehungskraft für eine Vielzahl von Menschen leider oftmals auch Tatort

von zahlreichen Straftaten. Dort, wo viele Menschen öffentlich zusammenkommen, erhöht sich die Gefahr, Opfer oder Geschädigter einer Straftat zu werden. Täter und Störer nutzen häufig die Anonymität der Masse, um unerkannt abzutauchen.

Vor diesem Hintergrund kann es erforderlich werden, im Umfeld entsprechender Veranstaltungen verstärkt Personenkontrollen durchzuführen, um potentielle Straftäter aus ihrer Anonymität zu holen und Straftaten zu verhindern. Mit den neuen Regelungen in § 27 Absatz 1 Nummer 2, § 34 Absatz 1 Nummer 3 und § 35 Nummer 4 werden die bestehenden polizeilichen Befugnisse daher erweitert und die Polizei in die Lage versetzt, bei Großveranstaltungen, die ein besonderes Gefährdungsrisiko aufweisen, verstärkt Personenfeststellungen durchzuführen sowie Personen und Sachen zu durchsuchen.

Um die Auswirkungen der neuen Befugnisse nach § 27 Absatz 1 Nummer 2, § 34 Absatz 1 Nummer 3 und § 35 Nummer 4 überprüfen zu können, sind die entsprechenden Regelungen ein Jahr nach ihrem Inkrafttreten einer Evaluation zu unterziehen. Neben dem Umfang der durchgeführten Maßnahmen und der Art der betroffenen Veranstaltungen soll insbesondere auch die Ausübung des Auswahlermessens evaluiert werden, also welche Personen aufgrund welcher Umstände für entsprechende Maßnahmen herangezogen wurden.

4. Mit den Änderungen der Regelungen über den offenen Einsatz technischer Mittel zur Bild- und Tonaufzeichnung werden die Einsatzmöglichkeiten der Bodycam erweitert. Künftig ist eine Verwendung auch in Wohnungen einschließlich Arbeits-, Betriebs- und Geschäftsräumen möglich.

Während der Erprobungsphase der Bodycam hat sich aus fachlicher Sicht gezeigt, dass die Beschränkung des Anwendungsbereichs auf öffentlich zugängliche Orte zu eng gefasst ist. Die Einsatzszenarien zwischen öffentlich zugänglichen Orten und Arbeits-, Betriebs- oder Geschäftsräumen sind bei grundsätzlich vergleichbaren Einschreitesituationen oftmals fließend. Häufig entwickeln sich Einsätze im Umfeld von Gaststätten, Einkaufszentren oder Diskotheken, die sich dann im weiteren Verlauf in diese hinein verlagern. Andersherum entstehen entsprechende Situationen auch in

solchen Räumlichkeiten, beispielsweise bei einem pöbelnden Gast oder bei Streitigkeiten mit dem Sicherheitspersonal in einer Diskothek, die dann ihre Fortsetzung im öffentlichen Raum finden. Die derzeitige Rechtslage enthält an dieser Stelle eine räumlich strikte Trennung, die den Gegebenheiten in der Realität nicht immer gerecht wird. Daher kann die deeskalierende Wirkung einer Bodycam derzeit in beiden Fallkonstellationen nicht umfassend ausgeschöpft werden.

Und auch in Wohnungen kann die Bodycam einen wichtigen Beitrag zum Schutz unserer Einsatzkräfte leisten. Polizeiliche Einsätze im Zusammenhang mit häuslicher Gewalt bergen erfahrungsgemäß ein erhöhtes Gefahrenpotential für die eingesetzten Polizeibeamtinnen und -beamten. Die alarmierte Polizei findet vor Ort häufig Situationen vor, die von Aggression und Gewalt geprägt sind. Diese Aggressionen können urplötzlich und ohne Vorwarnung umschwenken und sich gegen die eingesetzten Kräfte richten. Hierbei kann es auch zu Solidarisierungseffekten gegen die Polizei kommen. Denn gerade die polizeiliche Intervention und die zu treffenden straf- und polizeirechtlichen Maßnahmen, die nötigenfalls auch mit unmittelbarem Zwang durchgesetzt werden, können vermehrt zu Angriffen auf und Widerstandshandlungen gegen die Einsatzkräfte führen. Ein Großteil der Fälle häuslicher Gewalt trägt sich in privaten Wohnungen, also außerhalb der Öffentlichkeit zu. Gerade in diesen Situationen kann der Einsatz einer Bodycam zusätzlich deeskalierend wirken.

Auch die einschlägigen Zahlen aus der Polizeilichen Kriminalstatistik belegen den fachlichen Bedarf für eine Erweiterung der bestehenden Rechtslage. Im Jahr 2016 wurden in Baden-Württemberg insgesamt 4.394 Fälle registriert, in denen es zu Gewalt gegen Polizeibeamte kam. Davon wurden 1.222 Taten in Wohnungen (677) sowie Arbeits-, Betriebs- oder Geschäftsräumen (545) begangen. Im 5-Jahresvergleich bewegen sich die Fallzahlen „Gewalt gegen Polizeibeamte“ mit einem Tatort in Arbeits-, Betriebs- oder Geschäftsräumen sowie Wohnungen auf einem konstant hohen Niveau. Der Anteil der Fälle an diesen Tatörtlichkeiten beträgt mit steigender Tendenz zwischen 25 % und 30 %.

Die neue Regelung berücksichtigt in besonderem Maße die Vorgaben des Artikels 13 des Grundgesetzes (GG). Beim Einsatz einer Bodycam in Arbeits-, Betriebs- und Geschäftsräumen und insbesondere auch in Wohnungen kann nicht ausgeschlossen

werden, dass dies mit einem Eingriff in den Schutzbereich des Artikels 13 GG verbunden ist. Die erweiterte Regelung trägt den verfassungsrechtlichen Anforderungen Rechnung.

5. Die Regelung zum Einsatz automatischer Kennzeichenlesesysteme (AKLS) in § 51 wird an die Vorgaben des Bundesverfassungsgerichts (BVerfG vom 18. Dezember 2018 – 1 BvR 2795/09, 1 BvR 3187/10, 1 BvR 142/15) angepasst. Das Bundesverfassungsgericht hat mit diesen Entscheidungen die Regelungen zum Einsatz von AKLS in Baden-Württemberg, Bayern und Hessen teilweise beanstandet.

6. Die Polizei in Baden-Württemberg führt bereits seit einigen Jahren sog. Gefährderansprachen durch bzw. versendet entsprechende Gefährderanschreiben. Durch diese Kontaktaufnahme soll eine betroffene Person frühzeitig darauf hingewiesen werden, dass sie im Fokus der Polizei steht, weil Tatsachen die Annahme rechtfertigen, dass von ihr eine Störung der öffentlichen Sicherheit zu befürchten ist. Bislang werden diese Maßnahmen, soweit sie mit einem Eingriff in die geschützten Rechtsgüter der betroffenen Person verbunden sind, auf die polizeiliche Generalklausel nach §§ 1, 3 PolG gestützt. Mit der neuen Regelung des § 29 Absatz 1 werden die Gefährderansprache und das Gefährderanschreiben nunmehr als Standardmaßnahme in das Polizeigesetz aufgenommen.

Gleiches gilt für die sog. Gefährdetenansprache (§ 29 Absatz 2). Durch eine Gefährdetenansprache werden beispielsweise Kontaktpersonen von potentiellen Straftätern über bestehende Risiken informiert, sofern tatsächliche Anhaltspunkte eine entsprechende Information rechtfertigen. Auch diese Maßnahmen werden bislang auf die polizeiliche Generalklausel nach §§ 1, 3 PolG gestützt, sofern sie in geschützte Rechtsgüter des potentiellen Straftäters eingreifen.

Mit der Ergänzung in § 105 Absatz 3 wird zudem geregelt, dass der Polizeivollzugsdienst für die Durchführung sämtlicher Maßnahmen nach § 29 originär neben den Polizeibehörden zuständig ist.

7. Darüber hinaus wird mit der neuen Regelung des § 45 eine ausdrückliche Rechtsgrundlage zur Aufzeichnung bestimmter Telefonanrufe in das Polizeigesetz aufgenommen. Die Befugnis gilt sowohl für eingehende Notrufe als auch für die Aufzeichnung von Anrufen auf solche Nummern, die der Bevölkerung zur Mitteilung sachdienlicher Hinweise bekannt gegeben werden. Dabei handelt es sich insbesondere um die Rufnummern des Kriminaldauerdienstes, der Telefonzentrale, des Bürgertelefons, die zentralen Nummern der Öffentlichkeitsfahndung sowie Sonderrufnummern, die aus Anlass bestimmter Fahndungsmaßnahmen eingerichtet werden und über die von Anrufern Hinweise gegeben werden, die für die Aufgabenerfüllung des Polizeivollzugsdienstes von Bedeutung sein können.

8. Aufgrund der anhaltend hohen abstrakten Gefahr terroristischer Anschläge ist der Bedarf an der Durchführung von Zuverlässigkeitsüberprüfungen kontinuierlich angestiegen, zum Beispiel im Umfeld von Festivals, Sportbegegnungen oder sonstigen Großveranstaltungen, aber auch bei Zutrittsberechtigungen für öffentliche Liegenschaften. In diesem Zusammenhang werden personenbezogene Daten von Personen, denen zur Ausführung von Tätigkeiten Zutritt zu sicherheitsrelevanten Bereichen gewährt werden soll, mit polizeilichen Dateien abgeglichen. Zuverlässigkeitsüberprüfungen wurden bislang ausschließlich auf der Grundlage von Einwilligungen der betroffenen Personen durchgeführt. Mit der neuen Regelung des § 42 wird eine ausdrückliche Rechtsgrundlage für die Durchführung des für die Zuverlässigkeitsüberprüfung erforderlichen Datenabgleichs geschaffen. Allerdings ist weiterhin die Einwilligung der betroffenen Person in die damit verbundene Datenverarbeitung erforderlich, um ihr zumindest Entscheidungsspielräume zu belassen und damit ein höchstmögliches Maß an Datenschutz zu gewährleisten.

9. Mit Artikel 3 wird ein neuer § 13a in das Gesetz zur Ausführung des Gerichtsverfassungsgesetzes und von Verfahrensgesetzen der ordentlichen Gerichtsbarkeit (AGGVG) eingefügt. Hierdurch können Gerichtsvollzieherinnen und Gerichtsvollzieher in bestimmten Fällen zur Abschätzung der konkreten Gefährdungssituation bei einer beabsichtigten Vollstreckungsmaßnahme Informationen über die Schuldnerin oder den Schuldner bei der zuständigen Polizeidienststelle einholen. Dies dient der Vermeidung von Gefährdungssituationen sowie der Stärkung des Eigenschutzes der Gerichtsvollzieherinnen und Gerichtsvollzieher.

10. Die gesetzlichen Änderungen führen durch die Beschaffung und den Unterhalt von den neuen Anforderungen tragenden Softwareprodukten nach einer ersten Grobabschätzung zu Mehrausgaben für den Landeshaushalt in Höhe von mindestens 2 Mio. Euro. Eine genaue Bezifferung der Ausgaben ist zum jetzigen Zeitpunkt noch nicht möglich. Zudem verursacht das Gesetz für die Polizei, die Justiz und den Landesbeauftragten für den Datenschutz einen erheblichen personellen Zusatzaufwand vor allem durch die unionsrechtlich vorgegebenen neuen Datenschutzvorschriften, aber auch aufgrund der Vorgaben des Bundesverfassungsgerichts bei verdeckten Eingriffsmaßnahmen. Allerdings können auch die zusätzlichen Personalaufwände zum jetzigen Zeitpunkt noch nicht näher beziffert werden.

Grundsätzlich sind auch neue Aufgaben im Rahmen der vorhandenen Ressourcen zu erfüllen. Die Bereitstellung eventueller zusätzlicher personeller und sächlicher Mittel für diese Zwecke bleibt dem Haushaltsgesetzgeber vorbehalten. Hierüber ist in Haushaltsaufstellungsverfahren zu entscheiden.

Nennenswerte Kosten für Private entstehen durch die Gesetzesänderungen nicht.

11. Der Nachhaltigkeitscheck lässt keine nennenswerten Auswirkungen des Gesetzesvorhabens auf die ökonomischen, ökologischen und sozialen Verhältnisse erwarten. Insgesamt leistet der Gesetzentwurf einen wichtigen Beitrag, um das Sicherheitsgefühl in der Bevölkerung zu verbessern. Er ist mit den Zielen einer nachhaltigen Entwicklung vereinbar.

B. Einzelbegründung

I. Zu Artikel 1

1. Zu §§ 1 bis 10 (Allgemeines bis Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger)
Die Regelungen entsprechen weitestgehend den §§ 1 bis 10 des bisherigen PolG. Allerdings wird in § 4 die Versammlungsfreiheit in die Liste der Grundrechte aufgenommen, die durch polizeiliche Maßnahmen aufgrund des Polizeigesetzes eingeschränkt werden können, da die neue Standardmaßnahme nach § 29 im Einzelfall einen Eingriff in das Recht aus Artikel 8 Absatz 1 GG darstellen kann. Im Übrigen werden die Verweise aufgrund der neuen Nummerierung des Gesetzes angepasst.

2. Zu § 11 (Anwendungsbereich - Datenverarbeitung)
In Umsetzung von Artikel 1 Absatz 1 und Artikel 2 der Richtlinie (EU) 2016/680 definiert die Regelung den Anwendungsbereich der Vorschriften des Polizeigesetzes, die die Datenverarbeitung betreffen.

Zu Absatz 1
Absatz 1 Satz 1 bestimmt, dass die §§ 11 bis 16 sowie die Vorschriften des 3. Abschnitts für die Verarbeitung personenbezogener Daten zu solchen Zwecken gelten, die der Richtlinie (EU) 2016/680 unterfallen.

Adressat der genannten Vorschriften ist die Polizei, die sowohl den Polizeivollzugsdienst als auch die Polizeibehörden umfasst. Für die Anwendbarkeit der Vorschriften ist der Zweck entscheidend, zu dem die jeweilige Stelle innerhalb der Polizei tätig wird.

Sachlicher Anwendungsbereich der Vorschriften ist die Datenverarbeitung zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Maßgeblich ist folglich der mögliche Bezug zu einer Straftat oder einer Ordnungswidrigkeit. Dies gilt auch für den Bereich der Gefahrenabwehr,

wobei es ausreicht, dass die abzuwehrende Gefahr zu einer Straftat oder Ordnungswidrigkeit führen kann, ohne dass dies zum Zeitpunkt des Tätigwerdens bereits feststehen muss. Erwägungsgrund 12 der Richtlinie (EU) 2016/680 führt insoweit aus: „Die Tätigkeiten der Polizei oder anderer Strafverfolgungsbehörden sind hauptsächlich auf die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten ausgerichtet, dazu zählen auch polizeiliche Tätigkeiten in Fällen, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht. Solche Tätigkeiten können ferner die Ausübung hoheitlicher Gewalt durch Ergreifung von Zwangsmitteln umfassen, wie polizeiliche Tätigkeiten bei Demonstrationen, großen Sportveranstaltungen und Ausschreitungen. Sie umfassen auch die Aufrechterhaltung der öffentlichen Ordnung als Aufgabe, die der Polizei oder anderen Strafverfolgungsbehörden übertragen wurde, soweit dies zum Zweck des Schutzes vor und der Abwehr von Bedrohungen der öffentlichen Sicherheit und Bedrohungen für durch Rechtsvorschriften geschützte grundlegende Interessen der Gesellschaft, die zu einer Straftat führen können, erforderlich ist.“

Satz 2 stellt klar, dass besondere Rechtsvorschriften des Bundes, insbesondere zu Zwecken der Strafverfolgung, den genannten Vorschriften des Polizeigesetzes vorgehen. Solche besonderen Rechtsvorschriften des Bundes können sich insbesondere aus dem Gesetz über Ordnungswidrigkeiten sowie aus der Strafprozessordnung ergeben. Denn für die repressive Tätigkeit der Polizei besteht eine konkurrierende Gesetzgebungskompetenz des Bundes (Artikel 72 Absatz 1, Artikel 74 Absatz 1 Nummer 1 GG), von der der Bund mit der Strafprozessordnung, auf die auch das Gesetz über Ordnungswidrigkeiten verweist, abschließend Gebrauch gemacht hat.

Zu Absatz 2

Absatz 2 stellt klar, dass für die Verarbeitung personenbezogener Daten zu anderen als den in Absatz 1 genannten Zwecken, die also nicht dem Anwendungsbereich der Richtlinie (EU) 2016/680 unterfallen, die Verordnung (EU) 2016/679 sowie das Landesdatenschutzgesetz gelten.

Zu solchen anderen Zwecken, bei denen von vornherein ausgeschlossen werden kann, dass sie in den Anwendungsbereich der Richtlinie (EU) 2016/680 fallen, zählen

zum Beispiel die in § 36 LDSG a.F. genannten Zwecke der Durchführung innerdienstlicher planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, die dem Dienstbetrieb im engeren Sinne dienen. Ferner fallen darunter die Bewältigung von Gefahrenlagen ohne jeglichen Bezug zu einer Straftat oder Ordnungswidrigkeit, eindeutig festgestellte Suizide und der Schutz privater Rechte auf Antrag des Berechtigten im Sinne des § 2 Absatz 2.

Da die Polizei sowohl Aufgaben im Anwendungsbereich der Verordnung (EU) 2016/679 als auch im Anwendungsbereich der Richtlinie (EU) 2016/680 wahrnimmt, hat sie bei der Datenverarbeitung künftig im Einzelfall darauf zu achten, welchem Datenschutzregime sie unterliegt. Entweder sie handelt zu den in der Richtlinie (EU) 2016/680 definierten Zwecken der Straftatenverhütung und -verfolgung, dann unterliegt sie nach Absatz 1 den §§ 11 bis 16 und den Vorschriften des 3. Abschnitts, denen gegebenenfalls aber besondere Rechtsvorschriften des Bundes vorgehen. Oder sie handelt zu anderen Zwecken, in diesem Fall gilt nach Absatz 2 die Verordnung (EU) 2016/679 sowie das Landesdatenschutzgesetz.

Zu Absatz 3
Die Richtlinie (EU) 2016/680 nimmt keine Unterscheidung zwischen automatisierter und nichtautomatisierter Verarbeitung von Daten vor. Zur Eröffnung des Anwendungsbereichs bedarf es allerdings einer Speicherung in einem System, in dem die Daten nach einer gewissen Ordnung gespeichert und damit gezielt auffindbar sind. Unsortierte Handakten oder ähnlich unstrukturierte Aufzeichnungen unterfallen folglich nicht dem Anwendungsbereich der §§ 11 bis 16 sowie der Vorschriften des 3. Abschnitts.

3. Zu § 12 (Begriffsbestimmungen - Datenverarbeitung)
Die Vorschrift setzt Artikel 3 der Richtlinie (EU) 2016/680 um. Sie definiert Begrifflichkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten.

Der Begriff der „Verarbeitung“ (Ziffer 2) umfasst gemäß Artikel 3 Nummer 2 der Richtlinie (EU) 2016/680 sämtliche Vorgänge im Zusammenhang mit personenbezogenen Daten, unabhängig davon, ob sie automatisiert oder nicht automatisiert ausge-

führt werden. Die bisherige Unterscheidung zwischen der Erhebung, der Nutzung beziehungsweise Verwendung sowie der Übermittlung von Daten entfällt damit grundsätzlich, weil alle diese Vorgänge vom Begriff der „Verarbeitung“ erfasst werden. Zur Konkretisierung des jeweiligen Vorgangs werden die bisherigen Begrifflichkeiten in den Vorschriften teilweise dennoch weiter verwendet, insbesondere in den §§ 14 bis 16, die allgemeine Regeln für die Erhebung, die weitere Verarbeitung und die Übermittlung von Daten aufstellen.

Der bislang gebrauchte Begriff der „Datei“ geht in dem von der Richtlinie (EU) 2016/680 verwendeten und auch in der Entscheidung des Bundesverfassungsgerichts angelegten Begriff des „Dateisystems“ (Ziffer 6) auf.

Zum Zweck der Übersichtlichkeit wird die in Artikel 10 der Richtlinie (EU) 2016/680 enthaltene Definition der „besonderen Kategorien personenbezogener Daten“ aufgenommen (Ziffer 15).

Für die „Einwilligung“ wird die Definition aus Artikel 4 Ziffer 11 der Verordnung (EU) 2016/679 übernommen (Ziffer 18). Erwägungsgrund 35 der Richtlinie (EU) 2016/680 eröffnet die Möglichkeit, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke der Richtlinie (EU) 2016/680 zustimmen kann, wenn dies in einer Rechtsvorschrift vorgesehen ist.

Da die Richtlinie (EU) 2016/680 keine Unterscheidung zwischen automatisierter und nicht automatisierter Datenverarbeitung macht, kann diese Begriffsbestimmung, die das Landesdatenschutzgesetz in seiner alten Fassung noch vorsah, entfallen.

4. Zu § 13 (Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten)
Die Aufnahme dieser Vorschrift erfolgt in Umsetzung von Artikel 4 Absatz 1 und Absatz 4 der Richtlinie (EU) 2016/680 und ist überwiegend deklaratorischer Natur. Die festgelegten Grundsätze werden in den übrigen Vorschriften für die Verarbeitung personenbezogener Daten in konkretisierter Form umgesetzt, können in ihrer abstrakten Form aber bei der teleologischen Auslegung der übrigen Vorschriften herangezogen werden. Die Aufnahme der Grundsätze ins Gesetz resultiert auch daraus,

dass der Rückgriff auf ein allgemeines Landesdatenschutzgesetz für den Anwendungsbereich der Richtlinie (EU) 2016/680 nicht mehr möglich ist und sich damit alle einzuhaltenden datenschutzrechtlichen Grundprinzipien aus dem bereichsspezifischen Polizeirecht selbst ergeben müssen.

In Nummer 2 wird der Grundsatz der Zweckbindung normiert, der in § 15 Absatz 2 näher ausgestaltet wird.

Das Übermaßverbot in Nummer 3 entspricht dem schon nach bisheriger Rechtslage geltenden datenschutzrechtlichen Grundsatz der Datenminimierung beziehungsweise Datensparsamkeit und bedeutet, dass die Daten auf das für den jeweiligen Verarbeitungszweck notwendige Maß beschränkt sein müssen.

Nummer 5 setzt Artikel 7 Absatz 1 der Richtlinie (EU) 2016/680 um und konkretisiert den Grundsatz der sachlichen Richtigkeit. Aussagen von Opfern, Zeugen oder sonstigen Hinweisgebern basieren oft auf der subjektiven Wahrnehmung der aussagenden Personen und sind nicht immer nachprüfbar. Ob solche Daten den Tatsachen entsprechen, kann daher nicht immer eindeutig festgestellt werden. Infolgedessen kann sich der Grundsatz der sachlichen Richtigkeit diesbezüglich lediglich auf die Tatsache beziehen, dass eine bestimmte Aussage gemacht worden ist. Um solche auf persönlichen Einschätzungen beruhenden personenbezogenen Daten von nachweisbaren Fakten unterscheiden zu können, sind sie soweit wie möglich entsprechend kenntlich zu machen, zum Beispiel durch Angabe der Herkunft der Daten.

Aus Erwägungsgrund 26 der Richtlinie (EU) 2016/680 ergibt sich das zusätzliche grundsätzliche Erfordernis, dass die Datenverarbeitung in einer für die betroffene Person nachvollziehbaren Weise erfolgen muss. Nach demselben Erwägungsgrund steht dieser Umstand der Durchführung von Maßnahmen wie verdeckten Ermittlungen oder Videoüberwachung durch die Strafverfolgungsbehörden aber nicht entgegen. Danach können diese Maßnahmen zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, getroffen werden, sofern sie durch Rechtsvorschriften geregelt

sind und eine erforderliche und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft darstellen, bei der die berechtigten Interessen der betroffenen Person gebührend berücksichtigt werden. Um Missverständnissen vorzubeugen, die sich aus einer zusammenhanglosen Festschreibung des Transparenzkriteriums ergeben könnten, wird auf dessen explizite Aufnahme im Wortlaut dieser Vorschrift verzichtet, zumal es auch im Wortlaut des betreffenden Artikels 4 Absatz 1 a) der Richtlinie (EU) 2016/680 im Unterschied zum Wortlaut des betreffenden Artikels 5 Absatz 1 a) der Verordnung (EU) 2016/679 keinen Niederschlag findet.

Die Nachweispflicht in Satz 2 folgt aus Artikel 4 Absatz 4 der Richtlinie (EU) 2016/680.

5. Zu § 14 (Allgemeine Regeln für die Erhebung personenbezogener Daten)
Die Vorschrift legt allgemeine Regeln für die Erhebung von Daten fest.

Die Absätze 1 bis 3 entsprechen, bis auf geringfügige redaktionelle Änderungen, den Regelungen des § 19 PolG a.F.. Die Regelungen können beibehalten werden, da sie mit den Vorgaben der Richtlinie (EU) 2016/680 in Einklang stehen.

Absatz 3 ist bezüglich offener Maßnahmen als Ergänzung zur allgemeinen Informationspflicht nach § 85 zu sehen. Während die allgemeine Informationspflicht durch Erteilung allgemein gültiger Hinweise, zum Beispiel auf der Homepage, erfüllt werden kann, verlangt Absatz 3 die Benennung der Rechtsgrundlage gegenüber einer konkreten betroffenen Person sowie den Hinweis auf das Bestehen einer Auskunftspflicht oder auf die Freiwilligkeit der Auskunft im Einzelfall. Artikel 13 Absatz 2 der Richtlinie (EU) 2016/680 verlangt einen Hinweis auf die Rechtsgrundlage zwar nur „in besonderen Fällen“, damit der betroffenen Person die Ausübung ihrer Rechte ermöglicht wird. Diese Vorgabe wird in der Vorschrift über die Benachrichtigungspflicht bei verdeckten und eingriffsintensiven Maßnahmen umgesetzt, die insoweit als „besondere Fälle“ gelten. Dennoch wird Absatz 3, der für offen erhobene Daten gilt, inhaltlich unverändert aus § 19 PolG a.F. übertragen. Denn zum einen sollen die neuen Vorschriften nicht hinter dem Datenschutzniveau der alten Vorschriften zurückstehen und zum anderen sollte jedenfalls dann, wenn die betroffene Person die Benennung der Rechtsgrundlage verlangt, gleichermaßen von einem besonderen Fall im Sinne

des Artikels 13 Absatz 2 der Richtlinie (EU) 2016/680 ausgegangen werden, weil die betroffene Person zur Ausübung ihrer Rechte dann darauf angewiesen ist, dass ihrem Auskunftsverlangen nachgekommen wird.

6. Zu § 15 (Allgemeine Regeln für die weitere Verarbeitung personenbezogener Daten)

Die neue Vorschrift normiert die Voraussetzungen der Zweckbindung und der zweckändernden weiteren Verarbeitung von Daten und setzt dabei den vom Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 konkretisierten Grundsatz der hypothetischen Datenneuerhebung um. Die Regelung gilt für jegliche Datenverarbeitung durch die Polizei, unabhängig von der Eingriffsintensität der ursprünglichen Erhebung.

Zu Absatz 1

Absatz 1 setzt Artikel 8 Absatz 1 der Richtlinie (EU) 2016/680 um und lehnt sich dabei an § 16 Absatz 1 BKAG an. Die weitere Verarbeitung von erhobenen Daten ist zulässig, wenn sie zur Aufgabenerfüllung erforderlich ist, die Voraussetzungen einer der nachfolgenden Absätze zur Zweckbindung oder Zweckänderung vorliegen und keine besonderen zusätzlichen gesetzlichen Voraussetzungen zu erfüllen sind.

Die Ebene des Verantwortlichen wurde in der gesamten Vorschrift bewusst in Polizeibehörden sowie Dienststellen und Einrichtungen des Polizeivollzugsdienstes aufgeteilt, um deutlich zu machen, dass auch eine weitere Verarbeitung von Daten durch eine andere dieser Stellen innerhalb der Polizei beziehungsweise eine Übermittlung an eine andere dieser Stellen innerhalb der Polizei grundsätzlich eine Zweckänderung darstellt. Eine wesentliche Voraussetzung, die das Bundesverfassungsgericht für die Bindung an den ursprünglichen Zweck aufgestellt hat, ist die Verarbeitung durch denselben Verantwortlichen. Da aber auch die Übermittlung an eine andere der genannten Stellen innerhalb der Polizei eine Zweckänderung darstellt, muss der Verantwortliche in diesem Sinne auf die einzelne Polizeibehörde, Dienststelle oder Einrichtung heruntergebrochen werden.

Zu Absatz 2

Absatz 2 beschreibt den Grundsatz der Zweckbindung und regelt damit die weitere Verarbeitung personenbezogener Daten im Rahmen des ursprünglichen Zwecks, zu dem die Daten erhoben wurden.

Satz 1 legt fest, in welchem Rahmen die Verarbeitung von Daten noch vom ursprünglichen Erhebungszweck erfasst ist. Das ist der Fall, wenn die Daten durch dieselbe verantwortliche Stelle zur Wahrnehmung derselben Aufgabe und zum Schutz derselben Rechtsgüter oder zur Verhütung oder Verfolgung derselben Straftaten oder Ordnungswidrigkeiten weiter verarbeitet werden. Das Bundesverfassungsgericht führt hierzu in seinem Urteil (Rn. 278 f., 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.“

Die Speicherung seitens der erhebenden Behörde, auch wenn sie in den polizeilichen Dateien erfolgt und die Daten damit weiteren Behörden zugänglich sind, ist in der Regel vom ursprünglichen Zweck erfasst und fällt damit unter Absatz 2.

Satz 2 legt für solche Daten, die die Polizei nicht selbst erhoben hat, die aber dennoch bei ihr vorhanden sind (sogenannte „aufgedrängte“ Daten) fest, dass für diese der Zweck der Speicherung zu berücksichtigen ist. Satz 3 bestimmt, dass für solche Daten, die aus der eingriffsintensiven Maßnahme der Wohnraumüberwachung stammen, eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz unabhängig von einer dringenden Gefahr nicht in Betracht kommt. Vielmehr ist in diesem Fall Voraussetzung, dass eine solche Gefahr vorliegt, die auch diese Vorschrift selbst verlangt.

Zu Absatz 3

Absatz 3 Satz 1 regelt die weitere Verarbeitung personenbezogener Daten zu einem anderen Zweck als dem, zu dem sie erhoben wurden, solange der neue Zweck ebenfalls in den Anwendungsbereich der Richtlinie (EU) 2016/680 fällt. Nach Erwägungsgrund 27 der Richtlinie (EU) 2016/680 müssen die zuständigen Behörden personenbezogene Daten, die im Zusammenhang mit der Verhütung, Ermittlung, Aufdeckung oder Verfolgung einer bestimmten Straftat oder Ordnungswidrigkeit erhoben wurden, auch in einem anderen Kontext verarbeiten können, um sich ein Bild von den einzelnen Handlungen machen und Verbindungen zwischen verschiedenen aufgedeckten Straftaten oder Ordnungswidrigkeiten herstellen zu können. In Absatz 3 wird der vom Bundesverfassungsgericht für solche Zweckänderungen aufgestellte Grundsatz der hypothetischen Datenneuerhebung gesetzlich verankert. Danach ist Voraussetzung für eine erlaubte Zweckänderung, dass die Neuerhebung der Daten mit vergleichbaren Mitteln nach den geltenden Rechtsvorschriften zulässig sein müsste und die Verarbeitung für diesen anderen Zweck erforderlich und verhältnismäßig ist.

Das Bundesverfassungsgericht (Rn. 288 bis 290) hat 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 diesbe-

züglichen 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.“

Es kommt folglich darauf an, ob die weitere Straftat / das neu zu schützende Rechtsgut entsprechend schwer wiegend / bedeutsam zu den Straftaten oder Rechtsgütern ist, die von der ursprünglich zu Grunde liegenden Datenerhebungsbefugnis generell geschützt werden. Diese Unterscheidung ist insbesondere in solchen Fällen bedeutsam, in denen mit einer niederschwelligen Datenerhebungsmaßnahme zunächst schwer wiegende Straftaten verhütet / bedeutsame Rechtsgüter geschützt werden sollen und sich dabei konkrete Ermittlungsansätze zur Verhütung weniger schwer wiegender Straftaten / zum Schutz weniger bedeutsamer Rechtsgüter ergeben. Die weitere Verarbeitung der erlangten Daten ist in diesen Fällen zulässig, wenn die niederschwellige Datenerhebungsmaßnahme zur Verhütung der weniger schwer wiegenden Straftat / zum Schutz des weniger bedeutsamen Rechtsguts zulässig wäre. Die vom Bundesverfassungsgericht geforderte Vergleichbarkeit muss sich also an der Erhebungsschwelle der jeweiligen Maßnahme ausrichten.

Satz 1 erfüllt diese verfassungsrechtlichen Anforderungen und lässt demgemäß die Verarbeitung personenbezogener Daten zur Erfüllung polizeilicher Aufgaben zu anderen Zwecken als denjenigen, zu denen sie erhoben worden sind, nur zu, wenn nach Maßgabe der jeweiligen Datenerhebungsvorschrift mindestens entsprechend gewichtige Straftaten oder Ordnungswidrigkeiten verhütet, ermittelt, aufgedeckt oder

verfolgt oder mindestens entsprechend bedeutsame Rechtsgüter geschützt werden sollen und sich im Einzelfall konkrete Ermittlungsansätze zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung solcher Straftaten oder Ordnungswidrigkeiten ergeben oder zur Abwehr von in einem überschaubaren Zeitraum drohenden Gefahren für solche Rechtsgüter erkennen lassen.

Der Grundsatz der hypothetischen Datenneuerhebung wurde vom Bundesverfassungsgericht zwar nur für die beschwerdegegenständlichen besonders eingriffsintensiven Maßnahmen aufgestellt. Der dahinter stehende Grundgedanke ist jedoch allgemeiner Natur und sollte für jede Form der Datenverarbeitung, unabhängig von der jeweiligen Eingriffsintensität der ursprünglichen Erhebungsmaßnahme, Gültigkeit besitzen. Die Übertragung des Grundsatzes auf alle Vorgänge der Datenverarbeitung wird daher für das Polizeigesetz als angemessen und folgerichtig angesehen. Je schwerwiegender der Eingriff, desto schwerwiegender müssen die damit verfolgten Straftaten bzw. desto bedeutsamer die dadurch geschützten Rechtsgüter sein. Ein weniger schwerwiegender Eingriff ist auch für die Verhütung oder Verfolgung weniger schwerwiegender Straftaten bzw. zum Schutz weniger bedeutsamer Rechtsgüter zulässig. In Anbetracht der Tatsache, dass jede weitere Datenverarbeitung einen erneuten Eingriff darstellt, ist die zweckändernde weitere Verarbeitung an diesen Maßstäben zu messen.

In Satz 1 geht ferner § 38 Absatz 1 PolG a.F. auf, so dass dieser entfallen kann. Nach dieser Vorschrift konnten personenbezogene Daten, die im Rahmen von Ermittlungsverfahren bekanntgeworden sind, also zu repressiven Zwecken erhoben wurden, gespeichert, verändert und genutzt werden, soweit und solange dies zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten, also zu präventiven Zwecken, erforderlich ist. Nach der neuen Regelung kommt es hingegen nicht mehr darauf an, ob Daten zu präventiven oder repressiven Zwecken erhoben wurden, solange die Erhebung rechtmäßig erfolgt ist. Wenn die Voraussetzungen des Satzes 1 in Verbindung mit Absatz 1 vorliegen, dürfen gespeicherte Daten zu anderen Richtlinien-Zwecken weiter verarbeitet werden, unabhängig davon, ob der ursprüngliche Erhebungszweck präventiver oder repressiver Natur war. Die Einschränkungen in § 38 Absatz 1 PolG a.F. für Daten, die durch bestimmte Maßnahmen nach der Strafprozessordnung erhoben wurden, gehen ebenfalls in der neuen Vorschrift

auf, da in ihnen bereits der Grundsatz der hypothetischen Datenneuerhebung angelegt war, der nunmehr umfassend auf alle zweckändernden weiteren Verarbeitungen übertragen wird.

Satz 2 regelt, dass es abweichend von Satz 1 zulässig ist, die Grunddaten einer Person zu ihrer Identifizierung weiter zu verarbeiten. 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 Polizei muss daher zur Erfüllung ihrer Aufgaben die Grunddaten einer Person stets zu diesem Zweck verarbeiten können. Durch die enge Begrenzung der Verarbeitung auf die Grunddaten einerseits und den alleinigen Zweck der Identifizierung andererseits ist es mit den Vorgaben des Bundesverfassungsgerichts vereinbar, dass für diese Maßnahme die strengen Vorgaben der Zweckbindung und des Grundsatzes der hypothetischen Datenneuerhebung nicht gelten.

Satz 3 entspricht der Regelung des Absatzes 2 Satz 2 in Bezug auf „aufgedrängte“ Daten, die die Polizei nicht selbst erhoben hat. Satz 4 regelt entsprechend Absatz 2 Satz 3, dass für die weitere Verarbeitung solcher Daten, die aus der besonders eingriffsintensiven Maßnahme der Wohnraumüberwachung gewonnen wurden, eine solche Gefahr vorliegen muss, wie sie auch von dieser Vorschrift über die eingriffsintensive Maßnahme selbst gefordert wird.

Satz 6 regelt entsprechend den Anforderungen des Artikels 13 Absatz 5 GG, dass personenbezogene Daten, die mit Hilfe technischer Mittel zur Überwachung von Wohnungen erlangt wurden, die ausschließlich zum Eigenschutz der bei einem Einsatz in Wohnungen tätigen Personen vorgesehen sind, nur zu den dort bestimmten Zwecken und nur dann weiter verarbeitet werden dürfen, wenn die Rechtmäßigkeit der Maßnahme zuvor richterlich festgestellt ist. Bei Gefahr im Verzug ist die Entscheidung unverzüglich nachzuholen. Hintergrund für diesen Regelung ist, dass in Fällen der Wohnraumüberwachung zur Eigensicherung nach Artikel 13 Absatz 5 Satz 1 GG zwar keine vorherige richterliche Entscheidung erforderlich ist. Bei einer nachträglichen Zweckänderung der dadurch erlangten Daten muss die richterliche Entscheidung jedoch nachgeholt werden (vgl. Art 13 Absatz 5 Satz 2 GG). Die Vorschrift

kann Daten betreffen, die nach § 45 oder § 50 erlangt wurden. Mangels anderweitiger Regelung finden für diese Fälle die Zuständigkeits- und Verfahrensregelungen des § 132 Anwendung.

Zu Absatz 4
Absatz 4 regelt die weitere Verarbeitung personenbezogener Daten zu einem anderen Zweck als dem, zu dem sie erhoben wurden, wenn der neue Zweck nicht in den Anwendungsbereich der Richtlinie (EU) 2016/680 und damit nicht in den Anwendungsbereich dieses Gesetzes fällt. Voraussetzung für die Zulässigkeit einer solchen zweckändernden weiteren Verarbeitung ist nach Satz 1 eine ausdrückliche Erlaubnisnorm oder eine ausdrückliche Einwilligung der betroffenen Person, die zuvor über alle Umstände der weiteren Datenverarbeitung informiert worden sein muss. Satz 2 stellt klar, dass in diesen Fällen für die weitere Verarbeitung der Daten die Verordnung (EU) 2016/679 sowie die ergänzenden Bestimmungen des Landesdatenschutzgesetzes gelten. Satz 3 bestimmt, dass Daten, die aus der besonders eingriffsintensiven Maßnahme der Wohnraumüberwachung gewonnen wurden, nicht zu Zwecken verarbeitet werden dürfen, die außerhalb des Anwendungsbereichs der Richtlinie (EU) 2016/680 liegen.

Fälle, in denen personenbezogene Daten zu Zwecken erhoben wurden, die in den Anwendungsbereich der Verordnung (EU) 2016/679 fallen und zu anderen Zwecken weiter verarbeitet werden sollen, die entweder in den Anwendungsbereich der Verordnung (EU) 2016/679 oder in den der Richtlinie (EU) 2016/680 fallen, haben sich nach den Bestimmungen zur zweckändernden weiteren Verarbeitung zu richten, die sich aus der Verordnung (EU) 2016/679 und dem sie ergänzenden Landesdatenschutzgesetz ergeben.

Die Einhaltung der Bestimmungen dieser Vorschrift ist durch organisatorische und technische Vorkehrungen sicherzustellen.

7. Zu § 16 (Allgemeine Regeln für die Übermittlung personenbezogener Daten)
Die Vorschrift bestimmt allgemeine Regeln für die Übermittlung von Daten.

Zu Absatz 1

Absatz 1 Satz 1 bis 3 dient der Umsetzung von Artikel 7 Absatz 2 der Richtlinie (EU) 2016/680.

Die Pflicht zur Vermeidung einer Übermittlung unvollständiger Daten ist selbstverständlich auf solche Fälle zu beziehen, bei denen zum Zeitpunkt der (erstmaligen) Übermittlung bereits bekannt ist, dass der zu übermittelnde Datensatz unvollständig ist. Hingegen ist nicht jene Fallkonstellation gemeint, bei der sich im Nachhinein herausstellt, dass ein bereits übermittelter Datensatz unvollständig ist und dieser nun durch eine weitere (unvollständige) Übermittlung vervollständigt werden soll, die Vervollständigung unvollständiger Daten mithin also Sinn und Zweck der Datenübermittlung ist.

Bei der Anwendung der Vorschrift ist zu beachten, dass die Frage, ob Daten noch aktuell sind, nur im konkreten Zusammenhang und unter Beachtung des konkreten Verarbeitungszwecks zu beurteilen ist. Auch die Übermittlung von unter abstrakten Gesichtspunkten nicht (mehr) aktuellen Daten wie alte Meldeadressen, abweichende Geburtsnamen etc. können bedeutsam und für die Aufgabenerfüllung erforderlich und damit im konkreten Zusammenhang noch „aktuell“ sein.

Satz 4 dient der Umsetzung von Artikel 7 Absatz 3 der Richtlinie (EU) 2016/680. Dabei kann § 43 Absatz 3 Satz 2 PolG a.F. inhaltsgleich übernommen werden. Der Folgesatz in Artikel 7 Absatz 3 der Richtlinie (EU) 2016/680, wonach in diesen Fällen eine Berichtigung, Löschung oder Einschränkung der Verarbeitung der personenbezogenen Daten vorzunehmen ist, bedarf keiner eigenen Umsetzung, weil sich diese Verpflichtung bereits aus § 75 ergibt. Die empfangende Stelle unterliegt dieser Verpflichtung zwar nicht direkt aus diesem Gesetz, hat jedoch ihrerseits Vorschriften anzuwenden, mit denen die Vorgaben der Richtlinie (EU) 2016/680 gleichermaßen umgesetzt sein müssen.

Zu Absatz 2
Absatz 2 setzt Artikel 9 Absatz 3 der Richtlinie (EU) 2016/680 um.

Beispiele für besondere Bedingungen in diesem Sinne können Zweckbindungsregelungen für die weitere Verarbeitung durch den Empfänger, Fristen für die Löschung

beziehungsweise die Überprüfung der Erforderlichkeit der weiteren Speicherung, das Verbot der Weiterübermittlung ohne Genehmigung oder Konsultationserfordernisse vor der Beauskunftung betroffener Personen sein.

Zu Absatz 3
Absatz 3 setzt Artikel 9 Absatz 4 der Richtlinie (EU) 2016/680 um.

8. Zu §§ 17 bis 25 (Ermächtigung zum Erlass von Polizeiverordnungen bis Außerkrafttreten)
Die Regelungen entsprechen den §§ 10 bis 17 des bisherigen PolG. Die Verweise werden aufgrund der neuen Nummerierung des Gesetzes angepasst.

9. Zu § 26 (Ordnungswidrigkeiten)
Die Regelung entspricht weitgehend § 18 des bisherigen PolG.

In Absatz 2 wird auf die Bestimmung der Mindestgeldbuße in Höhe von fünf Euro verzichtet, da § 17 Absatz 1 des Gesetzes über Ordnungswidrigkeiten diese ohnehin zwingend vorgibt.

Mit dem neu eingefügten Absatz 3 werden die Kommunen in die Lage versetzt, durch Polizeiverordnung zu regeln, ob Gegenstände, auf die sich eine Ordnungswidrigkeit im Sinne von Absatz 1 bezieht oder die zu ihrer Vorbereitung oder Begehung verwendet worden sind, eingezogen werden können. Als Anwendungsbereich kommen vor allem Regelungen in Polizeiverordnungen in Betracht, die das Mitführen von gefährlichen, jedoch nicht verbotenen Gegenständen untersagen. In diesen Fällen dürften die Voraussetzungen des § 39 Absatz 1 regelmäßig nicht gegeben sein. Bei einem Verstoß gegen eine solche in einer Polizeiverordnung geregelten bußgeldbewehrten Verbotsnorm können die betroffenen Gegenstände künftig nicht nur beschlagnahmt (vgl. § 38 Absatz 1 Nummer 1) sondern auch eingezogen und somit dem Betroffenen dauerhaft entzogen werden, sofern dies in der Verordnung entsprechend vorgesehen ist. Damit kann im Einzelfall – insbesondere bei „uneinsichtigen“ Personen - unabhängig von der Verhängung eines Bußgelds eine nachhaltige generalpräventive Wirkung erzielt werden. Gleichzeitig kann die Polizei einen erneuten Verstoß mit demselben Gegenstand verhindern.

Durch die Regelung wird eine Lücke im Polizeigesetz geschlossen. Denn die Einziehung von Gegenständen als Nebenfolge einer Ordnungswidrigkeit ist nur zulässig, soweit es das Gesetz ausdrücklich zulässt (§ 22 Absatz 1 OWiG). In den meisten übrigen Bundesländern bestehen bereits vergleichbare Regelungen.

10. Zu § 27 (Personenfeststellung)
Die Regelung entspricht weitgehend § 26 des bisherigen PolG.

Zusätzlich werden in Absatz 1 die bisherigen polizeilichen Befugnisse zur Feststellung der Identität einer Person erweitert (Nummer 2) sowie die Nummern 5 und 6 (bisher § 26 Absatz 1 Nummern 4 und 5 PolG a.F.) an die höchstrichterliche Rechtsprechung des Bundesverfassungsgerichts angepasst.

a) Durch Einfügen einer neuen Nummer 2 ist die Identitätsfeststellung einer Person künftig auch zulässig, wenn diese bei oder im Zusammenhang mit öffentlichen Veranstaltungen und Ansammlungen angetroffen wird, die ein besonderes Gefährdungsrisiko im Sinne des § 44 Absatz 1 Satz 2 aufweisen und dort erfahrungsgemäß mit der Begehung von Straftaten gegen Leib, Leben oder Sachen von bedeutendem Wert zu rechnen ist.

Dabei sind öffentliche Veranstaltungen zu einem bestimmten Zweck gezielt veranlasste Zusammenkünfte einer größeren Anzahl von Personen, die grundsätzlich jedermann offenstehen, sei es auch erst nach Erfüllung bestimmter Bedingungen, z.B. Zahlung eines Eintrittsgeldes oder bestimmte Kleidung, aber nicht auf die Meinungsäußerung oder –bildung gerichtet sind. Öffentliche Ansammlungen sind zufällige Zusammenkünfte einer größeren Anzahl von Personen, die zumeist durch äußere Ereignisse bedingt sind (vgl. Belz/Mussmann/Kahlert/Sander, Polizeigesetz für Baden-Württemberg, 8. Auflage, § 21 Rn. 6 f.). Die Kontrolle von Teilnehmern einer Versammlung nach Artikel 8 GG ist von der Ermächtigungsgrundlage nicht erfasst. Durch die Formulierung „bei oder im Zusammenhang mit“ wird klargestellt, dass auch die Vor- bzw. Nachphase der Veranstaltung und Ansammlung umfasst ist. Erforderlich ist aber ein innerer Zusammenhang zwischen der Veranstaltung / Ansammlung und den polizeilichen Maßnahmen, d.h. eine räumliche und zeitliche Beziehung.

Durch den Verweis auf § 44 Absatz 1 Satz 2 liegt ein besonderes Gefährdungsrisiko zum einen vor, wenn Veranstaltungen und Ansammlungen von terroristischen Anschlägen bedroht sind. Dabei muss sich die Annahme einer Bedrohung aus einer aktuellen Gefährdungsanalyse ergeben. Damit wird der Nachweis eines erhöhten abstrakten Gefährdungsrisikos verlangt. Die Wahrscheinlichkeit eines Schadenseintritts muss sich aus einer aktuellen systematischen Untersuchung des Geschehens ergeben, wobei die Untersuchung auf der Basis von Tatsachen erfolgen muss (vgl. Belz/Mussmann/Kahlert/Sander, a.a.O., § 21 Rn. 13).

Zum anderen liegt ein besonderes Gefährdungsrisiko vor, wenn aufgrund der Art und Größe der Veranstaltungen und Ansammlungen erfahrungsgemäß erhebliche Gefahren für die öffentliche Sicherheit entstehen können. Das Vorliegen einer konkreten Gefahr ist hier zwar nicht erforderlich (vgl. Belz/Mussmann/Kahlert/Sander, a.a.O., § 21 Rn. 16), die Annahme der erheblichen Gefahr muss aber trotzdem durch konkrete auf Tatsachen gestützte Erfahrungswerte gerechtfertigt sein. Ein allgemeiner Hinweis auf eine bestimmte Veranstaltungsart und –größe genügt nicht, die Gefährlichkeit muss sich aus der Art und Größe im Einzelfall ergeben.

Darüber hinaus muss dort erfahrungsgemäß mit der Begehung von Straftaten gegen Leib, Leben oder Sachen von bedeutendem Wert zu rechnen sein.

Mit dem zweiten Halbsatz wird klargestellt, dass die Polizei bei der Auswahl der Person in besonderem Maße den Grundsatz der Verhältnismäßigkeit zu beachten hat. Der neu eingefügte Tatbestand verfolgt das Ziel, potentielle Straftäter aus ihrer Anonymität zu holen und dadurch Straftaten zu verhindern. Daher hat die Polizei vor allem bei der konkreten Auswahl eines Betroffenen auch unter Berücksichtigung vorhandener Erfahrungswerte besonders sorgfältig zu überprüfen, ob die vorgesehene Maßnahme im Hinblick auf die Zielsetzung der Regelung angemessen erscheint.

b) Mit den Änderungen in den Nummern 5 und 6 wird den Vorgaben des Bundesverfassungsgerichts aus seiner Entscheidung vom 18. Dezember 2018 (1 BvR 2795/09) Rechnung getragen. Die bisher bestehenden Regelungen (§ 26 Absatz 1 Nummern 4 und 5 PolG a.F.) dienten ihrem Wortlaut nach der Fahndung von Straftätern, also

einer repressiven Zielrichtung. Das Bundesverfassungsgericht hat hierzu ausgeführt, dass dem Land dafür die Gesetzgebungskompetenz fehle, da der Bund diese bereits ausgeschöpft habe.

Daher waren die Regelungen anzupassen und eindeutig mit präventiver Zielrichtung zu versehen. Nach der neugefassten Nummer 5 kann die Identität einer Person festgestellt werden, wenn sie an einer Kontrollstelle angetroffen wird, die von der Polizei eingerichtet worden ist, um Straftaten mit erheblicher Bedeutung (vgl. § 49 Absatz 3) zu verhindern. In Anlehnung an vergleichbare Vorschriften aus den übrigen Bundesländern und zur Beachtung des Grundsatzes der Verhältnismäßigkeit wird der Anwendungsbereich auf die Verhinderung von Straftaten mit erheblicher Bedeutung eingeschränkt. Die neue Nummer 6 regelt nunmehr die Identitätsfeststellung innerhalb eines Kontrollbereichs, der von der Polizei eingerichtet worden ist, um bestimmte Straftaten zu verhindern. Um dem im Verhältnis zu Nummer 5 leicht erhöhten Eingriff gerecht zu werden, wird der Anwendungsbereich diesbezüglich auf die Verhinderung von in § 100a der Strafprozessordnung bezeichneten Straftaten beschränkt und damit noch etwas enger gefasst.

11. Zu § 28 (Vorladung)
Die Regelung entspricht § 27 des bisherigen PolG.

12. Zu § 29 (Gefährderansprache / -anschreiben, Gefährdetenansprache)
Absatz 1 Satz 1 legt die Voraussetzungen fest, unter denen die Polizei eine Gefährderansprache durchführen bzw. ein Gefährderanschreiben versenden darf. Danach müssen Tatsachen die Annahme rechtfertigen, dass die betroffene Person in einem überschaubaren Zeitraum die öffentliche Sicherheit stören wird. Liegen diese Voraussetzungen vor, kann die Polizei dieser Person unter Hinweis auf die geltende Rechtslage mitteilen, dass sie unter Beobachtung steht und welche präventiven oder repressiven polizeilichen Maßnahmen im Fall einer bevorstehenden oder erfolgten Störung ergriffen werden. Durch diese „Ermahnung“ soll der Betroffene von der Störung abgehalten werden. Als Anwendungsfälle kommen beispielsweise gewaltbereite Problemfans vor Fußballspielen, strafrechtlich bereits in Erscheinung getretene Demonstrationsteilnehmer vor bestimmten Versammlungen, jugendliche Intensivtäter, häusliche Gewalttäter vor der Rückkehr in die Wohnung, Stalker, Sexualstraftäter vor

der Haftentlassung bzw. bei Wiederholungsgefahr aus anderen Gründen oder in Einzelfällen auch Personen, die dem islamistischen Spektrum zuzurechnen sind, in Betracht.

Eine Gefährderansprache, mit der infolge des damit verbundenen Einschüchterungs- und Abschreckungseffekts auf die Entschließungsfreiheit der betroffenen Person eingewirkt werden soll, kann insbesondere einen Eingriff in das Erziehungsrecht der Eltern nach Artikel 6 Absatz 2 Satz 1 GG (z.B. bei jugendlichen Intensivtätern), in das Versammlungsrecht nach Artikel 8 Absatz 1 GG oder das Recht auf Meinungsfreiheit nach Artikel 5 Absatz 1 GG (z.B. bei einer Einflussnahme auf die Teilnahme an einer Versammlung) oder das Recht auf allgemeine Handlungsfreiheit nach Artikel 2 Absatz 1 GG darstellen. Darüber hinaus kann auch ein Eingriff in das allgemeine Persönlichkeitsrecht nach Artikel 2 Absatz 1 i.V.m. Art. 1 Absatz 1 GG vorliegen, wenn eine Gefährderansprache vor Dritten durchgeführt wird, wie z.B. am Arbeitsplatz oder im Beisein von Nachbarn. Diese verfassungsmäßig geschützten Rechte können jedoch durch ein formelles Gesetz, wie der vorliegenden Regelung, eingeschränkt werden.

Es wird darauf hingewiesen, dass bloße Belehrungen oder einfache Hinweise, die mit keinem Grundrechtseingriff in diesem Sinne verbunden sind, weiterhin auf die allgemeine Aufgabenzuweisungsnorm des § 1 Absatz 1 PolG gestützt werden können.

Absatz 1 Satz 2 berechtigt die Polizei, die betroffene Person zu den in Satz 1 genannten Zwecken anzusprechen oder sie anzuschreiben.

Eine Gefährderansprache sollte im Regelfall an der Wohnung der betroffenen Person durchgeführt werden. An einem anderen Ort kommt diese Maßnahme beispielsweise in Betracht, wenn ein fester Wohnsitz nicht besteht oder nicht bekannt ist, die Person an der Wohnung nicht angetroffen wird, die Ansprache an der Wohnung den Zweck der Maßnahme gefährden würde oder anlässlich einer anderen polizeilichen Maßnahme erfolgt.

Um den mit einer Gefährderansprache verbundenen Eingriff möglichst gering zu halten und eine Stigmatisierung des Betroffenen zu vermeiden, ist eine Durchführung

der Maßnahme vor Dritten, insbesondere am Arbeitsplatz der betroffenen Person, aus Gründen der Verhältnismäßigkeit nur zulässig, soweit dies zur Zweckerreichung unerlässlich ist.

Absatz 2 normiert die Voraussetzungen unter denen die Polizei eine sog. Gefährdetenansprache durchführen kann. Danach müssen Tatsachen die Annahme rechtfertigen, dass eine Person in einem überschaubaren Zeitraum eine Straftat begehen oder zu ihrer Begehung beitragen wird, die sich gegen Leib, Leben, Freiheit, sexuelle Selbstbestimmung, den Bestand oder die Sicherheit des Bundes oder eines Landes oder bedeutende fremde Sach- oder Vermögenswerte richtet. Anders als bei der in Absatz 1 geregelten Gefährderansprache /-anschreiben sind bevorstehende Störungen der öffentlichen Sicherheit nicht ausreichend. Sind die Voraussetzungen gegeben, kann die Polizei andere Personen über die bestehenden Risiken informieren, sofern diese als Opfer der drohenden Straftat in Betracht kommen oder deren Kenntnis von der drohenden Straftat aus anderen Gründen unbedingt erforderlich ist.

Ein Anwendungsbereich ist im Bereich der Sexualdelikte zu finden. Wiederholt kommt es vor, dass Kontaktpersonen von KURS-Probanden hinsichtlich der bestehenden Risiken gewarnt werden müssen, weil tatsächliche Anhaltspunkte für die Begehung einer weiteren Straftat bestehen. Dies gilt beispielsweise für die neue Lebenspartnerin des betroffenen KURS-Probanden, wenn diese Kinder hat und der Betroffene wegen Kindesmissbrauchs verurteilt worden war oder etwa für den Vorstand eines Sportvereins wenn sich der Betroffene als Trainer im Jugendbereich bewirbt. Im Bereich der häuslichen Gewalt kann es bei einem einschlägig in Erscheinung getretenen Gewalttäter ebenfalls erforderlich werden, die ehemalige oder die neue Lebenspartnerin und ggfls. auch deren Familie über bestehende Risiken zu informieren.

Zudem kommt es durch Angehörige bestimmter Milieus, bspw. Rockervereinigungen oder Gruppierungen, die der organisierten Kriminalität zuzuordnen sind, wiederkehrend zu schweren Gewaltstraftaten gegen ehemalige Mitglieder oder Angehörige anderer Vereinigungen, die sich zwar gegen bestimmte Personen richten, aber deren direktes Umfeld ggfls. ebenso erheblich gefährdet ist.

Dabei stellt die Gefährdetenansprache einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Person dar, von der die Begehung einer Straftat droht. Der Eingriff in dieses Grundrecht kann jedoch durch ein formelles Gesetz, wie der vorliegenden Regelung, eingeschränkt werden.

Absatz 2 Satz 2 berechtigt die Polizei, die betroffene Person zu den in Satz 1 genannten Zwecken anzusprechen.

13. Zu § 30 (Platzverweis, Aufenthaltsverbot, Wohnungsverweis, Rückkehrverbot, Annäherungsverbot)
Die Regelung entspricht weitgehend § 27a des bisherigen PolG. In Absatz 2 wird mit dem neu angefügten Satz 4 klargestellt, dass sich nach Ablauf eines Aufenthaltsverbotes ein weiteres anschließen kann, jedoch nur, wenn dieses aufgrund einer neuen Gefahrenprognose gerechtfertigt ist (vgl. Urteil des VGH Baden-Württemberg vom 18. Mai 2017, 1 S 1193/16).

14. Zu § 31 (Aufenthaltsvorgabe und Kontaktverbot zur Verhütung terroristischer Straftaten)
Die Regelung entspricht im Wesentlichen § 27b des bisherigen PolG. § 27b PolG a.F. ist – gemeinsam mit den Ermächtigungsgrundlagen zur Telekommunikationsüberwachung (§ 23b PolG a.F.; im vorliegenden Gesetzentwurf § 54) und zur elektronischen Aufenthaltsüberwachung zur Verhütung terroristischer Straftaten (§ 27c PolG a.F.; im vorliegenden Gesetzentwurf § 32) - mit dem Gesetz vom 28. November 2017 (GBl. S. 631) in das Polizeigesetz eingefügt worden. Angesichts der hohen Grundrechtsintensität solcher Eingriffe sind die Maßnahmen jeweils an Richtervorbehalte geknüpft. Nach der Konzeption des geltenden Rechts ist dabei das Amtsgericht zuständig, in dessen Bezirk die zuständige Polizeidienststelle ihren Sitz hat (§ 23b Absatz 4 Satz 1, § 27b Absatz 3 Satz 1, § 27c Absatz 5 Satz 1 PolG a.F.). Hieraus folgt, dass insgesamt vierzehn Amtsgerichte mit Anträgen nach den §§ 23b, 27b, 27c PolG a.F. befasst werden können.

Nach Inkrafttreten der gesetzlichen Regelungen hat sich jedoch gezeigt, dass die neuen gerichtlichen Zuständigkeiten die betroffenen Amtsgerichte vor beachtliche Herausforderungen stellen können. Denn den Fällen der §§ 23b, 27b, 27c PolG a.F.

ist es eigen, dass richterliche Entscheidungen mit erheblicher Tragweite in sehr kurzer Zeit getroffen werden sollten; dies zudem in einem vergleichsweise speziellen Regelungsbereich. Hieraus ergeben sich hohe Anforderungen an die Einarbeitung der mit Fällen dieser Art befassten Richterinnen und Richter.

Angesichts dieser Herausforderungen hat die Präsidentin des Oberlandesgerichts Stuttgart den Vorschlag unterbreitet, die gerichtlichen Zuständigkeiten für Anordnungen nach §§ 23b, 27b, 27c PolG a.F. bei jeweils einem Amtsgericht je Oberlandesgerichtsbezirk zu konzentrieren. Weiter hat die Präsidentin des Oberlandesgerichts Stuttgart angeregt, die Zuständigkeiten bei größeren Amtsgerichten zu bündeln, denen nach § 162 Absatz 1 StPO auch Zuständigkeiten des Ermittlungsrichters zugewiesen sind, weil die Befugnisse nach §§ 23b, 27b, 27c PolG a.F. oftmals im Grenzbereich zwischen Prävention und Repression angesiedelt sind.

Aufgrund der daraufhin erfolgten Neubewertung der Sachlage hat sich das Ministerium der Justiz und für Europa dafür ausgesprochen, den Vorschlag der Präsidentin des Oberlandesgerichts Stuttgart aufzugreifen und die Zuständigkeiten nach §§ 23b, 27b, 27c PolG a.F. bei zwei Präsidentenamtsgerichten mit Ermittlungsrichterzuständigkeit zu bündeln (Amtsgerichte Stuttgart und Mannheim).

Diesem Vorschlag trägt Absatz 3 Satz 6 Rechnung. Die Vorschrift ermöglicht es, ein ausreichendes Fallaufkommen bei den Gerichten zu gewährleisten.

Soweit in Absatz 3 PolG keine speziellen Regelungen getroffen werden, ergibt sich das einschlägige Verfahrensrecht aus der „vor die Klammer gezogenen“ neuen Bestimmung des § 132.

15. Zu § 32 (Elektronische Aufenthaltsüberwachung zur Verhütung terroristischer Straftaten)
Die Regelung entspricht weitgehend § 27c des bisherigen PolG. Die bislang in Absatz 2 Sätze 5, 7, 8 und 9 enthaltenen Regelungen zur Kennzeichnung bzw. Protokollierung der aus einer entsprechenden Maßnahme erhobenen Daten sind nunmehr zentral in §§ 72 und 73 geregelt. Absatz 5 wird hinsichtlich der gerichtlichen Zuständigkeiten und des einschlägigen Verfahrensrechts neu gefasst. Für die in Absatz 5

Satz 6 vorgesehene Konzentration der gerichtlichen Zuständigkeiten bei den Amtsgerichten Mannheim und Stuttgart wird auf die Ausführungen zu § 31 Bezug genommen. Das einschlägige Verfahrensrecht ergibt sich nunmehr aus der „vor die Klammer gezogenen“ neuen Bestimmung des § 132, soweit in Absatz 5 keine speziellen Regelungen getroffen werden. Zudem werden die Verweise aufgrund der neuen Nummerierung des Gesetzes angepasst.

16. Zu § 33 (Gewahrsam)
Die Regelung entspricht mit geringfügigen Anpassungen § 28 des bisherigen PolG.

Da mittlerweile keine wie auch immer gearteten Verstöße allein gegen die öffentliche Ordnung denkbar sind, die eine Ingewahrsamnahme einer Person rechtfertigen könnten, wird diese bisher in § 28 Absatz 1 Nummer 1 bestehende Alternative ersatzlos gestrichen.

Absatz 4 trifft spezielle Regelungen zu den gerichtlichen Zuständigkeiten und zum gerichtlichen Verfahren. Auf die allgemeine Vorschrift des § 132 kann in Gewahrsamsangelegenheiten nur zurückgegriffen werden, soweit dies Absatz 4 Satz 8 ausdrücklich bestimmt (§ 132 Absatz 2 Sätze 2 und 4 bis 6 sowie Absatz 3). Für die richterliche Entscheidung nach Absatz 3 Satz 3 ist – abweichend von § 132 Absatz 1 – das Amtsgericht zuständig, in dessen Bezirk die in Gewahrsam genommene Person festgehalten wird; über die Beschwerde entscheidet – abweichend von § 132 Absatz 2 Satz 3 – das Landgericht. Dies entspricht dem derzeit geltenden Recht. Auch der eingeschränkte Verweis in Absatz 4 Satz 2 auf das Verfahrensrecht des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit schreibt das bislang geltende Recht fort.

Im neuen Absatz 4 Satz 3 wird ergänzt, dass eine richterliche Entscheidung auch aus sonstigen Gründen ohne persönliche Anhörung der in Gewahrsam genommenen Person ergehen kann, wenn diese außerstande ist, den Gegenstand der persönlichen Anhörung durch das Gericht ausreichend zu erfassen und in der Anhörung zur Feststellung der entscheidungserheblichen Tatsachen beizutragen. Diese Änderung geht auf einen Vorschlag aus der gerichtlichen Praxis zurück. Dort wurden Fallkonstellationen identifiziert, die im Einzelfall ebenfalls einen Verzicht auf eine persönliche

Anhörung rechtfertigen können. Zum einen sind dies Sachverhalte, wenn die Person, die in Gewahrsam genommen werden soll, zwar anhörungsfähig ist, jedoch ein entsprechender Dolmetscher trotz Ausschöpfung aller bestehenden Möglichkeiten nicht rechtzeitig zu erreichen ist. Gleiches kann in besonderen Einzelfällen bei äußerst aggressiven Personen in Betracht kommen, bei denen die Anhörung für den jeweiligen Anzuhörenden mit nicht unerheblichen Gefahren verbunden sein kann.

17. Zu § 34 (Durchsuchung von Personen)
Die Regelung entspricht weitgehend § 29 des bisherigen PolG.

Entsprechend § 27 Absatz 1 Nummer 2 wird in Absatz 1 eine neue Nummer 3 eingefügt, die es der Polizei gestattet, eine Person zu durchsuchen, wenn sie bei oder im Zusammenhang mit öffentlichen Veranstaltungen und Ansammlungen angetroffen wird, die ein besonderes Gefährdungsrisiko im Sinne des § 44 Absatz 1 Satz 2 aufweisen und dort erfahrungsgemäß mit der Begehung von Straftaten gegen Leib, Leben oder Sachen von bedeutendem Wert zu rechnen ist. Mit dem zweiten Halbsatz wird auch hier klargestellt (vgl. § 27), dass die Polizei bei der Auswahl der Person in besonderem Maße den Grundsatz der Verhältnismäßigkeit zu beachten hat. Zur Begründung im Einzelnen wird auf die Ausführungen zu § 27 verwiesen.

Im Übrigen werden die Verweise aufgrund der neuen Nummerierung des Gesetzes sowie des Einfügens einer neuen Nummer 2 in § 27 Absatz 1 angepasst.

18. Zu § 35 (Durchsuchung von Sachen)
Die Regelung entspricht weitgehend § 30 des bisherigen PolG.

Entsprechend § 27 Absatz 1 Nummer 2 und § 34 Absatz 1 Nummer 3 wird eine neue Nummer 4 in die Regelung eingefügt, die es der Polizei gestattet, eine Sache zu durchsuchen, wenn sie sich am Ort oder in unmittelbarer Nähe von öffentlichen Veranstaltungen und Ansammlungen befindet, die ein besonderes Gefährdungsrisiko im Sinne des § 44 Absatz 1 Satz 2 aufweisen und dort erfahrungsgemäß mit der Begehung von Straftaten gegen Leib, Leben oder Sachen von bedeutendem Wert zu rechnen ist. Eine Durchsuchung von Sachen, die von Personen mitgeführt werden, die bei oder im Zusammenhang mit öffentlichen Veranstaltungen und Ansammlungen

angetroffen werden, die ein besonderes Gefährdungsrisiko im Sinne des § 44 Absatz 1 Satz 2 aufweisen, richtet sich nach § 35 Nummer 1 in Verbindung mit § 34 Absatz 1 Nummer 3. Zur Begründung im Einzelnen wird auf die Ausführungen zu § 27 verwiesen.

Im Übrigen werden die Verweise aufgrund der neuen Nummerierung des Gesetzes sowie des Einfügens einer neuen Nummer 2 in § 27 Absatz 1 angepasst.

19. Zu § 36 (Betreten und Durchsuchung von Wohnungen)
Die Regelung entspricht weitgehend § 31 des bisherigen PolG. Allerdings wird Absatz 4 in Anlehnung an die Entscheidung des BVerfG vom 12. März 2019 – 2 BvR 675/14 – dahingehend geändert, dass die Nachtzeit künftig ganzjährig die Stunden von 21 Uhr bis 6 Uhr umfasst. Die bisherige Differenzierung zwischen den Sommer- und Wintermonaten wird aufgehoben. Darüber hinaus werden die bisherigen Sätze 2 bis 4 des Absatzes 5 gestrichen, da das anzuwendende Verfahrensrecht für gerichtliche Entscheidungen aufgrund dieses Gesetzes „vor die Klammer gezogen“ und zentral im neuen § 132 geregelt wird.

20. Zu §§ 37 bis 41 (Sicherstellung bis Erkennungsdienstliche Maßnahmen)
Die Regelungen entsprechen weitestgehend den §§ 32 bis 36 des bisherigen PolG. Die Verweise werden aufgrund der neuen Nummerierung des Gesetzes angepasst. In § 38 Absatz 5 wird klarstellend geregelt, dass § 132 Absatz 2 Satz 2 keine Anwendung findet.

21. Zu § 42 (Verarbeitung personenbezogener Daten aufgrund einer Einwilligung)
Nach § 4 Absatz 1 LDSG a.F. war die Einwilligung der betroffenen Person als Alternative zu einer gesetzlichen Vorschrift eine ausreichende Grundlage für die Verarbeitung personenbezogener Daten. Aufgrund des Wegfalls der Geltung dieser Vorschrift für den Anwendungsbereich der Richtlinie (EU) 2016/680 muss im Polizeigesetz eine eigene Regelung getroffen werden.

Nach Erwägungsgrund 35 der Richtlinie (EU) 2016/680 soll in Fällen, in denen die Polizei eine betroffene Person auffordern oder anweisen kann, ihren Anordnungen

nachzukommen, eine Einwilligung keine rechtliche Grundlage für die Datenverarbeitung darstellen, weil die Einwilligung mangels einer echten Wahlfreiheit dann nicht als freiwillig abgegebene Willensbekundung betrachtet werden kann. Mit anderen Worten kann die Polizei zur Wahrnehmung ihrer Aufgaben gesetzlich dazu ermächtigt werden, Daten ohne Einwilligung der betroffenen Person zu verarbeiten. Allerdings wird den Mitgliedstaaten zugestanden, durch Rechtsvorschriften vorzusehen, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für Zwecke der Richtlinie zustimmen kann.

Es gibt Bereiche, in denen eine polizeiliche Datenverarbeitung erforderlich sein kann, obwohl sie nicht besonders gesetzlich geregelt ist und auch nicht für jeden denkbaren Einzelfall geregelt werden kann. Ein Anwendungsfall ist zum Beispiel die Durchführung von Zuverlässigkeitsüberprüfungen von Personen, für die ein privilegierter Zutritt zu einer besonders gefährdeten Veranstaltung beantragt wird. Gerade in der heutigen Zeit, mit einer hohen abstrakten Gefährdung durch terroristische Anschläge, gibt es zahlreiche Konstellationen, in denen aufgrund einer Gefährdungsbeurteilung die Notwendigkeit besteht, bestimmte Personen oder Personenkreise, die Zugang zu einer Veranstaltung erhalten sollen, auf ihre Zuverlässigkeit zu überprüfen. Insbesondere betrifft dies Personen, die im Umfeld von Veranstaltungen, wie etwa Festivals, beschäftigt sind oder Journalisten, die in diesem Zusammenhang eine Akkreditierung zu bestimmten sicherheitsrelevanten Bereichen begehren. In solchen Fällen besteht ein großes öffentliches Interesse daran, dass zu Zwecken der Gefahrenabwehr oder der Straftatenverhütung nur Personen Zutritt erhalten, die auf ihre Zuverlässigkeit überprüft wurden.

Ferner werden Zuverlässigkeitsüberprüfungen zum Schutz staatlicher Einrichtungen durchgeführt, zum Beispiel bei Personen, die zeitweisen Zugang zu sicherheitsrelevanten Bereichen öffentlicher Gebäude erhalten sollen, etwa Handwerker oder Reinigungspersonal. Die Durchführung der Zuverlässigkeitsüberprüfung richtet sich in diesen Fällen nach dem Landesdatenschutzgesetz, der von der Polizei vorzunehmende Datenabgleich jedoch nach dem Polizeigesetz.

Zur Durchführung einer Zuverlässigkeitsüberprüfung ist es grundsätzlich erforderlich, Grunddaten der betroffenen Person mit dem Datenbestand bestimmter polizeilicher

Dateien (z.B. POLAS) abzugleichen, um zu überprüfen, ob bereits Daten zu dieser Person gespeichert sind und aufgrund welcher Vorgänge. Sind zur Person Eintragungen vorhanden, ist anhand einer Einzelfallbeurteilung zu entscheiden, ob dadurch die Zuverlässigkeit im konkreten Fall in Frage gestellt wird.

Wird die Polizei von einer Behörde um Durchführung einer Zuverlässigkeitsüberprüfung ersucht, übermittelt sie ihr das Ergebnis des Datenabgleichs in der Regel einschließlich der festgestellten Erkenntnisse. Die ersuchende Behörde beurteilt anhand des Ergebnisses selbst, ob die Zuverlässigkeit gegeben ist oder nicht. Bei Ersuchen einer Stelle außerhalb des öffentlichen Bereichs übermittelt die Polizei keine Einzelheiten des Überprüfungsergebnisses, sondern teilt lediglich mit, ob Sicherheitsbedenken bestehen. Die abschließende Entscheidung trifft auch in letztgenanntem Fall die ersuchende Stelle, die jedoch mitzuteilen hat, ob sie beabsichtigt, der Empfehlung der Polizei zu folgen.

Wenn eine Person in einem als sicherheitsrelevant festgestellten Bereich eine Tätigkeit ausüben will, muss sie dieser Form der Verarbeitung ihrer Daten zustimmen, andernfalls muss sie auf die Tätigkeit in diesem Bereich verzichten. Dabei erscheint es vorzugswürdig, Zuverlässigkeitsüberprüfungen zwar auf der Grundlage einer gesetzlichen Regelung vorzunehmen, jedoch nicht ohne dass die betroffene Person zuvor über die Verarbeitung ihrer Daten umfassend informiert wird und der Verarbeitung ausdrücklich zustimmt. Denn dadurch wird der betroffenen Person zumindest die Möglichkeit belassen, die Einwilligung zu verweigern und sich der Zuverlässigkeitsüberprüfung zu entziehen. Zwar könnte in diesen Fällen die für eine Einwilligung grundsätzlich erforderliche Freiwilligkeit der Willensbildung angezweifelt werden, da häufig Arbeitnehmer- oder Auftragnehmerverhältnisse vorliegen, denen eine gewisse Abhängigkeit immanent ist. Allerdings ist dabei zu berücksichtigen, dass eine gesetzliche Befugnis ohne die Möglichkeit einer Einwilligung eine Willensbildung der betroffenen Person schon von vorneherein gänzlich ausschließen würde. Die Einholung einer informierten Einwilligung räumt der betroffenen Person hingegen überhaupt erst eine Entscheidungsmöglichkeit ein und stellt damit ein „Mehr“ gegenüber einer gesetzlichen Befugnis ohne Einwilligungsmöglichkeit dar.

Mit der vorliegenden Vorschrift wird daher die Befugnis der Polizei zur Datenverarbeitung auf der Grundlage einer informierten Einwilligung geschaffen.

Zu Absatz 1

Absatz 1 erteilt der Polizei in den genannten Fällen die Befugnis zur Datenverarbeitung zum Zweck der Durchführung einer Zuverlässigkeitsüberprüfung unter der Voraussetzung, dass ihr von der um Zuverlässigkeitsüberprüfung ersuchenden Stelle die Überprüfung der Identität der betroffenen Person und deren Einwilligung in die dafür erforderliche Datenverarbeitung gemäß den Anforderungen des Absatzes 2 schriftlich bestätigt werden. Die Verarbeitung der Daten umfasst dabei begrifflich insbesondere das Erheben der Daten, den Abgleich der Daten mit dem vorhandenen Datenbestand sowie die Übermittlung des Ergebnisses an die anfragende Stelle. In zahlreichen Fällen erfolgt eine Zuverlässigkeitsüberprüfung zwar aus Anlass einer entsprechenden Gefährdungsbeurteilung der Polizei im Rahmen ihrer allgemeinen Aufgabenwahrnehmung. Für den Nachweis der Zuverlässigkeit ist jedoch in aller Regel nicht die Polizei, sondern die tatsächlich ersuchende Stelle verantwortlich. Dies kann ein Unternehmer sein, der einen öffentlichen Auftrag erhalten hat und die Zuverlässigkeit seines Personals nachzuweisen hat oder ein Veranstalter, der auf Veranlassung der Genehmigungsbehörde oder der Polizei die Zuverlässigkeit der beschäftigten Personen nachzuweisen hat, beziehungsweise der Hausrechtsinhaber, wenn die Überprüfung zum Schutz staatlicher Einrichtungen erfolgt. Die Verantwortung für das Vorliegen ordnungsgemäßer Einwilligungserklärungen der betroffenen Personen verbleibt bei der um Zuverlässigkeitsüberprüfung ersuchenden Stelle, etwa dem Konzertveranstalter. Nur in Ausnahmefällen wird diese Verantwortung der Polizei zukommen, nämlich dann, wenn diese selbst um die Überprüfung von Personen ersucht, die Zutritt zu polizeilichen Liegenschaften erhalten sollen.

Die Einwilligung muss die mit der Zuverlässigkeitsüberprüfung verbundene Datenverarbeitung umfassen. Daraus folgt, dass im Einzelfall vor Einholung der Einwilligung festzulegen ist, welche Form der Datenverarbeitung (Erhebung welcher Daten, Abgleich mit den Beständen welcher Dateien, Übermittlung welcher Daten des Ergebnisses an welche Empfänger) erforderlich ist. Die betroffene Person muss vor Abgabe ihrer Willenserklärung hierüber umfassend informiert werden.

Zu Absatz 2

Absatz 2 regelt, welchen Anforderungen die Einwilligung der betroffenen Person genügen muss. Die betroffene Person muss zuvor ausreichend und in verständlicher Form über alle Umstände der Verarbeitung und die Folgen der Einwilligung oder ihrer Verweigerung informiert worden sein. Nur dann kann von einer informierten Einwilligung ausgegangen werden, die der betroffenen Person ein höchstmögliches Maß an Freiwilligkeit bei ihrer Willensbekundung einräumt.

Die Einwilligung sowie die zuvor erteilte Information sollten bei Bedarf von der ersuchenden Stelle in Schriftform nachgewiesen werden können, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Die Aufklärung hat in verständlicher und leicht zugänglicher Form zu erfolgen. Beispielsweise ist die Einwilligung im äußeren Erscheinungsbild der Erklärung hervorzuheben, wenn sie zusammen mit anderen Erklärungen schriftlich erteilt werden soll, damit sie von anderen Sachverhalten klar zu unterscheiden ist.

Die Verarbeitung besonderer Kategorien personenbezogener Daten, wie zum Beispiel die politische Meinung sowie religiöse oder weltanschauliche Überzeugungen, wird im Rahmen von Zuverlässigkeitsüberprüfungen in vielen Fällen unbedingt erforderlich sein beziehungsweise ergibt sich automatisch im Trefferfall, etwa bei einer Eintragung in einer Gewalttäterdatei, die unter anderem zwischen linkspolitisch, rechtspolitisch oder religiös motivierten Taten unterscheidet. Aufgrund des besonderen Schutzes solcher Daten muss sich die Einwilligung der betroffenen Person ausdrücklich auch auf diese Daten beziehen.

Zu Absatz 3

Absatz 3 bestimmt, dass die Polizei den Empfänger des Ergebnisses der Zuverlässigkeitsüberprüfung auf die Zweckbindung der Daten hinzuweisen hat und regelt, welche Daten an die ersuchende Stelle übermittelt werden dürfen. Dabei wird zwischen ersuchenden Stellen innerhalb und solchen außerhalb des öffentlichen Bereichs unterschieden. Einer ersuchenden öffentlichen Stelle wird mitgeteilt, ob und, soweit erforderlich, welche sicherheitsrelevanten Erkenntnisse vorliegen. In diesem Fall entscheidet die ersuchende Stelle selbst, ob die sicherheitsrelevanten Erkennt-

nisse im konkreten Einzelfall der Zuverlässigkeit der betroffenen Person entgegenstehen. Die Rückmeldung an eine ersuchende nicht öffentliche Stelle hat sich dagegen auf die Auskunft zu beschränken, ob Sicherheitsbedenken vorliegen. Hier nimmt die Polizei selbst die Einschätzung vor, ob sicherheitsrelevante Erkenntnisse der Zuverlässigkeit entgegenstehen. Details der Erkenntnisse werden nicht mitgeteilt. Allerdings hat die Polizei die ersuchende nicht öffentliche Stelle zu verpflichten, ihr mitzuteilen, ob diese beabsichtigt, der Empfehlung der Polizei zu folgen. Anderenfalls hätte die Polizei keinerlei Kontrolle darüber, ob ihrer Gefährdungseinschätzung Rechnung getragen wird.

Zu Absatz 4

Absatz 4 regelt, dass die Polizei die Ergebnisse der Zuverlässigkeitsüberprüfung zu Dokumentationszwecken aufzubewahren und zwölf Monate nach Abschluss der Überprüfung zu löschen hat. Davon umfasst sind sowohl positive als auch negative Überprüfungsergebnisse, da in beiden Fällen eine Dokumentation erforderlich sein kann, um die Überprüfung nachträglich nachvollziehen zu können. Allerdings kann die Aufbewahrung zu Dokumentationszwecken keine Wiederholungsprüfung ersetzen. Bei einem geplanten erneuten Einsatz einer betroffenen Person ist eine wiederholte Zuverlässigkeitsüberprüfung schon nach kurzer Zeit unvermeidbar, weil sich sicherheitsrelevante Erkenntnisse auch kurzfristig ergeben können.

Zu Absatz 5

Absatz 5 eröffnet die Möglichkeit weiterer Fälle von Datenverarbeitungen auf der Grundlage einer informierten Einwilligung. Die Regelung ist aufgrund des Wegfalls der bisherigen Regelung des § 4 LDSG a.F. erforderlich, um neben der Zuverlässigkeitsüberprüfung weitere Fallgestaltungen zu erfassen, in denen die Polizei allein auf der Grundlage einer Einwilligung der betroffenen Person, mithin ohne ausdrückliche gesetzliche Grundlage, Daten verarbeitet. Allerdings sollte von dieser Möglichkeit vor dem Hintergrund des Erwägungsgrundes 35 der Richtlinie (EU) 2016/680 nur restriktiv Gebrauch gemacht werden. Die Einholung einer Einwilligung als Grundlage der Datenverarbeitung sollte nur in sehr begrenzten Ausnahmefällen zur Anwendung kommen. In Betracht kommt die Anwendung vorrangig in solchen Fällen, in denen die Polizei Maßnahmen durchführt, die für die betroffene Person vorteilhaft sind und

die gleichzeitig der Straftatenverhütung und damit der polizeilichen Aufgabenwahrnehmung dienen. Hierunter fallen insbesondere die Ausstiegsberatung im Bereich des politisch oder religiös motivierten Extremismus und die Durchführung von Fallkonferenzen im Rahmen der behördenübergreifenden Zusammenarbeit in opferschutzbezogenen Angelegenheiten sowie bei Intensivstraftätern. Mit dem interdisziplinären Ansatz von (anlassbezogenen) Fallkonferenzen soll gerade in Fällen von häuslicher Gewalt eine übergreifende Situationsanalyse vorgenommen und abgestimmte Maßnahmen entwickelt werden, um die Gefahr von wiederholter Gewalt unter Kontrolle zu bringen. Um den bereits praktizierten Bedarf an einer Datenverarbeitung auf der Grundlage von Einwilligungen zu konkretisieren, jedoch die Möglichkeit für künftige, ähnlich gelagerte Fallkonstellationen zu belassen, wurden die genannten Anwendungsbereiche als Regelbeispiele normiert.

22. Zu § 43 (Befragung und Datenerhebung)
Die Befugnis zur Befragung und Datenerhebung war bislang gemeinsam mit den Kategorien betroffener Personen in § 20 PolG a.F. geregelt. Da die Kategorien betroffener Personen an die Vorgaben der Richtlinie (EU) 2016/680 anzupassen sind und nunmehr in einer eigenständigen Vorschrift definiert werden, wird in den neuen Absätzen 2 und 3 nur noch der erlaubte Zweck der Datenerhebung in Verbindung mit einem Verweis auf die jeweilige Kategorie betroffener Personen aufgelistet.

Die bisher in § 20 Absatz 4 PolG a.F. geregelte Befugnis zur Datenerhebung zum Zwecke der Vorbereitung auf die Gefahrenabwehr richtet sich künftig nach der Verordnung (EU) 2016/679 bzw. dem LDSG (vgl. § 11 Absatz 2). Gleiches gilt für die Befugnis zur Erhebung von Daten, wenn dies zum Schutz privater Rechte oder zur Vollzugshilfe erforderlich ist (bisher § 20 Absatz 5 PolG a.F.).

In Bezug auf die weiteren in § 70 definierten Kategorien betroffener Personen, nämlich die der verurteilten Straftäter und die jener Personen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie eine Straftat begangen haben, bedarf es keiner Datenerhebungsbefugnis im Polizeigesetz. Die Erhebung von Daten dieser Personen richtet sich vielmehr nach der Strafprozessordnung.

Zu Absatz 1

Absatz 1 wird bis auf wenige redaktionelle Anpassungen unverändert übernommen.

Zu Absatz 2

Absatz 2 erteilt der Polizei gemäß der Vorgängervorschrift die Befugnis zur Datenerhebung zur konkreten Gefahrenabwehr und bezieht sich nach wie vor sowohl auf Personen, die nach den §§ 6 oder 7 verantwortlich sind (Verhaltens- und Zustandsstörer) als auch auf andere Personen. Da der Störer nunmehr ausdrücklich als eigene Kategorie betroffener Personen definiert ist, wird aus Gründen der Einheitlichkeit als Verweisnorm die Vorschrift angeführt, die die verschiedenen Kategorien definiert.

Die Regelung umfasst auch die Befugnis zur Erhebung von Daten, die der Polizei durch Gerichtsvollzieherinnen und Gerichtsvollzieher zur Abschätzung der konkreten Gefährdungssituation bei einer beabsichtigten Vollstreckungsmaßnahme übermittelt werden (vgl. neue Regelung in § 13a AGGVG – Artikel II dieses Gesetzes).

Zu Absatz 3

Absatz 3 bestimmt die Befugnis zur Datenerhebung, soweit sie zur vorbeugenden Bekämpfung von Straftaten erforderlich ist, in Bezug auf folgende Kategorien betroffener Personen:

- Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat begehen werden oder deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines überschaubaren Zeitraums eine Straftat begehen werden,
- Opfer einer Straftat oder Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie Opfer einer Straftat sind oder werden,
- andere Personen wie insbesondere Zeugen, Hinweisgeber oder Kontakt- beziehungsweise Verbindungspersonen.

Hier ergeben sich aufgrund der Änderungen bei der Definition der verschiedenen Kategorien betroffener Personen automatisch entsprechende Änderungen bei der Befugnis zur Datenerhebung.

Zu Absatz 4

Absatz 4 entspricht § 20 Absatz 6 PolG a.F.

23. Zu § 44 (Offener Einsatz technischer Mittel zur Bild- und Tonaufzeichnung)
Die Regelung entspricht in weiten Teilen § 21 des bisherigen PolG.

Zu Absatz 2
Aufgrund der neuen Nummerierung des Gesetzes sowie des Einfügens einer neuen Nummer 2 in § 27 Absatz 1 wird der Verweis in Absatz 2 entsprechend angepasst.

Zu Absatz 5
In Satz 1 wird die bisherige Beschränkung des Einsatzes einer Bodycam auf öffentlich zugängliche Orte gestrichen.

Der neu eingefügte Satz 2 regelt, dass das Anfertigen von Bild- und Tonaufzeichnungen mittels körpernah getragener Aufnahmegeräte nach Satz 1 in Wohnungen nur zur Abwehr einer dringenden Gefahr für Leib oder Leben einer Person zulässig ist. Mit der Beschränkung auf dringende Gefahren wird den Vorgaben des Artikels 13 Absatz 7 GG bei der hier vorgesehenen Aufzeichnung personenbezogener Daten Rechnung getragen.

Dabei werden vom Begriff der Wohnung grundsätzlich auch Arbeits-, Betriebs- oder Geschäftsräume erfasst (vgl. Jarass/Pieroth, GG für die Bundesrepublik Deutschland, 14. Auflage 2016, Artikel 13 Rn. 5). Allerdings fallen die Anforderungen des Artikels 13 Absatz 7 GG geringer aus, wenn es sich um reine Arbeits-, Betriebs- oder Geschäftsräume handelt (vgl. Jarass/Pieroth, a.a.O., Artikel 13 Rn. 38). Das Bundesverfassungsgericht hat hierzu ausgeführt: „Je größer ihre Offenheit nach außen ist und je mehr sie zur Aufnahme sozialer Kontakte für Dritte bestimmt sind, desto schwächer ist der grundrechtliche Schutz“ (BVerfGE 97, 228, [266]). Somit ist hinsichtlich der vorliegenden Einschreitschwelle zwischen Arbeits-, Betriebs- und Geschäftsräumen auf der einen Seite und Wohnungen im engeren Sinne auf der anderen Seite eine Differenzierung vertretbar. Daher regelt der neu eingefügte Satz 3 quasi als Rückausnahme zu Satz 2, dass für den Einsatz einer Bodycam in Arbeits-, Betriebs oder Geschäftsräumen keine dringende Gefahr erforderlich ist. Satz 4 entspricht § 21 Absatz 5 Satz 2 des bisherigen PolG.

Zu Absatz 6

Absatz 6 regelt, dass die weitere Verarbeitung der Aufzeichnung einer Bodycam in Wohnungen einer richterlichen Zustimmung bedarf. Für die weitere Verarbeitung einer Aufzeichnung in Arbeits- Betriebs- oder Geschäftsräumen ist eine richterliche Zustimmung nicht erforderlich.

Zu Absatz 7

Der neu eingefügte Absatz 7 dient der Gewährleistung des verfassungsrechtlich garantierten Schutzes des Kernbereichs privater Lebensgestaltung beim polizeilichen Einsatz einer Bodycam in Wohnungen. Da nicht auszuschließen ist, dass im Rahmen einer entsprechenden Maßnahme in Wohnungen auch intime oder der innersten Privatsphäre zuzurechnende Sachverhalte ins Visier der Bodycam geraten können, stellt Satz 1 klar, dass solche Aufzeichnungen unzulässig sind. Satz 2 enthält das Gebot der unverzüglichen Unterbrechung der Maßnahme, falls sich während der Aufzeichnung tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte aus dem Kernbereich der persönlichen Lebensgestaltung erfasst werden. Aufzeichnungen hierüber sind nach Satz 3 unverzüglich zu löschen. Satz 4 regelt, dass die unterbrochene Maßnahme nur fortgesetzt werden darf, wenn durch sie keine Daten aus dem Kernbereich privater Lebensgestaltung mehr erhoben werden. Satz 5 sieht klarstellend vor, dass Erkenntnisse aus dem Kernbereich privater Lebensgestaltung nicht verwertet werden dürfen. Die bisherigen Absätze 6 bis 9 des § 21 PolG werden zu den Absätzen 8 bis 11.

Zu Absatz 8

Der neu eingefügte Satz 2 des Absatzes 8 berücksichtigt die Vorgaben des Artikels 13 Absatz 7 GG im Zusammenhang mit den erhöhten Anforderungen an die Speicherung von Daten, die durch den Einsatz einer Bodycam in Wohnungen aufgezeichnet wurden. Die Speicherung dieser aufgezeichneten Daten für eine Dauer von mehr als 60 Sekunden ist nur zulässig, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz von Polizeibeamten oder anderen Personen gegen eine dringende Gefahr für Leib und Leben erforderlich ist. Der neu eingefügte Satz 3 stellt klar, dass in Arbeits-, Betriebs- oder Geschäftsräumen eine „einfache“ Gefahr ausreichend ist

(vgl. hierzu auch die Ausführungen zu Absatz 5). Satz 4 entspricht weitestgehend § 21 Absatz 6 Satz 2 des bisherigen PolG.

Zu Absatz 11
Aufgrund der neu eingefügten Absätze 6 und 7 werden in Absatz 11 die Verweise entsprechend angepasst.

24. Zu § 45 (Aufzeichnung eingehender Telefonanrufe)
Die neue Vorschrift gibt dem Polizeivollzugsdienst die Ermächtigung zur Aufzeichnung bestimmter eingehender Telefonanrufe, soweit dies zu seiner Aufgabenerfüllung erforderlich ist. Zwar war die Aufzeichnung bestimmter eingehender Anrufe schon bislang auf der Grundlage allgemeiner polizeirechtlicher oder strafprozessrechtlicher Bestimmungen beziehungsweise auf der Grundlage ausdrücklicher oder konkludenter Einwilligungen der betroffenen Personen zulässig. Aus Gründen der Rechtssicherheit wird nunmehr jedoch eine ausdrückliche Rechtsgrundlage geschaffen.

Zu Absatz 1
Die Befugnis gilt nach Absatz 1 Nummer 1 zum einen für eingehende Notrufe. Deren Speicherung ist primär zur Gefahrenabwehr erforderlich, da Anrufer aufgrund einer akuten Stresssituation oft aufgeregt sind, so dass ihre Angaben unpräzise oder schwer verständlich sein können und ein erneutes Abspielen notwendig ist, um alle Informationen generieren zu können. Der Anrufer einer Notrufnummer hat im Normalfall ein ureigenes Interesse daran, dass alle erforderlichen Maßnahmen ergriffen werden, um ihm oder ihr schnellst- und bestmögliche Hilfe zu bieten, so dass in aller Regel auch eine zumindest konkludente Einwilligung der betroffenen Person zur Aufzeichnung des Notrufs vorliegen dürfte. Zudem gehört das wissentlich an die Adresse eines Strafverfolgungsorgans gerichtete Wort nicht der Privat- oder Intimsphäre an, die in Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG vor der Einwirkung der öffentlichen Gewalt geschützt ist (BVerfGE 34, 238). Eine Aufzeichnung von Notrufen ist mithin verhältnismäßig und verfassungsgemäß.

Zum anderen gilt die Befugnis nach Absatz 1 Nummer 2 für die Aufzeichnung von Anrufen auf solche Nummern, die der Bevölkerung zur Mitteilung sachdienlicher Hinweise bekannt gegeben werden. Das sind insbesondere die Rufnummern des Kriminaldauerdienstes, der Telefonzentrale, des Bürgertelefons, die zentralen Nummern der Öffentlichkeitsfahndung sowie Sonderrufnummern, die aus Anlass bestimmter Fahndungsmaßnahmen, zum Beispiel im Rahmen der Fernsehsendung „Aktenzeichen XY ungelöst“, eingerichtet werden und über die von Anrufern Hinweise gegeben werden, die für die Aufgabenerfüllung des Polizeivollzugsdienstes von Bedeutung sein können. Um die im Telefongespräch gemachten Angaben überprüfen zu können und die Auswertung der Äußerungen zu ermöglichen, kann es notwendig sein, die Telefongespräche aufzuzeichnen und dem Polizeivollzugsdienst damit über einen längeren, dennoch begrenzten, Zeitraum nutzbar zu machen.

Zu Absatz 2

Die aufgezeichneten Daten sind unverzüglich, spätestens aber nach drei Monaten zu löschen, es sei denn, sie werden zu den in Absatz 2 Satz 1 ausdrücklich genannten Zwecken weiterhin benötigt. Auch erst im Nachgang zu einem Anruf kann sich dessen Bedeutung als Ermittlungsansatz oder Beweismittel herausstellen, weshalb eine ausreichende Speicherfrist erforderlich ist. Da außerdem im Vergleich zu § 44 keine Bildaufzeichnungen angefertigt werden, erscheint angesichts des geringeren Eingriffs eine längere Speicherfrist angemessen. Ferner ist nach Absatz 2 Satz 4 in den Fällen des Absatzes 1 Nummer 2 in geeigneter Weise auf die Aufzeichnung hinzuweisen. Dies wird zweckmäßigerweise durch eine automatische Bandansage erfolgen. In den Fällen des Absatzes 1 Nummer 1 muss dieses Erfordernis aus Gründen der Dringlichkeit eines Notrufs, die keine weitere Verzögerung erlaubt, entfallen.

25. Zu § 46 (Projektbezogene gemeinsame Dateien mit dem Landesamt für Verfassungsschutz)

Die Vorschrift regelt die Befugnis zur Einrichtung gemeinsamer projektbezogener Dateien mit dem Landesamt für Verfassungsschutz und entspricht weitgehend der bisherigen Regelung in § 48 a PolG a.F.. Zwar sieht die Konzeption der künftigen polizeilichen Informationsstruktur keine vertikale Dateienlandschaft mehr vor, sondern soll aufgrund der Anforderungen des Grundsatzes der hypothetischen Datenneuer-

hebung horizontal aufgebaut sein. Für den Sonderbereich der gemeinsamen projektbezogenen Dateien soll dennoch am bisherigen Dateibegriff festgehalten werden, um der Besonderheit und der Bedeutung der Zusammenführung von Erkenntnissen und der gemeinsamen Verarbeitung personenbezogener Daten von Landeskriminalamt, Polizeidienststellen und Landesamt für Verfassungsschutz Rechnung zu tragen.

Die Änderungen sind überwiegend redaktioneller Art (in Absatz 1 Satz 2 Nummer 3 aufgrund der Änderung der Vorschriften des Außenwirtschaftsgesetzes), beziehungsweise erfolgen in Anpassung an Begrifflichkeiten der Richtlinie (EU) 2016/680 sowie an die vergleichbare Vorschrift des § 17 BKAG. Hierzu wird der Straftatenkatalog in Absatz 1 Satz 2 auf das gesamte Terrorismusstrafrecht ausgeweitet.

Anzuwendende Regelungen bezüglich der Pflichten zur Protokollierung, Kennzeichnung, Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten sowie zum Auskunftsrecht der betroffenen Person werden explizit genannt, weil projektbezogene gemeinsame Dateien aufgrund der Beteiligung des Landesamtes für Verfassungsschutz nicht ausschließlich den polizeilichen Vorschriften unterliegen und somit einen Sonderfall darstellen, für den die allgemeinen Regelungen nicht automatisch gelten.

26. Zu § 47 (Datenabgleich)
Die Vorschrift entspricht im Wesentlichen § 39 PolG a.F. Sie wird geringfügig an die vergleichbare Vorschrift des § 16 Absatz 4 BKAG angepasst.

Die vorgenommenen Änderungen sind aufgrund der künftigen Informationsstruktur des Bundeskriminalamtes notwendig, die keine Dateienlandschaft mehr vorsieht. In Anlehnung an die Formulierung des § 16 Absatz 4 BKAG wird daher auf den Begriff der „Datei“ verzichtet und stattdessen auf den Abgleich der Daten abgestellt, unabhängig von der Struktur, in der diese gespeichert sind. Dies lässt den Abgleich der Daten mit dem Inhalt von Dateien gleichermaßen zu, was für die Übergangszeit bis zur Inbetriebnahme der künftigen Informationsstruktur auch notwendig ist. So kann die Befugnis zum Abgleich von Daten sowohl auf das bisherige Dateiensystem als auch auf das künftige dateilose Informationssystem bzw. den Informationsverbund des Bundeskriminalamts angewendet werden.

Ferner werden, ebenfalls in Anpassung an § 16 Absatz 4 BKAG, die bisherigen Voraussetzungen nach § 39 Absatz 1 Satz 2 PolG a.F. dahingehend erleichtert, dass ein Abgleich von Daten anderer Personen bereits zulässig ist, wenn Grund zu der Annahme besteht, dass dies zur Wahrnehmung einer polizeilichen Aufgabe erforderlich ist.

Die Regelung umfasst auch die Befugnis zum Abgleich von Daten, die der Polizei durch Gerichtsvollzieherinnen und Gerichtsvollzieher zur Abschätzung der konkreten Gefährdungssituation bei einer beabsichtigten Vollstreckungsmaßnahme übermittelt werden (vgl. neue Regelung in § 13a AGGVG – Artikel II dieses Gesetzes).

Die in der Vorgängervorschrift enthaltene Befugnis des Polizeivollzugsdienstes, im Rahmen seiner Aufgabenwahrnehmung erlangte personenbezogene Daten mit dem Fahndungsbestand abzugleichen, kann entfallen, weil der Fahndungsbestand von den Daten im Sinne der Sätze 1 und 2 erfasst ist.

27. Zu § 48 (Rasterfahndung)
Die Vorschrift entspricht im Wesentlichen § 40 PolG a.F., wird jedoch an einigen Stellen sowohl redaktionell als auch inhaltlich angepasst.

Zu Absatz 1
In Absatz 1 wird die Eingriffsschwelle an die Anforderungen des Urteils des Bundesverfassungsgerichts vom 20. April 2016 angepasst. Die geschützten Rechtsgüter werden in Anlehnung an die Regelung des Bundeskriminalamtgesetzes („oder für wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen“) ergänzt.

Zu Absatz 2
In Absatz 2 wird der Begriff der „Datenübermittlung“ in „Datenerhebung“ geändert, weil es sich systematisch um eine Erhebungsbefugnis für die Polizei handelt und nicht um eine Übermittlungsbefugnis für die Stellen, die die Daten an die Polizei übermitteln. Ferner wird aufgrund der Bestimmungen der Richtlinie (EU) 2016/680 der Begriff der „Verwendung“ in „Verarbeitung“ geändert.

Zu Absatz 3

In Absatz 3 wird gemäß den Anforderungen des Urteils des Bundesverfassungsgerichts vom 20. April 2016 ein Richtervorbehalt aufgenommen. Dafür entfallen die bislang erforderliche Zustimmung des Innenministeriums sowie die Unterrichtung der Aufsichtsbehörde für den Datenschutz.

Zu Absatz 4

Durch Aufnahme des Zusatzes „unter Berücksichtigung von § 15“ wird die weitere Verarbeitung der mit der Rasterfahndung generierten Daten eingeschränkt. Die bisherige Formulierung („soweit sie nicht zur Verfolgung von Straftaten erforderlich sind“) war ohne diese Einschränkung vor dem Hintergrund des Grundsatzes der Zweckbindung zu weit gefasst. Die bislang enthaltene Regelung zur Benachrichtigungspflicht solcher Personen, gegen die nach Abschluss des Datenabgleichs weitere Maßnahmen durchgeführt werden, geht in der neu geschaffenen Vorschrift zur Benachrichtigungspflicht bei verdeckten und eingriffsintensiven Maßnahmen auf.

Zu Absatz 5

Absatz 5 schafft in Anlehnung an § 48 Absatz 3 BKAG eine Dokumentationspflicht, die der Einhaltung der Pflicht zur Benachrichtigung der betroffenen Personen sowie der Datenschutzkontrolle dient.

28. Zu § 49 (Besondere Mittel der Datenerhebung)

Mit der Regelung wird § 22 des bisherigen PolG an die Vorgaben der Entscheidung des Bundesverfassungsgerichts vom 20. April 2016 angepasst. Die in diesem Zusammenhang maßgeblichen Regelungen zur Benachrichtigung der betroffenen Personen, zur Protokollierung der erhobenen Daten, zur Kennzeichnung der Daten, zur Kontrolle der Datenerhebungen durch die Aufsichtsbehörde für den Datenschutz sowie zur Unterrichtung des Landtages finden sich in den §§ 72, 74, 86, 90 und 98 Absatz 1 Nummer 14.

Zu Absatz 1

In Absatz 1 werden die bislang in § 22 Absätze 2 und 3 geregelten Eingriffsvoraussetzungen für den Einsatz besonderer Mittel der Datenerhebung unter Berücksichtigung der Entscheidung des Bundesverfassungsgerichts vom 20. April 2016 neu gefasst.

Nummer 1 ersetzt § 22 Absatz 3 Nummer 1 des bisherigen PolG. Danach darf der Polizeivollzugsdienst die in Absatz 2 genannten besonderen Mittel der Datenerhebung zur Abwehr von Gefahren für hochrangige Rechtsgüter einsetzen, vorliegend Leib, Leben oder Freiheit einer Person, den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist. Als Adressaten einer entsprechenden Maßnahme kommen sowohl Störer nach den §§ 6 oder 7, aber auch Nichtstörer unter den Voraussetzungen des § 9 in Betracht (vgl. Rn. 159). Damit wird die bisherige Regelung des Polizeigesetzes (§ 22 Absatz 3 Nummer 1 i.V.m. § 20 Absatz 2 PolG a.F.) geringfügig eingeschränkt, die diesbezüglich auch eine Datenerhebung gegenüber anderen Personen zugelassen hat.

Die neuen Nummern 2 und 3 ersetzen § 22 Absatz 3 Nummer 2 des bisherigen PolG. Sie erlauben entsprechende Maßnahmen auch gegenüber Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat mit erheblicher Bedeutung begehen werden oder deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines überschaubaren Zeitraums eine Straftat mit erheblicher Bedeutung begehen werden. Damit wird den Vorgaben des Bundesverfassungsgerichts aus seiner Entscheidung vom 20. April 2016 und den darin aufgestellten Anforderungen an die zu treffende Prognoseentscheidung bezüglich der Gefahrenlage im Vorfeld einer konkreten Gefahr für die Begehung terroristischer Straftaten Rechnung getragen (vgl. Rn. 112 sowie 162 ff.). § 22 Absatz 3 Nummer 2 i.V.m. § 20 Absatz 3 Nummer 1 des bisherigen PolG enthielt eine vergleichbare Regelung, wie die vom Bundesverfassungsgericht als zu unbestimmt bemängelte Regelung des § 20g Absatz 1 Nummer 2 BKAG a.F.. Aufgrund der unterschiedlichen Aufgabenwahrnehmung des Bundeskriminalamts und der Polizei in Baden-Württemberg war die Regelung jedoch auf Straftaten mit erhebli-

cher Bedeutung und nicht auf terroristische Straftaten beschränkt. Das Bundesverfassungsgericht hat in diesem Zusammenhang ausdrücklich offen gelassen, wo diesbezüglich die verfassungsrechtlichen Grenzen im Allgemeinen, etwa auch für entsprechende Befugnisse ohne Terrorismusbezug nach den Landespolizeigesetzen liegen (vgl. Rn. 156). Aus Gründen der Verhältnismäßigkeit erscheint es jedoch erforderlich, die neue Regelung des Polizeigesetzes wie bisher dahingehend einzuschränken, dass die prognostizierte Rechtsgutverletzung von bestimmten besonders qualifizierten Straftaten ausgehen muss. Diese bisher schon enthaltene Beschränkung auf Straftaten mit besonderer Bedeutung im Sinne des Absatzes 2 dürfte den Anforderungen des Bundesverfassungsgerichts genügen.

Mit Satz 1 Nummer 4 wird geregelt, dass sich entsprechende Maßnahmen auch auf Kontakt- und Verbindungspersonen einer der in Nummern 2 oder 3 genannten Personen erstrecken dürfen. Allerdings ist ein Eingriff nur gerechtfertigt, wenn die Kontakt- und Verbindungsperson in einem besonderen Näheverhältnis zu dieser Person steht und von der Vorbereitung einer Straftat mit erheblicher Bedeutung Kenntnis hat, aus der Verwertung der Tat Vorteile ziehen oder die Person nach den Nummern 2 oder 3 sich ihrer zur Begehung der Straftat bedienen könnte.

Um die Verhältnismäßigkeit einer Maßnahme nach Absatz 1 zu gewährleisten, wird wie bisher in allen Fällen vorausgesetzt, dass die Abwehr der Gefahr oder die Verhütung der Straftat auf andere Weise gefährdet oder erheblich erschwert wäre. Die Maßnahmen dürfen auch dann durchgeführt werden, wenn unbeteiligte Dritte betroffen sind (vgl. § 22 Absatz 4 PolG a.F.).

§ 22 Absatz 2 des bisherigen PolG geht im neuen Absatz 1 vollständig auf und bedarf keiner ausdrücklichen Regelung mehr.

Zu Absatz 2

Absatz 2 entspricht bis auf eine redaktionelle Änderung (Nummer 2) der Regelung des § 22 Absatz 1 des bisherigen PolG.

Zu Absatz 3

Absatz 3 entspricht § 22 Absatz 5 des bisherigen PolG.

Zu Absatz 4

Die neue Regelung in Absatz 4 dient der verfahrensmäßigen Absicherung und unterwirft die in Satz 1 genannten eingriffsintensiven Maßnahmen dem nach der Rechtsprechung des Bundesverfassungsgerichts vom 20. April 2016 (Rn. 117 und 174) erforderlichen Richtervorbehalt. Der Antrag auf richterliche Entscheidung ist durch die Leitung eines regionalen Polizeipräsidiums, des Polizeipräsidiums Einsatz oder des Landeskriminalamts schriftlich zu stellen und zu begründen. Eine Delegation der Antragsbefugnis auf besonders beauftragte Beamte des höheren Dienstes ist möglich. Bei Gefahr im Verzug kann die Anordnung auch von einer der in Satz 3 genannten Personen selbst getroffen werden. Eine Delegation der Anordnungsbefugnis auf besonders beauftragte Beamte des höheren Dienstes ist diesbezüglich möglich. Die als Eilfall getroffene Anordnung bedarf der unverzüglichen Bestätigung durch das Gericht. Die übrigen Maßnahmen nach Absatz 2 sind außer bei Gefahr im Verzug durch die in Satz 3 genannten Personen anzuordnen. Eine Delegation der Anordnungsbefugnis auf besonders beauftragte Beamte des höheren Dienstes ist auch hier möglich.

Zu Absatz 5

Absatz 5 setzt die Anforderungen des Bundesverfassungsgerichts (vgl. Rn. 118) an den zu stellenden Antrag um.

Zu Absatz 6

Absatz 6 Satz 1 sieht vor, dass die Anordnungen schriftlich zu ergehen haben. Durch die schriftliche Fixierung wird der äußere Rahmen abgesteckt, innerhalb dessen die heimliche Maßnahme durchzuführen ist, sodass der Eingriff messbar und kontrollierbar bleibt. Die Anordnung des Gerichts muss die Angabe der Person enthalten, gegen die sich die Maßnahme richtet, soweit möglich mit Name und Anschrift. Daneben müssen Art, Umfang und Dauer der Maßnahme angegeben werden sowie die wesentlichen Gründe. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, solange die Voraussetzungen für die Maßnahme fortbestehen. Für das gerichtliche Verfahren gelten die Vorschriften über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (vgl. § 132).

Zu Absatz 7
Absatz 7 entspricht § 24 des bisherigen PolG.

Zu Absatz 8
Absatz 8 normiert, wie vom Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 (Rn. 119 ff., 176 f.) gefordert, eine ausdrückliche gesetzliche Kernbereichsregelung für Maßnahmen nach Absatz 2. Dem Kernbereichsschutz ist nach den Ausführungen des Bundesverfassungsgerichts auf zwei Ebenen Rechnung zu tragen (Rn. 177): „Der Gesetzgeber hat hierzu in normenklarer Weise Schutzvorkehrungen sowohl auf der Ebene der Datenerhebung als auch auf der Ebene der Datenauswertung und Datenverwertung vorzusehen."

Nach Satz 1 ist daher vor der Durchführung einer Maßnahme nach Absatz 2, also auf der Erhebungsebene, eine Prognose dahingehend zu treffen, ob mit der Maßnahme Äußerungen erfasst werden, die allein den Kernbereich der persönlichen Lebensgestaltung betreffen. Diese Prognose muss sich auf tatsächliche Anhaltspunkte stützen. Vollständige Gewissheit ist nicht erforderlich. Schützenswert ist insbesondere die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens. Zu diesen Personen können insbesondere Ehe- oder Lebenspartner, Geschwister und Verwandte in gerader Linie, vor allem, wenn sie im selben Haushalt leben, sowie Strafverteidiger, Ärzte, Geistliche und enge persönliche Freunde zählen.

Satz 2 stellt zum Schutz des Kernbereichs privater Lebensgestaltung beim Einsatz von Verdeckten Ermittlern und Vertrauenspersonen sicher, dass die Maßnahme zu unterbrechen ist, sobald dies ohne Gefährdung der beauftragten Person möglich ist.

Satz 3 enthält das Gebot der unverzüglichen Unterbrechung der Maßnahmen nach Absatz 2 Nummern 1 bis 3 und regelt, was zu unternehmen ist, wenn sich während der Überwachung unerwartet tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte aus dem Kernbereich der persönlichen Lebensgestaltung erfasst werden. Bestehen diesbezüglich Zweifel, darf in den Fällen des Absatzes 2 Nummer 2 Buchstabe a und b nach Satz 4 nur noch eine automatische Aufzeichnung fortgesetzt werden. Die Re-

gelung dient dem Schutz des Kernbereichs, indem sie bestimmt, dass auch in solchen Fällen, in denen keine eindeutigen Anhaltspunkte für eine Kernbereichsrelevanz sprechen, eine unmittelbare Überwachung durch die ausführenden Stellen ausgeschlossen ist. Diese den Kernbereichsschutz sichernden Verfahrensvorschriften erfüllen die verfassungsrechtlichen Vorgaben des Bundesverfassungsgerichts, indem bereits auf der Erhebungsebene ein Eingriff in den Kernbereich der privaten Lebensgestaltung weitestgehend ausgeschlossen wird.

Nach Satz 5 sind Aufzeichnungen von Zweifelsfällen unverzüglich dem anordnenden Gericht vorzulegen, welches nach Satz 6 unverzüglich die Feststellung zu treffen hat, ob eine Kernbereichsrelevanz vorliegt oder nicht und damit eine Entscheidung über die Löschung oder Verwertbarkeit der Daten trifft. Eine solche Regelung für Zweifelsfälle trägt dem Umstand Rechnung, dass es häufig bei einmaligem Mithören nicht möglich sein wird, das Geschehen vollständig zu erfassen. Es kann insbesondere erforderlich werden, ein Gespräch mehrfach abzuhören, um Inhalt, Betonungen und Nuancen in der Sprache zu erkennen. Oftmals sind Dolmetscher erst nach mehrfachem Abhören in der Lage, den wirklichen Aussagegehalt einer Äußerung zu bestimmen und damit überhaupt erst festzustellen, ob Anhaltspunkte für eine Kernbereichsrelevanz gegeben sind. In solchen Zweifelsfällen werden die Grundrechte der Betroffenen dadurch weiter geschützt, dass ein Richter die Auswertung der automatischen Aufzeichnung übernimmt. Satz 7 regelt, dass die unterbrochenen Maßnahmen nur fortgeführt werden dürfen, wenn durch sie zwischenzeitlich keine Erkenntnisse aus dem Kernbereich privater Lebensgestaltung mehr erhoben werden. Da es nicht ausgeschlossen werden kann, dass Daten erfasst werden, die den Kernbereich privater Lebensgestaltung betreffen, werden die Regelungen durch das in den Sätzen 8 bis 10 enthaltene Verwertungsverbot und Löschungsgebot flankiert. Die Sätze 11 bis 13 dienen der Umsetzung des Urteils des Bundesverfassungsgerichts vom 20. April 2016 zur Aufbewahrungsfrist der Löschungsprotokolle zwecks effektiver Ausübung der Betroffenenrechte und einer wirksamen Kontrolle durch den Landesbeauftragten für den Datenschutz und Informationssicherheit.

Zu Absatz 9

Absatz 9 entspricht § 22 Absatz 7 des bisherigen PolG. Im Übrigen gelten für die weitere Verarbeitung der nach Absatz 1 erhobenen Daten die allgemeinen Vorschriften, insbesondere § 15.

29. Zu § 50 (Besondere Bestimmungen über den Einsatz technischer Mittel zur Datenerhebung in oder aus Wohnungen)

Mit der Regelung wird § 23 des bisherigen PolG an die Vorgaben der Entscheidung des Bundesverfassungsgerichts vom 20. April 2016 angepasst. Die in diesem Zusammenhang maßgeblichen Regelungen zur Benachrichtigung der betroffenen Personen, zur Protokollierung der erhobenen Daten, zur Kennzeichnung der Daten, zur Kontrolle der Datenerhebungen durch die Aufsichtsbehörde für den Datenschutz sowie zur Unterrichtung des Landtages finden sich in den §§ 72, 74, 86, 90 und 98 Absatz 1 Nummer 14. Für die weitere Verarbeitung der so erhobenen Daten gelten die allgemeinen Vorschriften, insbesondere § 15.

Zu Absatz 1
In Absatz 1 werden die bislang in § 23 Absatz 1 geregelten Eingriffsvoraussetzungen für den Einsatz technischer Mittel zur Datenerhebung in oder aus Wohnungen unter Berücksichtigung der Entscheidung des Bundesverfassungsgerichts vom 20. April 2016 geringfügig angepasst.

Nach Absatz 1 kann der Polizeivollzugsdienst personenbezogene Daten in oder aus Wohnungen durch den verdeckten Einsatz technischer Mittel nach § 49 Absatz 2 Nummer 2 zur Abwehr einer dringenden Gefahr (vgl. Art 13 Absatz 4 GG) für besonders hochrangige Rechtsgüter erheben, vorliegend Leib, Leben oder Freiheit einer Person, den Bestand oder die Sicherheit des Bundes oder eines Landes. Als Adressaten einer entsprechenden Maßnahme kommen wie bislang Störer nach den §§ 6 oder 7 sowie, unter den dort genannten Voraussetzungen, Nichtstörer im Sinne des § 9 in Betracht.

Eine Maßnahme nach Absatz 1 ist wie bisher nur zulässig, wenn die Abwehr der Gefahr oder die Verhütung der Straftat auf andere Weise gefährdet oder erheblich erschwert wäre.

Satz 2 stellt klar, dass Maßnahmen nach Satz 1 wie bisher auch dann durchgeführt werden dürfen, wenn unbeteiligte Dritte betroffen sind (vgl. § 23 Absatz 1 Satz 2 PolG a.F.).

Zu Absatz 2

Absatz 2 dient wie bisher der verfahrensmäßigen Absicherung und unterwirft Maßnahmen nach Absatz 1 auch weiterhin einem Richtervorbehalt. Das Bundesverfassungsgericht hat die Erforderlichkeit eines solchen Richtervorbehalts für Maßnahmen der Wohnraumüberwachung in seiner Entscheidung vom 20. April 2016 noch einmal betont (Rn. 117 und 194). Abweichend von § 132 Absatz 1 ist die in § 74a Absatz 4 des Gerichtsverfassungsgesetzes genannte Kammer des Landgerichts zuständig, in deren Zuständigkeitsbereich die zuständige Polizeidienststelle ihren Sitz hat. Dabei wird im Hinblick auf die bisherige Rechtslage präzisiert, dass es für die Bestimmung der örtlichen Zuständigkeit des Gerichts nicht auf den Gerichtsbezirk des Landgerichts ankommt, sondern auf den Zuständigkeitsbereich der Kammer nach § 74a Absatz 4 des Gerichtsverfassungsgesetzes. Dieser umfasst den gesamten Bezirk des Oberlandesgerichtes, das seinen Sitz im Bezirk des Landgerichtes hat. Der Antrag auf richterliche Entscheidung ist durch die Leitung eines regionalen Polizeipräsidiums, des Polizeipräsidiums Einsatz oder des Landeskriminalamts schriftlich zu stellen und zu begründen. Eine Delegation der Antragsbefugnis ist nicht möglich.

Zu Absatz 3

Absatz 3 setzt die Anforderungen des Bundesverfassungsgerichts (vgl. Rn. 118) an den zu stellenden Antrag um.

Zu Absatz 4

Absatz 4 Satz 1 sieht vor, dass eine entsprechende Anordnung schriftlich zu ergehen hat. Sie muss die Angabe der Person enthalten, gegen die sich die Maßnahme richtet, soweit möglich mit Name und Anschrift. Daneben müssen die zu überwachende Wohnung oder die zu überwachenden Wohnräume, Art, Umfang und Dauer der Maßnahme sowie die wesentlichen Gründe angegeben werden. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als ei-

nen Monat ist zulässig, solange die Voraussetzungen für die Maßnahme fortbestehen. Für das gerichtliche Verfahren gelten die Vorschriften über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (vgl. § 132 Absatz 2).

Zu Absatz 5
Bei Gefahr im Verzug kann eine Anordnung nach Absatz 1 auch durch die Leitung eines regionalen Polizeipräsidiums, des Polizeipräsidiums Einsatz oder des Landeskriminalamts selbst getroffen werden. Eine Delegation der Anordnungsbefugnis ist aus Gründen der Verhältnismäßigkeit nicht mehr möglich. Die als Eilfall getroffene Anordnung bedarf der unverzüglichen Bestätigung durch das in Absatz 2 genannte Gericht. Sie tritt außer Kraft, soweit die gerichtliche Bestätigung nicht binnen drei Tagen erfolgt.

Satz 4 entspricht § 23 Absatz 4 Satz 1 des bisherigen PolG. Auch in diesem Fall ist die Anordnung von einer der in Satz 1 genannten Personen zu treffen.

Zu Absatz 6
Absatz 6 ergänzt die bisher in § 23 Absätze 2 und 5 PolG a.F. enthaltenen Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung unter Berücksichtigung der Vorgaben des Bundesverfassungsgerichts aus seinem Urteil vom 20. April 2016 (Rn. 119 ff., 196 ff.).

Die Sätze 1 und 2 entsprechen § 23 Absatz 2 des bisherigen PolG.

Satz 3 enthält das Gebot der unverzüglichen Unterbrechung einer Maßnahme nach Absatz 1 und regelt, was zu unternehmen ist, wenn sich während der Überwachung unerwartet tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte aus dem Kernbereich der persönlichen Lebensgestaltung erfasst werden. Bestehen diesbezüglich Zweifel, darf nach Satz 4 nur noch eine automatische Aufzeichnung fortgesetzt werden. Die Regelung dient dem Schutz des Kernbereichs, indem sie bestimmt, dass auch in solchen Fällen, in denen keine eindeutigen Anhaltspunkte für eine Kernbereichsrelevanz sprechen, eine unmittelbare Überwachung durch die ausführenden

Stellen ausgeschlossen ist. Nach Satz 5 darf die Maßnahme nur unter den Voraussetzungen der Sätze 1 und 2 uneingeschränkt fortgesetzt werden.

Nach Satz 6 sind sämtliche Erkenntnisse, die durch Maßnahmen nach Absatz 1 erlangt worden sind, unverzüglich dem anordnenden Gericht vorzulegen, welches nach Satz 7 unverzüglich die Feststellung zu treffen hat, ob eine Kernbereichsrelevanz vorliegt oder nicht und damit eine Entscheidung über die Löschung oder Verwertbarkeit der Daten trifft.

Da es nicht ausgeschlossen werden kann, dass Daten erfasst werden, die den Kernbereich privater Lebensgestaltung betreffen, werden die Regelungen durch das in den Sätzen 8 bis 10 enthaltene Verwertungsverbot und Löschungsgebot flankiert. Die Sätze 11 bis 13 dienen der Umsetzung des Urteils des Bundesverfassungsgerichts vom 20. April 2016 zur Aufbewahrungsfrist der Löschungsprotokolle zwecks effektiver Ausübung der Betroffenenrechte und einer wirksamen Kontrolle durch den Landesbeauftragten für den Datenschutz und Informationssicherheit.

30. Zu § 51 (Einsatz automatischer Kennzeichenlesesysteme)

Mit der Regelung wird § 22a des bisherigen PolG vor allem an die Vorgaben des Bundesverfassungsgerichts vom 18. Dezember 2018 (1 BvR 2795/09, 1 BvR 3187/10, 1 BvR 142/15) angepasst. Darüber hinaus werden unter Berücksichtigung der Vorgaben des Bundesverfassungsgerichts vom 20. April 2016 auch für den Einsatz automatischer Kennzeichenlesesysteme Regelungen zur Benachrichtigung der betroffenen Personen im Trefferfall, zur Protokollierung der erhobenen Daten sowie zur Kennzeichnung der Daten in das Polizeigesetz aufgenommen, die in den §§ 72, 74 und 86 enthalten sind. Im Übrigen werden die Verweise aufgrund der neuen Nummerierung des Gesetzes sowie des Einfügens von Satz 2 sowie einer neuen Nummer 2 in § 27 Absatz 1 angepasst.

Zu Absatz 1
In Satz 1 wird die Bezugnahme auf den jetzt maßgeblichen § 27 Absatz 1 etwas deutlicher gefasst. Damit wird klargestellt, dass eine Kennzeichenerfassung als Grundlage für eine Kennzeichenkontrolle „unter den Voraussetzungen“ erlaubt ist, für

die auch eine Identitätsfeststellung nach § 27 Absatz 1 zulässig ist. Die dort genannten Tatbestände haben alle – inklusive der neu gefassten Nummern 5 und 6 – präventive Zweckrichtungen, die im Einzelnen auch für den Einsatz von AKLS maßgeblich sind. Auf die bisher in § 22a Absatz 1 Satz 1 PolG a.F. enthaltene allgemeine Zielsetzung „zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten“ kann daher verzichtet werden.

Mit dem neu eingefügten Satz 2 werden die Vorgaben des BVerfG an den Grundsatz der Verhältnismäßigkeit erfüllt und die Voraussetzungen für eine Kennzeichenerfassung unter Bezugnahme auf die beiden beanstandeten Tatbestandsvarianten in § 27 Absatz 1 Nummern 1 und 7b hinreichend begrenzt. Nach § 51 Absatz 1 Sätze 1 und 2 i.V.m. § 27 Absatz 1 Nummer 1 ist der Einsatz von AKLS künftig zur Abwehr einer Gefahr für Leib, Leben, Freiheit, sexuelle Selbstbestimmung, den Bestand oder die Sicherheit des Bundes oder eines Landes oder bedeutende fremde Sachen oder Vermögenswerte zulässig und damit auf den Schutz von Rechtsgütern von zumindest erheblichem Gewicht beschränkt. Der im Hinblick auf § 51 Absatz 1 Sätze 1 und 2 i.V.m. § 27 Absatz 1 Nummer 7b vom BVerfG geforderte hinreichend bestimmte Grenzbezug wird durch die Beschränkung auf Bundesautobahnen, Europa- und Bundesstraßen umgesetzt. Bundesautobahnen und Europastraßen wurden vom BVerfG in seiner Entscheidung ausdrücklich für zulässig erklärt (BVerfG, 1 BvR 2795/09, Rn. 75). Darüber hinaus dienen neben den Bundesautobahnen auch Bundesstraßen – gemeinsam als Bundesfernstraßen - dem weiträumigen Verkehr (vgl. § 1 FStrG). Daher ist auch für Bundesstraßen in einer den Bestimmtheitsanforderungen genügenden Weise ein konsequenter Grenzbezug sichergestellt.

In dieser Ausgestaltung sind die Voraussetzungen für die Durchführung von Kennzeichenkontrollen, wie sie sich aus dem Verweis auf die jeweilige Regelung zur Identitätskontrolle ergeben, verfassungsrechtlich weder hinsichtlich der Anforderungen an einen hinreichend bestimmten Anlass noch hinsichtlich der Anforderungen an einen hinreichend gewichtigen Rechtsgüterschutz zu beanstanden (vgl. BVerfG, 1 BvR 2795/09, Rn 78). Dies gilt auch in Bezug auf den neu eingefügten § 27 Absatz 1 Nummer 2.

Aufgrund der Neufassung von § 27 Absatz 1 Nummern 5 und 6 ist die bisherige Regelung des § 22a Absatz 1 Satz 3 Nummer 3 entbehrlich und wird daher gestrichen.

Zu Absatz 2
Absatz 2 entspricht der bisherigen Regelung des § 22a Absatz 2 PolG. In diesem Zusammenhang wird darauf hingewiesen, dass die Regelung nach den Vorgaben des BVerfG verfassungskonform auszulegen ist mit der Maßgabe, dass die in den Datenabgleich des AKLS einzubeziehenden Fahndungsbestände zu selektieren und auf den jeweiligen Zweck der Kennzeichenkontrolle zu beschränken sind.

Zu Absatz 3
Absatz 3 entspricht bis auf eine redaktionelle Änderung der bisherigen Regelung des § 22a Absatz 3. Es wird darauf hingewiesen, dass Absatz 3 Satz 2 eine andere Regelung im Sinne des § 74 Absatz 1 Satz 1 darstellt.

Zu Absatz 4
In Absatz 4 wird Satz 4 der bisherigen Regelung des § 22a Absatz 4 PolG gestrichen. Das BVerfG hat diese Regelung für mit der Verfassung unvereinbar erklärt, weil die darin geregelte zweckändernde weitere Verarbeitung der Daten im Zusammenhang mit dem Einsatz von AKLS nicht auf den Schutz von Rechtsgütern von erheblichem Gewicht oder einem vergleichbar gewichtigen öffentlichen Interesse begrenzt wird. Durch die Streichung der Regelung gelten die allgemeinen Vorschriften, insbesondere der Grundsatz der hypothetischen Datenneuerhebung nach § 15 Absatz 3, mit dem die Vorgaben des BVerfG erfüllt werden.

31. Zu § 52 (Bestandsdatenauskunft)
Die Regelung entspricht § 23 a Absatz 9 Sätze 1 bis 4 i.V.m. Absatz 1 Satz 4 sowie Absatz 5 Sätze 1, 3 und 4 des bisherigen PolG. Die in diesem Zusammenhang unter Berücksichtigung der Vorgaben des Bundesverfassungsgerichts vom 20. April 2016 maßgeblichen Regelungen zur Benachrichtigung der betroffenen Personen (vgl. § 23 a Absatz 9 Sätze 5 bis 7 PolG a.F.), zur Protokollierung der erhobenen Daten sowie zur Kennzeichnung der Daten finden sich in den §§ 72, 74 und 86. Für die wei-

tere Verarbeitung der so erhobenen Daten gelten die allgemeinen Vorschriften, insbesondere § 15. Weitere Änderungen werden infolge der Entscheidung des Bundesverfassungsgerichts vom 20. April 2016 nicht für erforderlich erachtet.

32. Zu § 53 (Erhebung von Telekommunikationsverkehrsdaten und Nutzungsdaten)
Mit der Regelung wird § 23 a Absätze 1 bis 5 und 8 des bisherigen PolG an die Vorgaben der Entscheidung des Bundesverfassungsgerichts vom 20. April 2016 angepasst. Die in diesem Zusammenhang maßgeblichen Regelungen zur Benachrichtigung der betroffenen Personen, zur Protokollierung der erhobenen Daten, zur Kennzeichnung der Daten, zur Kontrolle der Datenerhebungen durch die Aufsichtsbehörde für den Datenschutz sowie zur Unterrichtung des Landtages finden sich in den §§ 72, 74, 86, 90 und 98 Absatz 1 Nummer 14. Für die weitere Verarbeitung der so erhobenen Daten gelten die allgemeinen Vorschriften, insbesondere § 15.

Zu Absatz 1
In Absatz 1 Satz 1 werden die bislang in § 23 a Absatz 1 geregelten Eingriffsvoraussetzungen für die Erhebung von Telekommunikationsverkehrsdaten und Nutzungsdaten unter Berücksichtigung der Entscheidung des Bundesverfassungsgerichts vom 20. April 2016 neu gefasst.

Satz 1 Nummer 1 ersetzt § 23 a Absatz 1 Satz 1 des bisherigen PolG. Danach darf der Polizeivollzugsdienst Telekommunikationsverkehrsdaten und Nutzungsdaten zur Abwehr von Gefahren für hochrangige Rechtsgüter erheben, vorliegend Leib, Leben oder Freiheit einer Person, den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist. Die geringfügige Erweiterung der bisherigen Regelung um „Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist“, steht im Einklang mit den Vorgaben des Bundesverfassungsgerichts (Rn. 231, 247). Als Adressaten einer entsprechenden Maßnahme kommen wie bisher sowohl Störer nach den §§ 6 oder 7, aber auch Nichtstörer unter den Voraussetzungen des § 9 in Betracht.

Der neue Satz 1 Nummern 2 und 3 ersetzt § 23 a Absatz 1 Satz 2 des bisherigen PolG und erlaubt entsprechende Maßnahmen auch gegenüber Personen, bei denen

bestimmte Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat begehen werden, die sich gegen die in Nummer 1 genannten Rechtsgüter richtet oder deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines überschaubaren Zeitraums eine Straftat begehen werden, die sich gegen die in Nummer 1 genannten Rechtsgüter richtet. Einschränkend sind in beiden Fällen jedoch nur terroristisch motivierte Straftaten einschlägig, also Straftaten, die dazu bestimmt sind, die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen, und dabei durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen können. Die Regelung entspricht den Vorgaben des Bundesverfassungsgerichts aus seiner Entscheidung vom 20. April 2016 und den darin aufgestellten Anforderungen an die zu treffende Prognoseentscheidung bezüglich der Gefahrenlage im Vorfeld einer konkreten Gefahr für die Begehung terroristischer Straftaten (vgl. Rn. 112 und 251). Das Bundesverfassungsgericht hat es in diesem Zusammenhang ausdrücklich offen gelassen, wo diesbezüglich die verfassungsrechtlichen Grenzen im Allgemeinen, etwa auch für entsprechende Befugnisse nach den Landespolizeigesetzen liegen (vgl. Rn. 156).

Mit dem neuen Satz 1 Nummer 4 wird geregelt, dass sich die Maßnahmen auch gegen sog. Nachrichtenmittler richten können. Satz 1 Nummer 5 weitet die Eingriffsgrundlage auf Dritte aus, bei denen aufgrund bestimmter Tatsachen die Annahme besteht, dass eine Person nach Nummer 1 den Telekommunikationsanschluss oder das Endgerät des Dritten benutzen wird.

Um die Verhältnismäßigkeit einer Maßnahme nach Absatz 1 zu gewährleisten, wird wie bisher in allen Fällen vorausgesetzt, dass sonst die Erfüllung der polizeilichen Aufgabe gefährdet oder wesentlich erschwert würde. Die Maßnahmen dürfen auch dann durchgeführt werden, wenn unbeteiligte Dritte betroffen sind (vgl. § 23 a Absatz 1 Satz 4 PolG a.F.).

Zu Absatz 2

Absatz 2 dient wie bisher der verfahrensmäßigen Absicherung und unterwirft Maßnahmen nach Absatz 1 auch weiterhin einem Richtervorbehalt. Für die Zuständigkeit des Gerichts gilt § 132 Absatz 1. Der Antrag auf richterliche Entscheidung ist durch die Leitung eines regionalen Polizeipräsidiums oder des Landeskriminalamts schriftlich zu stellen und zu begründen. Eine Delegation der Antragsbefugnis auf besonders beauftragte Beamte des höheren Dienstes ist weiterhin möglich.

Zu Absatz 3

Absatz 3 setzt die Anforderungen des Bundesverfassungsgerichts an den zu stellenden Antrag um (vgl. Rn. 118).

Zu Absatz 4

Absatz 4 Satz 1 sieht vor, dass eine entsprechende Anordnung wie bisher schriftlich zu ergehen hat. Sie muss die Angabe der Person enthalten, gegen die sich die Maßnahme richtet, soweit möglich mit Name und Anschrift. Daneben muss die Rufnummer oder eine Kennung des Telekommunikationsanschlusses oder des Endgerätes, bei dem die Datenerhebung über eine in Absatz 1 genannte Person durchgeführt wird oder eine Bezeichnung des Nutzers der Telemedien, dessen Daten erhoben werden, angegeben werden (vgl. § 23 a Absatz 2 Satz 5 PolG a.F.). Abweichend davon genügt eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation oder Telemediennutzung, sofern andernfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre (vgl. § 23 a Absatz 2 Satz 6 PolG a.F.). Auch sind Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie die wesentlichen Gründe schriftlich niederzulegen.

Entsprechend der bisherigen Regelung ist die Anordnung auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, solange die Voraussetzungen für die Maßnahme fortbestehen. Für das gerichtliche Verfahren gelten die Vorschriften über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (vgl. § 132 Absatz 2).

Zu Absatz 5

Bei Gefahr im Verzug kann eine Anordnung nach Absatz 1 wie bisher (§ 23 a Absatz 2 Satz 7 i.V.m. § 23 Absatz 3 Satz 8 PolG a.F.) durch die Leitung eines regionalen Polizeipräsidiums oder des Landeskriminalamts selbst getroffen werden. Eine Delegation der Anordnungsbefugnis auf besonders beauftragte Beamte des höheren Dienstes ist weiterhin möglich. Die als Eilfall getroffene Anordnung bedarf der unverzüglichen Bestätigung durch das Gericht.

Zu Absatz 6
Absatz 6 entspricht § 23 a Absatz 5 des bisherigen PolG.

Zu Absatz 7
Absatz 7 entspricht weitgehend § 23 a Absatz 3 des bisherigen PolG. Allerdings wird die bisher in Satz 2 enthaltene Einschränkung, wonach die Anordnungsbefugnis nur auf besonders beauftragte Beamte des höheren Dienstes übertragen werden kann, gestrichen. Künftig ist eine Delegation der Anordnungsbefugnis auch auf die Polizeiführer vom Dienst in den Führungs- und Lagezentren der Polizeipräsidien möglich. Diese gehören in der Regel dem gehobenen Polizeivollzugsdienst an. Die Polizeiführer vom Dienst sind jedoch aufgrund ihrer besonderen Funktion bestens geeignet, entsprechende Sachverhalte insbesondere auch zur Nachtzeit rasch und zielgerichtet zu bewerten. Zudem sind solche Maßnahmen nur mit einem geringfügigen Grundrechtseingriff verbunden, da die Ortung regelmäßig zugunsten der vermissten, suizidgefährdeten oder hilflosen Person erfolgt. Daher ist die geringfügige Erweiterung des anordnungsbefugten Personenkreises sachlich gerechtfertigt. § 4 DVO PolG wird entsprechend angepasst.

Zu Absatz 8
Absatz 8 entspricht § 23 a Absatz 4 des bisherigen PolG.

33. Zu § 54 (Überwachung der Telekommunikation)
Die Regelung entspricht inhaltlich § 23 b Absätze 1 bis 9 des bisherigen PolG. Die bisher in § 23 b Absätze 10 bis 14 PolG a.F. enthaltenen Regelungen zur Benachrichtigung der betroffenen Personen, zur Protokollierung der erhobenen Daten, zur Kennzeichnung der Daten, zur Kontrolle der Datenerhebungen durch die Aufsichts-

behörde für den Datenschutz sowie zur Unterrichtung des Landtages werden aus redaktionellen Gründen „vor die Klammer gezogen“ (§§ 72, 74, 86, 90 und 98 Absatz 1 Nummer 14), da entsprechende Regelungen auch für andere verdeckte Eingriffsmaßnahmen Anwendung finden. Für die weitere Verarbeitung der nach dieser Vorschrift erhobenen Daten gelten nunmehr die allgemeinen Vorschriften, insbesondere § 15. Die Übergangsbestimmungen des § 85 PolG a.F. werden aufgehoben.

Hinsichtlich der in Absatz 4 Satz 4 vorgesehenen Konzentration der gerichtlichen Zuständigkeiten bei den Amtsgerichten Mannheim und Stuttgart wird auf die Ausführungen zu § 31 Absatz 3 Bezug genommen.

34. Zu § 55 (Weitere Bestimmungen über polizeiliche Maßnahmen mit Bezug zur Telekommunikation)
Mit der Regelung wird § 23 a Absätze 6 und 8 des bisherigen PolG an die Vorgaben der Entscheidung des Bundesverfassungsgerichts vom 20. April 2016 angepasst.
Die in Zusammenhang mit Absatz 1 maßgeblichen Regelungen zur Benachrichtigung der betroffenen Personen, zur Protokollierung der erhobenen Daten sowie zur Kennzeichnung der Daten finden sich in den §§ 72, 74 und 86. Für die weitere Verarbeitung der so erhobenen Daten gelten die allgemeinen Vorschriften, insbesondere § 15. Darüber hinaus wird § 23 a Absatz 7 PolG a. F in die neue Regelung übernommen.

Zu Absatz 1
In Absatz 1 werden die bislang in § 23 a Absatz 6 PolG a.F. geregelten Eingriffsvoraussetzungen für den Einsatz technischer Mittel zur Standortermittlung eines Mobilfunkgerätes oder der Kennung eines Telekommunikationsanschlusses oder eines Endgerätes unter Berücksichtigung der Entscheidung des Bundesverfassungsgerichts vom 20. April 2016 neu gefasst.

Danach kann der Polizeivollzugsdienst unter den Voraussetzungen des neuen § 53 Absatz 1 technische Mittel einsetzen, um den Standort eines Mobilfunkgerätes oder die Kennung eines Telekommunikationsanschlusses oder eines Endgerätes zu ermitteln. Satz 2 entspricht der Regelung des § 23 a Absatz 6 Satz 2 PolG a.F. Satz 3 ver-

weist hinsichtlich des nunmehr erforderlichen Richtervorbehalts und der Anordnungsbefugnis bei Gefahr im Verzug auf § 53 Absätze 2 und 5. Eine Anordnung im Sinne des Absatzes 1 ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, solange die Voraussetzungen für die Maßnahme fortbestehen. Die aufgrund der Anordnung ergriffenen Maßnahmen sind unverzüglich zu beenden, soweit die Voraussetzungen der Anordnung nicht mehr vorliegen. Für die gerichtlichen Zuständigkeiten und das Verfahren gilt § 132.

Zu Absatz 2
Absatz 2 entspricht weitestgehend der bisherigen Regelung des § 23 a Absatz 7 PolG a.F. Danach kann der Polizeivollzugsdienst unter den Voraussetzungen des neuen § 53 Absatz 1 bei Vorliegen einer unmittelbaren Gefahr technische Mittel einsetzen, um Telekommunikationsverbindungen der dort genannten Personen zu unterbrechen oder zu verhindern. Wie bisher ist die Anordnung einer entsprechenden Maßnahme durch die Leitung eines regionalen Polizeipräsidiums oder des Landeskriminalamts zu treffen. Eine Delegation der Anordnungsbefugnis auf besonders beauftragte Beamte des höheren Dienstes ist weiterhin möglich.

35. Zu § 56 (Ausschreibung von Personen und Kraftfahrzeugen)
Die Regelung entspricht § 25 Absätze 1 bis 3 des bisherigen PolG. Unter Berücksichtigung der Vorgaben der Entscheidung des Bundesverfassungsgerichts vom 20. April 2016 finden sich die maßgeblichen Regelungen zur Benachrichtigung der betroffenen Personen, zur Protokollierung der erhobenen Daten sowie zur Kennzeichnung der Daten in den §§ 72, 74 und 86. § 25 Absatz 4 PolG a.F., der die bisherige Regelung über die Benachrichtigung betroffener Personen enthielt, entfällt. Im Übrigen werden die Verweise aufgrund der neuen Nummerierung des Gesetzes angepasst.

36. Zu § 57 (Weitere Verarbeitung zu Zwecken der wissenschaftlichen Forschung)
Es ist grundsätzlich zu unterscheiden zwischen wissenschaftlicher Forschung, die polizeilichen Zwecken dient und somit zu Zwecken der Richtlinie (EU) 2016/680 betrieben wird, und wissenschaftlicher Forschung, die sonstigen, nicht polizeilichen Zwecken dient und somit in den Anwendungsbereich der Verordnung (EU) 2016/679 fällt. Die Vorschrift regelt die weitere Verarbeitung von Daten zu Zwecken der Richtlinie (EU) 2016/680 durch die Polizei selbst oder andere durch die Polizei beauftragte

Stellen. Für die weitere Verarbeitung oder Übermittlung von Daten zu Zwecken der wissenschaftlichen Forschung, die nicht polizeilichen Zwecken dient und damit nicht dem Anwendungsbereich der Richtlinie (EU) 2016/680 unterfällt, gilt § 11 Absatz 2.

Nach Artikel 4 Absatz 3 der Richtlinie (EU) 2016/680 kann die Verarbeitung durch denselben oder einen anderen Verantwortlichen die wissenschaftliche Verwendung für Zwecke der Richtlinie (EU) 2016/680 umfassen, sofern geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorhanden sind. Hierzu zählen insbesondere eine so zeitnah wie möglich durchzuführende Anonymisierung der Daten und geeignete technische und organisatorische Maßnahmen, um die Daten gegen unbefugte Kenntnisnahme zu schützen.

Zu Absatz 1

Absatz 1 Satz 1 erteilt der Polizei die Befugnis zur selbständigen weiteren Verarbeitung vorhandener Daten zu wissenschaftlichen Forschungszwecken. So betreibt zum Beispiel das Landeskriminalamt praxisbezogene Forschung in besonderen Bereichen der polizeilichen Kriminalitätsbekämpfung und der Kriminal- und Verkehrsunfallprävention oder das Polizeipräsidium Einsatz führt praxisbezogene Forschung zur polizeilichen Einsatzbewältigung durch. Absatz 1 Satz 2 stellt klar, dass eine solche weitere Verarbeitung personenbezogener Daten, die aus besonders eingriffsintensiven Maßnahmen erlangt wurden, nicht zulässig ist. Damit trägt die Regelung dem Grundsatz der hypothetischen Datenneuerhebung Rechnung.

Zu Absatz 2

Absatz 2 enthält eine spezielle Übermittlungsvorschrift, durch die die Polizei ermächtigt wird, personenbezogene Daten an öffentliche und nichtöffentliche Stellen außerhalb der Polizei zu übermitteln, wenn diese zur Durchführung einer wissenschaftlichen Forschungsarbeit beauftragt werden, die polizeilichen Zwecken dient.

Zu Absatz 3 bis Absatz 7

Die Absätze 3 bis 7 legen gemäß den Anforderungen des Artikels 4 Absatz 3 der Richtlinie (EU) 2016/680 geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen fest. Absatz 7 ist in diesem Zusammenhang notwendig, weil Per-

sonen oder Stellen außerhalb der Polizei, an die personenbezogene Daten zu Forschungszwecken übermittelt werden, nicht direkt durch dieses Gesetz verpflichtet werden können, so dass die Polizei die Einhaltung der einschlägigen Bestimmungen mit diesen Personen oder Stellen vertraglich oder auf sonstige geeignete Weise zu vereinbaren hat.

37. Zu § 58 (Weitere Verarbeitung zu Zwecken der Aus- und Fortbildung, zu statistischen Zwecken und zur Vorgangsverwaltung)
Nach Artikel 4 Absatz 3 der Richtlinie (EU) 2016/680 kann die Verarbeitung personenbezogener Daten durch den Verantwortlichen auch die Archivierung im öffentlichen Interesse sowie neben der wissenschaftlichen oder historischen auch die statistische Verwendung für richtlinienkonforme Zwecke umfassen, sofern geeignete Vorkehrungen zum Schutz der Rechtsgüter der betroffenen Person getroffen werden. Dazu gehört insbesondere eine frühestmögliche Anonymisierung der Daten. Es handelt sich mithin um eine erlaubte Zweckänderung. Die in § 15 Absatz 3 LDSG a.F. enthaltene Regelung, nach der es sich bei diesen Nutzungen nicht um eine Zweckänderung handelte, kann mit dem engen Zweckbindungsbegriff der Richtlinie (EU) 2016/680 nicht aufrecht erhalten werden.

Die sowohl in Absatz 1 als auch in Absatz 2 enthaltene Einschränkung, dass die Aus- oder Fortbildung, die Statistik beziehungsweise die Vorgangsverwaltung polizeilichen Zwecken dienen muss, ist erforderlich, um im Anwendungsbereich der Richtlinie (EU) 2016/680 zu bleiben. Für Aus- und Fortbildungszwecke, Statistiken sowie die Vorgangsverwaltung für nicht-polizeiliche Zwecke sollten polizeiliche Daten ausschließlich anonymisiert verwendet werden.

Zu Absatz 1
Absatz 1 Satz 1 sieht vor, dass vorhandene Daten zur polizeilichen Aus- und Fortbildung sowie zur Erstellung polizeilicher Statistiken weiter verarbeitet werden dürfen, bestimmt aber gleichzeitig, dass eine frühestmögliche Anonymisierung der personenbezogenen Daten erforderlich ist und dass berechtigte Geheimhaltungsinteressen der betroffenen Person nicht offensichtlich überwiegen dürfen. Absatz 1 Satz 2 stellt klar, dass personenbezogene Daten, die aus besonders eingriffsintensiven Maßnahmen erlangt wurden, nicht zu Zwecken der Aus- und Fortbildung oder zu statistischen

Zwecken weiter verarbeitet werden dürfen. Dieses Verbot steht der Pflicht zur Berichterstattung an den Landtag, die gerade für solche Maßnahmen gilt und zu deren Erfüllung statistische Erhebungen durchgeführt werden müssen, nicht entgegen. Denn um der Berichtspflicht nachzukommen, genügt regelmäßig die Verarbeitung anonymisierter Daten.

Zu Absatz 2
Absatz 2 eröffnet die Möglichkeit der weiteren Verarbeitung von Daten zu Zwecken der Vorgangsverwaltung.

38. Zu § 59 (Datenübermittlung im nationalen Bereich)
Die Vorschrift setzt die Vorgaben des Bundesverfassungsgerichts um, das in seinem Urteil vom 20. April 2016 (Rn. 276) ausführt, dass auch die Anforderungen an die Übermittlung staatlich erhobener Daten dem Grundsatz der hypothetischen Datenneuerhebung unterliegen. Die Ausgestaltung der Vorschrift orientiert sich an § 42 PolG a.F. aber auch an § 25 BKAG, um die Voraussetzungen zur Datenübermittlung im nationalen Bereich vor dem Hintergrund der Teilnahme am Informationsverbund mit jenen des Bundeskriminalamts zu harmonisieren.

Zu Absatz 1
Absatz 1 übernimmt § 42 Absatz 1 PolG a.F.. Der zusätzliche Bezug auf die Vorschrift zur Zweckbindung und zweckändernden Verarbeitung von Daten hat rein deklaratorischen Charakter und soll verdeutlichen, dass sich die Zulässigkeit einer Datenübermittlung innerhalb der Polizei, also zwischen Polizeibehörden sowie Dienststellen und Einrichtungen des Polizeivollzugsdienstes, ebenfalls am Grundsatz der hypothetischen Datenneuerhebung zu messen hat.

Zu Absatz 2
Unter Aufstellung paralleler Voraussetzungen zu Absatz 1 setzt Absatz 2 den vom Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 aufgestellten Grundsatz der hypothetischen Datenneuerhebung für Datenübermittlungen an andere Polizeien sowohl des Bundes als auch anderer Bundesländer um.

Zu Absatz 3

Absatz 3 setzt den Grundsatz der hypothetischen Datenneuerhebung für Übermittlungen an öffentliche Stellen um, die keine originären polizeilichen Aufgaben wahrnehmen. Die bisherige Unterscheidung im Polizeigesetz zwischen der Übermittlung an andere öffentliche Stellen, die für die Gefahrenabwehr zuständig sind (§ 42 Absatz 2 PolG a.F.) und an solche andere öffentliche Stellen, die nicht für die Gefahrenabwehr zuständig sind (§ 42 Absatz 7 PolG a.F.), entfällt damit. Mit der neuen Regelung wird nur noch zwischen Polizeien und anderen öffentlichen Stellen unterschieden. Eine solche übergreifende Zusammenfassung der „sonstigen öffentlichen Stellen“ hat das Bundesverfassungsgericht als mit dem Bestimmtheitsgebot vereinbar angesehen. Welche Stellen hierunter zu verstehen sind, richte sich nach den jeweiligen Übermittlungszwecken, die die verschiedenen Übermittlungsbefugnisse näher regeln (vgl. Rn 306). In seinem Urteil führt das Bundesverfassungsgericht (vgl. Rn. 287) ferner 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. Maßgeblich für die Beurteilung der Zulässigkeit der Datenübermittlung ist damit nicht der Empfänger, sondern, im Einklang mit dem Grundsatz der Zweckbindung und Zweckänderung, der Zweck, zu dem die Daten übermittelt werden sollen.

In Bezug auf die Datenübermittlung an das Landesamt für Verfassungsschutz ist es nach Auffassung des Bundesverfassungsgerichts notwendig, dass in Anwendung des Grundsatzes der hypothetischen Datenneuerhebung neben konkreten Ermittlungsansätzen für die Aufdeckung von Straftaten oder Gefahren für hochrangige Rechtsgüter zugleich konkrete Erkenntnisse zu einer Gefährdung hochrangiger Rechtsgüter erkennbar sind, die für die Lagebeurteilung nach Maßgabe der Aufgaben des Verfassungsschutzes bedeutsam sind (Rn. 320). Die bisherige Regelung des § 42 Absatz 8 PolG a.F., wonach sich die Übermittlung personenbezogener Daten an das Landesamt für Verfassungsschutz nach dem Landesverfassungsschutzgesetz richtete, geht hier in Nummer 1 auf.

Nummer 2b) umfasst bei Vorliegen der entsprechenden Voraussetzungen auch die Befugnis zur Übermittlung des Ergebnisses eines seitens des Polizeivollzugsdienstes durchgeführten Datenabgleichs an Gerichtsvollzieherinnen oder Gerichtsvollzieher

zur Abschätzung einer konkreten Gefährdungssituation bei einer beabsichtigten Vollstreckungsmaßnahme (vgl. neue Regelung in § 13a AGGVG – Artikel II dieses Gesetzes).

Zu Absatz 4

Absatz 4 gleicht die Voraussetzungen zur Übermittlung an nichtöffentliche Stellen zwar an diejenigen zur Übermittlung an öffentliche Stellen an, erhöht gegenüber Absatz 3 aber die Anforderungen an die Nachweisführung und fordert zusätzlich zur Protokollierung weitere Angaben. Auch in dieser Regelung kommt zum Ausdruck, dass es nicht auf die Stelle des Empfängers ankommt, sondern auf den Zweck der Übermittlung. Es bedarf einer zulässigen Zweckänderung, die im Rahmen des Anwendungsbereichs der Richtlinie (EU) 2016/680 liegt, ansonsten ist die Zweckänderung an den Vorgaben der Verordnung (EU) 2016/679 zu messen. Unter letzteren Fall ist der bisherige § 44 Absatz 2 PolG a.F. zu fassen (Datenübermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs auf deren Antrag). Anwendungsfall für eine Übermittlung an eine nichtöffentliche Stelle für polizeiliche Zwecke ist die Übermittlung personenbezogener Daten an Telekommunikationsdiensteanbieter, um von diesen Verkehrsdaten abzufragen.

Zu Absatz 5

Absatz 5 übernimmt weitgehend die Regelungen des § 42 Absätze 3, 5 und 6 PolG a.F. zur Einrichtung automatisierter Abrufverfahren und ergänzt diese um die Vorgabe, dass auch für diese Form der Datenübermittlung der Grundsatz der hypothetischen Datenneuerhebung einzuhalten ist. In Harmonisierung mit § 25 Absatz 7 BKAG wird der Zusatz aufgenommen, dass ein automatisiertes Abrufverfahren nur eingerichtet werden darf, „soweit diese Form der Datenübermittlung unter Berücksichtigung der schutzwürdigen Interessen der betroffenen Personen wegen der Vielzahl der Übermittlungen oder wegen ihrer besonderen Eilbedürftigkeit angemessen ist“. Die in § 42 Absatz 5 Satz 2 und Absatz 6 PolG a.F. in Verbindung mit § 8 Absatz 2 LDSG a.F. ausdrücklich festgelegte Protokollierungspflicht kann aufgrund der nunmehr allgemein geltenden Protokollierungspflichten entfallen.

Zu Absatz 6

Absatz 6 ist inhaltlich weitgehend an die Regelung des § 25 Absatz 6 BKAG angelehnt.

Zu Absatz 7
Absatz 7 ist inhaltlich weitgehend an die Regelung des § 25 Absatz 8 BKAG sowie die bislang gültige allgemeine Regelung des § 16 Absatz 2 LDSG a.F. angelehnt.

39. Zu § 60 (Datenübermittlung an Mitgliedstaaten der Europäischen Union)
Gemäß Artikel 9 Absatz 4 der Richtlinie (EU) 2016/680 dürfen Datenübermittlungen an Mitgliedstaaten der Europäischen Union keinen anderen Verarbeitungsbedingungen unterstellt werden als Datenübermittlungen im Inland. Ein effektiver und wirksamer polizeilicher Informationsaustausch zwischen den Sicherheitsbehörden der Mitgliedstaaten der Europäischen Union ist ein Schlüsselelement für die Gewährleistung der Sicherheit in Deutschland und der Europäischen Union. Dementsprechend stellt die Vorschrift Datenübermittlungen an andere Mitgliedstaaten der Europäischen Union den inländischen Datenübermittlungen gleich. Die §§ 43 ff. PolG a.F. können in ihrer bisherigen Form nicht aufrechterhalten werden, weil sie für die innereuropäische Datenübermittlung teilweise andere Bedingungen vorsahen als für die Übermittlung im nationalen Bereich und damit nicht den Vorgaben der Richtlinie (EU) 2016/680 entsprechen.

Der Rahmenbeschluss 2008/977/JI (Rahmenbeschluss Datenschutz) wird gemäß Artikel 59 Absatz 1 der Richtlinie (EU) 2016/680 mit Wirkung vom 6. Mai 2018 aufgehoben. Aus Artikel 60 der Richtlinie (EU) 2016/680 ergibt sich, dass der Rahmenbeschluss 2006/960/JI (Schwedische Initiative) sowie der Ratsbeschluss 2008/615/JI (Ratsbeschluss Prüm) von der Richtlinie (EU) 2016/680 unberührt bleiben.

Zu Absatz 1
Durch Verweis auf die Vorschrift zur Datenübermittlung im nationalen Bereich wird mit Absatz 1 sowohl das Gleichbehandlungsgebot für innereuropäische Datenübermittlungen konsequent umgesetzt, als auch die Geltung des Grundsatzes der hypothetischen Datenneuerhebung sichergestellt.

Nummer 1 stellt die Übermittlung an Behörden, sonstige öffentliche und nichtöffentliche Stellen anderer Mitgliedstaaten der Europäischen Union der Übermittlung an entsprechende inländische Stellen gleich. Auch bei der innereuropäischen Datenübermittlung ist folglich danach zu differenzieren, ob es sich um eine polizeiliche Stelle, eine sonstige öffentliche Stelle oder eine nichtöffentliche Stelle eines anderen Mitgliedstaates handelt. Je nachdem sind die Regelungen des § 59 Absatz 2, Absatz 3 oder Absatz 4 zu berücksichtigen. Den Regelfall einer Übermittlung nach Nummer 1 wird eine Übermittlung an eine Polizeibehörde oder eine sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stelle eines Mitgliedstaates der Europäischen Union darstellen. Als solche können insbesondere jene Stellen gelten, die vom betreffenden 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 15.3.2007, S. 26) benannt wurden.

Mit Nummer 2 wird klargestellt, dass sich auch Datenübermittlungen an zwischen- und überstaatliche Stellen der Europäischen Union oder deren Mitgliedstaaten, die mit Aufgaben der Verhütung und Verfolgung von Straftaten befasst sind, nach denselben Regelungen 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, etwa Europol.

Nummer 3 war in Umsetzung des Rahmenbeschlusses 2006/960/JI (Schwedische Initiative) bereits in § 43a Absatz 8 PolG a.F. enthalten und bestimmt die Gleichstellung der Schengen-assoziierten Staaten.

Zu Absatz 2
Absatz 2 entspricht § 43c PolG a.F..

40. Zu § 61 (Datenübermittlung im internationalen Bereich)
An die Datenübermittlung im außereuropäischen Bereich legen sowohl die Richtlinie (EU) 2016/680 als auch das Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 strenge Maßstäbe an.

Die Richtlinie (EU) 2016/680 unterscheidet in den Artikeln 35 ff. zwischen der Übermittlung aufgrund eines Angemessenheitsbeschlusses der Europäischen Kommission, der Übermittlung ohne Angemessenheitsbeschluss, jedoch vorbehaltlich geeigneter Garantien, und der Übermittlung ohne Angemessenheitsbeschluss und ohne geeignete Garantien.

Sofern ein Beschluss der Europäischen Kommission vorliegt, dass ein Drittland oder eine internationale Organisation ein angemessenes Datenschutzniveau bietet, bedarf eine Datenübermittlung dorthin keiner besonderen Genehmigung. Liegt kein solcher Beschluss vor, hat die übermittelnde Stelle entweder sicherzustellen, dass in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind, oder nach Beurteilung aller Umstände, die bei der Übermittlung personenbezogener Daten eine Rolle spielen, eine Bewertung zu treffen, ob geeignete Garantien zum Schutz personenbezogener Daten bestehen. Liegen weder ein Angemessenheitsbeschluss noch geeignete Garantien vor, ist eine Übermittlung nur im Einzelfall und nur unter engen Voraussetzungen zulässig.

Das Bundesverfassungsgericht (Rn. 324ff.) hat hierzu ausgeführt, dass die Übermittlung personenbezogener Daten an öffentliche Stellen anderer Staaten, ebenso wie die Übermittlung an innerstaatliche Stellen, eine Zweckänderung darstellt und insoweit nach den allgemeinen Grundsätzen jeweils an den Grundrechten zu messen ist, in die bei der Datenerhebung eingegriffen wurde. Für die Übermittlung ins internationale Ausland müssten aber auch mit Blick auf die Achtung fremder Rechtsordnungen und Rechtsanschauungen eigene verfassungsrechtliche Bedingungen gelten. Obwohl eine Übermittlung von Daten ins Ausland dazu führe, dass die Gewährleistungen des Grundgesetzes nach der Übermittlung nicht mehr als solche zur Anwendung gebracht werden können und stattdessen die im Ausland geltenden Standards Anwendung finden, stünde dies einer Übermittlung ins Ausland nicht grundsätzlich entgegen. Allerdings hat das Bundesverfassungsgericht mit Blick auf die Wahrung datenschutzrechtlicher Garantien für eine Übermittlung Grenzen aufgezeigt. Der Gesetzgeber habe dafür Sorge zu tragen, dass der Grundrechtsschutz durch eine Übermittlung der von deutschen Behörden erhobenen Daten ins Ausland und an internationale Organisationen ebenso wenig ausgehöhlt wird wie durch eine Entgegennahme

und Verwertung von durch ausländische Behörden menschenrechtswidrig erlangten Daten. Ferner ergeben sich nach den Ausführungen des Bundesverfassungsgerichts Grenzen hinsichtlich der Nutzung der Daten durch den Empfängerstaat, wenn dort Menschenrechtsverletzungen zu besorgen sind. Zwingend auszuschließen sei danach eine Datenübermittlung an Staaten, wenn zu befürchten ist, dass dort elementare rechtsstaatliche Grundsätze verletzt werden. Keinesfalls dürfe der Staat seine Hand zu Verletzungen der Menschenwürde reichen (vgl. auch BVerfG, Beschluss des Zweiten Senats vom 15. Dezember 2015 - 2 BvR 2735/14 -, Rn. 62 m.w.N.). Danach setze die Übermittlung von Daten an das internationale Ausland eine Begrenzung auf hinreichend gewichtige Zwecke, für die die Daten übermittelt und genutzt werden dürfen, sowie die Vergewisserung seitens des deutschen Staates über einen rechtsstaatlichen Umgang mit diesen Daten im Empfängerland voraus. Dazu bedürfe es der Gewährleistung einer wirksamen inländischen Kontrolle, deren Anforderungen durch normenklare Grundlagen im deutschen Recht sicherzustellen seien. Vor diesem Hintergrund hält das Bundesverfassungsgericht Regelungen zur aufsichtlichen Kontrolle und zu Berichtspflichten hinsichtlich der Übermittlungspraxis für erforderlich.

Zu Absatz 1

In Anlehnung an § 27 Absatz 1 BKAG bestimmt Absatz 1 allgemeine Voraussetzungen für die Datenübermittlung in das internationale Ausland, die kumulativ zu den Voraussetzungen einer der Absätze 2 bis 4 vorliegen müssen. Durch den Verweis auf die Vorschrift zur Zweckbindung und Zweckänderung wird klargestellt, dass der Grundsatz der hypothetischen Datenneuerhebung auch für die Übermittlung von Daten im internationalen Bereich gilt, wobei die Übermittlung selbst die Zweckänderung darstellt.

Zu Absatz 2

Absatz 2 regelt in Umsetzung von Artikel 35 und Artikel 36 der Richtlinie (EU) 2016/680 und in Anlehnung an § 78 des Bundesdatenschutzgesetzes (BDSG) die allgemeinen Voraussetzungen für die Übermittlung von Daten im internationalen Bereich, wenn ein entsprechender Angemessenheitsbeschluss der Europäischen Kommission vorliegt.

Zu Absatz 3

In Absatz 3 werden in Umsetzung von Artikel 37 der Richtlinie (EU) 2016/680 und in Anlehnung an § 79 BDSG zusätzliche Voraussetzungen für Datenübermittlungen an Stellen in Drittstaaten, zu denen die Europäische Kommission keinen Angemessenheitsbeschluss gemäß Artikel 36 der Richtlinie (EU) 2016/680 gefasst hat, formuliert. In diesen Konstellationen kommt dem Verantwortlichen die Aufgabe zu, das Vorliegen geeigneter Garantien für den Schutz personenbezogener Daten beim Empfänger zu beurteilen. Um die Beurteilung zu sichern und zu dokumentieren, kann die Datenübermittlung mit Verarbeitungsbedingungen, etwa Löschverpflichtungen nach Zweckerreichung oder Weiterübermittlungsverboten, verbunden werden. Ferner werden die in Artikel 37 Absatz 2 und 3 der Richtlinie (EU) 2016/680 vorgesehenen Dokumentations- und Unterrichtungspflichten festgeschrieben.

Zu Absatz 4

Absatz 4 dient der Umsetzung von Artikel 38 der Richtlinie (EU) 2016/680 und legt in Anlehnung an § 80 BDSG Möglichkeiten zur Datenübermittlung in solchen Konstellationen fest, in denen weder ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt noch die in Absatz 3 Nummern 1 und 2 beschriebenen Garantien bestehen. In solchen Fällen ist die Zulässigkeit einer Übermittlung an die genannten engen Voraussetzungen geknüpft.

Zu Absatz 5

Absatz 5 dient der Umsetzung von Artikel 39 der Richtlinie (EU) 2016/680 und regelt in Anlehnung an § 81 BDSG sowie § 27 Absatz 8 BKAG Übermittlungen in besonderen Einzelfällen, die sich dadurch auszeichnen, dass der Kreis der möglichen Empfänger über öffentliche Stellen, die für Richtlinien-Zwecke zuständig sind, hinaus auf sonstige öffentliche und private Stellen ausgeweitet wird. Anwendungsbeispiel ist etwa das Ersuchen an einen im internationalen Ausland ansässigen Telekommunikationsdienstleister, was notwendigerweise mit der Übermittlung personenbezogener Daten verbunden ist. Für solche Fälle gelten die genannten engen Voraussetzungen, insbesondere die normierte strikte Zweckbindung der übermittelten Daten.

Zu Absatz 6

Absatz 6 regelt die Verantwortlichkeit für die Zulässigkeit der Datenübermittlung. In Abweichung von der entsprechenden Regelung bei der Datenübermittlung im nationalen Bereich sowie innerhalb der Europäischen Union obliegt die Verantwortung hier stets der Polizei, unabhängig davon, welche Stelle die Übermittlung initiiert hat.

Zu Absatz 7
Gemäß Artikel 61 der Richtlinie (EU) 2016/680 stellt Absatz 7 klar, dass vor dem 6. Mai 2016 geschlossene internationale Übereinkünfte von den Regelungen dieser Vorschrift unberührt bleiben.

41. Zu § 62 (Übermittlungsverbote und Verweigerungsgründe)
Die Vorschrift orientiert sich an § 28 BKAG, der schon zuvor bestehende Übermittlungsverbote und Verweigerungsgründe in einer Zentralnorm zusammenfasst und um die Vorgaben des Bundesverfassungsgerichts ergänzt.

Zu Absatz 1
Die in Absatz 1 genannten Gründe, die einer Datenübermittlung entgegenstehen, gelten für sämtliche Übermittlungen nach diesem Gesetz, also sowohl innerstaatliche als auch solche an Stellen in anderen Mitgliedstaaten der Europäischen Union als auch an Stellen in Drittstaaten.

Zu Absatz 2
Absatz 2 Satz 1 ergänzt Absatz 1 um weitere Übermittlungsverbote, die allerdings nur bezüglich Datenübermittlungen an Stellen in anderen Mitgliedstaaten der Europäischen Union und an Stellen in Drittstaaten gelten. Um den Anforderungen des Bundesverfassungsgerichts (Rn. 328) gerecht zu werden, wird die Besorgnis der Verletzung von elementaren rechtsstaatlichen Grundsätzen oder Menschenrechten als Regelbeispiel explizit genannt.

Satz 2 verweist auf die beim Bundeskriminalamt zu führende 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. Zum Führen dieser Aufstellung ist das Bundeskriminalamt nach § 28 Absatz 3 BKAG verpflichtet.

Damit wird den vom Bundesverfassungsgericht aufgestellten Anforderungen an die Vergewisserung über das Vorhandensein eines datenschutzrechtlich angemessenen und mit elementaren Menschenrechtsgewährleistungen zu vereinbarenden Umgangs mit den übermittelten Daten im Empfängerstaat Rechnung getragen. Das Bundeskriminalamt hat die Aufstellung fortlaufend zu aktualisieren und hierbei insbesondere die jeweiligen Erkenntnisse der Bundesregierung und die Angemessenheitsbeschlüsse der Europäischen Kommission gemäß Artikel 36 der Richtlinie (EU) 2016/680 zu berücksichtigen.

42. Zu §§ 63 bis 69 (Allgemeines bis Gebrauch von Explosivmitteln)
Die Regelungen entsprechen den §§ 49 bis 54a des bisherigen PolG. Die Verweise werden aufgrund der neuen Nummerierung des Gesetzes angepasst.

43. Zu § 70 (Unterscheidung verschiedener Kategorien betroffener Personen)
Entsprechend den Vorgaben des Artikels 6 der Richtlinie (EU) 2016/680 werden in der Vorschrift verschiedene Kategorien betroffener Personen festgelegt, zwischen denen bei der Verarbeitung von Daten zu unterscheiden ist. Dabei gibt Artikel 6 der Richtlinie (EU) 2016/680 Kategorien betroffener Personen vor, belässt aber Spielräume für weitere. Um den Änderungsbedarf der landesspezifischen Datenbestände möglichst gering zu halten, werden die bereits normierten Kategorien des § 20 PolG a.F. weitgehend übernommen. Gleichzeitig wird eine Harmonisierung mit den entsprechenden Kategorien des BKAG angestrebt, um die Teilnahme am Informationsverbund des Bundeskriminalamts zu erleichtern und rechtssicherer zu gestalten. Unter welchen Voraussetzungen die Verarbeitung personenbezogener Daten von betroffenen Personen der hier nur abstrakt aufgeführten Kategorien tatsächlich zulässig ist, wird in den konkreten Eingriffsbefugnissen bestimmt.

Die Kategorie des „potentiellen Straftäters“ in Nummer 3 wird an die restriktive Auslegung des Bundesverfassungsgerichts angeglichen.

Der Anwendungsbereich des § 20 Absatz 3 Nummer 4 PolG a.F. („Personen im räumlichen Umfeld einer in besonderem Maß als gefährdet erscheinenden Person“) zielte sowohl auf potentielle Täter als auch auf sonstige Personen im Umkreis einer gefährdeten Person ab. Vor dem Hintergrund der restriktiven Auslegung des Begriffs

des potentiellen Täters durch die Rechtsprechung erscheint der Anwendungsbereich einer solchen Kategorie bedenklich weit (so im Ergebnis auch Belz/Mussmann, § 20 Rn. 49). Die Kategorie wurde daher bewusst so nicht übernommen. Verbindungspersonen zu potentiellen Opfern sind jedoch über den Verweis in Nummer 5 auf Nummer 4 erfasst. Potentielle Täter sind nunmehr von der zwar engeren, aber verfassungskonformen Nummer 3 erfasst.

Anders als in § 20 PolG a.F. werden in Nummer 6 der Zustands- und der Verhaltensstörer nun explizit in die Auflistung der zu unterscheidenden Kategorien betroffener Personen aufgenommen.

Um die Unterscheidung der verschiedenen Kategorien betroffener Personen bei der weiteren Verarbeitung der Daten zu gewährleisten, ist es erforderlich, dass die Kategorisierung bereits bei der erstmaligen Speicherung der Daten vorgenommen wird. Diese Möglichkeit ist in den technischen Systemen entsprechend zu verankern.

44. Zu § 71 (Verarbeitung besonderer Kategorien personenbezogener Daten)
Die Vorschrift dient der Umsetzung des Artikels 10 der Richtlinie (EU) 2016/680. Sie bestimmt, dass die Verarbeitung besonderer Kategorien personenbezogener Daten nur zulässig ist, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist.

Zu Absatz 1
Die in § 33 Absatz 3 LDSG a.F. u.a. für Zwecke der Gefahrenabwehr und der Strafverfolgung enthaltene Ausnahme von der in Absatz 1 festgelegten eingeschränkten Zulässigkeit der Verarbeitung besonderer Arten personenbezogener Daten kann vor dem Hintergrund des Artikels 10 der Richtlinie (EU) 2016/680 nicht aufrecht erhalten werden. Auch zu Zwecken der polizeilichen Aufgabenerfüllung dürfen besondere Kategorien personenbezogener Daten nur verarbeitet werden, wenn dies unbedingt erforderlich ist und wenn gleichzeitig geeignete Garantien für die Rechtsgüter der betroffenen Person vorgesehen werden.

Solche geeigneten Garantien für die Rechtsgüter der betroffenen Person können zum Beispiel darin bestehen, dass spezifische Anforderungen an die Datensicherheit, die Zugriffsregelungen oder die Datenschutzkontrolle gestellt werden, dass die

an den Verarbeitungsvorgängen Beteiligten besonders sensibilisiert werden oder dass insbesondere im Fall einer Übermittlung oder Verarbeitung zu anderen Zwecken die Daten entsprechend gekennzeichnet werden. Aus Erwägungsgrund 37 der Richtlinie folgt zudem, dass besondere Kategorien personenbezogener Daten nur in Verbindung mit anderen Daten über die betroffene natürliche Person erhoben werden sollten. Damit kann zum Beispiel ein sogenanntes „racial profiling“ vermieden werden.

Die Verarbeitung zu den in Artikel 10 Buchstaben b) und c) der Richtlinie (EU) 2016/680 genannten Zwecken, d. h. zur Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person oder wenn Daten verarbeitet werden sollen, die die betroffene Person offensichtlich öffentlich gemacht hat, sind von der Voraussetzung, dass die Verarbeitung zur Aufgabenerfüllung unbedingt erforderlich sein muss, umfasst.

Zu Absatz 2
Absatz 2 wurde in Anlehnung an § 16 Absatz 6 BKAG neu in das PolG aufgenommen. Vor dem Hintergrund der strengen Vorgaben der Richtlinie (EU) 2016/680 hinsichtlich der Verarbeitung besonderer Kategorien personenbezogener Daten wird die Verarbeitung personengebundener und ermittlungsunterstützender Hinweise, die oftmals besondere Kategorien personenbezogener Daten umfassen, explizit geregelt.

Ermittlungsunterstützende Hinweise im Sinne der Nummer 2 sind Hinweise auf Besonderheiten einer natürlichen Person, die dazu geeignet sind, einen polizeilichen Kontext zu verdeutlichen, polizeiliches Handeln zielgerichteter zu steuern beziehungsweise zu unterstützen oder die dem Schutz Dritter dienen. Sie sind darüber hinaus auch geeignet, Datenbestände für Ermittlungen zu kennzeichnen beziehungsweise zu selektieren.

45. Zu § 72 (Kennzeichnungspflicht)
Der vom Bundesverfassungsgericht (Rn. 284 ff.) konkretisierte Grundsatz der hypothetischen Datenneuerhebung lässt sich nur umsetzen, wenn erhobene personenbezogene Daten bei ihrer Speicherung in den polizeilichen Informationssystemen mit den notwendigen Zusatzinformationen versehen, also gekennzeichnet werden. Die

Teilnahme am Informationsverbund des Bundeskriminalamts wird künftig nur noch statthaft sein, wenn die Kennzeichnungsregelungen bei allen Verbundteilnehmern umgesetzt werden. Da sich das Urteil des Bundesverfassungsgerichts nur auf eingriffsintensive Maßnahmen bezieht, wäre eine Kennzeichnung bei weniger schwerwiegenden Erhebungsmaßnahmen und außerhalb der Teilnahme am Informationsverbund zwar nicht zwingend erforderlich. Gleichwohl wird eine Kennzeichnungspflicht für alle personenbezogenen Daten festgelegt, die in einem Informationssystem der Polizei gespeichert werden. Zum einen ist dies vor dem Hintergrund konsequent, dass der Grundsatz der hypothetischen Datenneuerhebung in § 15 auch auf Daten aus nicht eingriffsintensiven Maßnahmen übertragen wird. Zum anderen kann sich die Verbundrelevanz bestimmter Daten auch erst zu einem späteren Zeitpunkt ergeben, womit aufwendige Nachkennzeichnungen erforderlich würden, wenn die Daten nicht bereits bei ihrer ursprünglichen Speicherung eine Kennzeichnung erhielten.

Zu Absatz 1

Absatz 1 Satz 1 sieht 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 betroffener Personen (Nummer 2), durch die Angabe der Rechtsgüter, deren Schutz die Erhebung dient oder der Straftaten oder Ordnungswidrigkeiten, deren Verhütung, Ermittlung, Aufdeckung oder Verfolgung die Erhebung dient (Nummer 3), und durch die Angabe der Stelle, die sie erhoben hat (Nummer 4) zu kennzeichnen sind. Nach Satz 2 kann die Kennzeichnung durch die Angabe der Rechtsgrundlage des der Erhebung zugrunde liegenden Mittels ergänzt werden. Satz 3 sieht für personenbezogene Daten, die die Polizei nicht aktiv erhoben, sondern anderweitig erlangt hat (sogenannte „aufgedrängte Daten“) vor, dass diese soweit möglich unter Angabe der Herkunft der Daten zu kennzeichnen sind.

Zu Absatz 2

Zur Vermeidung einer weiteren Verarbeitung von Daten, die nicht dem Grundsatz der hypothetischen Datenneuerhebung entspricht, bestimmt Absatz 2, dass personenbezogene Daten, die nicht den Anforderungen des Absatzes 1 entsprechend gekennzeichnet sind, solange nicht weiter verarbeitet werden dürfen, bis die Kennzeichnung nachgeholt wurde.

Zu Absatz 3

Damit der Grundsatz der hypothetischen Datenneuerhebung auch bei der weiteren Verarbeitung von Daten durch andere Stellen beachtet werden kann, regelt Absatz 3, dass im Falle der Übermittlung von Daten die empfangende Stelle darauf hinzuweisen ist, die Kennzeichnung aufrechtzuerhalten.

Zu Absatz 4

Absatz 4 Satz 1 legt eine Ausnahme von der Kennzeichnungspflicht nach Absatz 1, dem Weiterverarbeitungsverbot nach Absatz 2 und der Hinweispflicht nach Absatz 3 für den Fall fest, dass eine Kennzeichnung tatsächlich nicht möglich ist.

Ferner enthält Satz 2 eine Übergangsregelung, deren Geltung in § 135 zeitlich begrenzt wird. Sie soll die weitere Verarbeitung von Altdaten in den polizeilichen Informationssystemen ermöglichen, wenn diese nicht so schnell technisch weiterentwickelt werden können, dass den Anforderungen der Kennzeichnungspflicht bereits mit Inkrafttreten dieses Gesetzes nachgekommen werden kann. In der Übergangsphase zwischen Geltung der Neuregelungen und technischer Ertüchtigung der Systeme sollte durch Dienstanweisungen oder ähnliche Maßnahmen sichergestellt werden, dass zumindest freitextlich die nach dieser Vorschrift erforderlichen Angaben zu personenbezogenen Daten erfasst werden.

46. Zu § 73 (Protokollierungspflicht)

Die Vorschrift setzt Artikel 25 der Richtlinie (EU) 2016/680 um, der eine generelle Pflicht zur Protokollierung der wesentlichen Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen vorsieht. § 135 Absatz 2 enthält in Umsetzung von Artikel 63 Absatz 2 der Richtlinie (EU) 2016/680 eine Übergangsregelung bis zum 6. Mai 2023 für solche Verarbeitungssysteme, die vor dem 6. Mai 2016 eingerichtet wurden und die die technischen Anforderungen noch nicht erfüllen, so dass die Einhaltung der Pflichten des § 73 mit einem unverhältnismäßigen Aufwand verbunden wäre.

Zu Absatz 1

Absatz 1 bestimmt die Verarbeitungsvorgänge, die zu protokollieren sind, soweit nichts anderes geregelt ist. Abweichende Regelungen finden sich insbesondere in § 74 für verdeckte und eingriffsintensive Maßnahmen.

Zu Absatz 3
In Umsetzung von Artikel 25 Absatz 2 der RL (EU) 2016/680 bestimmt Absatz 3 Satz 1, zu welchen Zwecken die Protokolldaten verwendet werden dürfen.

Aufgrund der gesetzlichen Regelung der Protokollierungspflichten kann § 7 DVO-PolG entfallen.

47. Zu § 74 (Protokollierungspflicht bei verdeckten und eingriffsintensiven Maßnahmen)
An die Protokollierung von Verarbeitungsvorgängen bezüglich solcher Daten, die aus verdeckten beziehungsweise eingriffsintensiven Maßnahmen gewonnen werden, setzt das Bundesverfassungsgericht mit seinem Urteil vom 20. April 2016 (Rn. 141) strenge Maßstäbe an. Danach ist erforderlich, dass die Datenerhebungen vollständig protokolliert werden und die Protokollierung hinreichende Angaben zu dem zu kontrollierenden Vorgang enthält. Die Protokollierungspflicht dient insbesondere der Gewährleistung einer wirksamen aufsichtlichen Kontrolle und damit der Gewährleistung eines effektiven Grundrechtsschutzes der betroffenen Personen.

Zu Absatz 1
Absatz 1 bestimmt die Angaben, auf die sich jede Protokollierung bei den genannten verdeckten und eingriffsintensiven Maßnahmen zu erstrecken hat. Eine andere Regelung im Sinne des Halbsatzes 1 ist zum Beispiel in § 51 Absatz 3 Satz 2 enthalten, wonach die Datenerhebung und der Datenabgleich beim Einsatz automatischer Kennzeichenlesesysteme gerade nicht protokolliert werden dürfen.

Zu Absatz 2
Bezogen auf die jeweilige Maßnahme legt Absatz 2 weitere zu protokollierende Angaben und insbesondere die zu protokollierenden Personen fest. Betreffen die Angaben die vorgenommenen nicht nur flüchtigen Veränderungen an einem informations-

technischen System, genügt eine abstrakte Bezeichnung, wenn der konkreten Bezeichnung gewichtige Gründe, insbesondere des Geheimschutzes oder einsatztaktischer Art, entgegenstehen.

Zu Absatz 3

Absatz 3 bestimmt, dass der Aufwand zur Feststellung der Identität der betroffenen Personen verhältnismäßig sein muss. Andernfalls kann eine Protokollierung unterbleiben.

Zu Absatz 4

Absatz 4 Satz 1 schreibt eine strenge Zweckbindung der Protokolldaten fest, die nur für Zwecke der Benachrichtigung der betroffenen Person oder dafür verwendet werden dürfen, um der betroffenen Person oder einer dazu befugten Stelle die Prüfung der Rechtmäßigkeit der Maßnahme zu ermöglichen. Satz 2 fordert die automatisierte Löschung der Protokolldaten nach Abschluss der Kontrolle durch die Aufsichtsbehörde für den Datenschutz, es sei denn, die Aufbewahrung ist zu Benachrichtigungszwecken noch erforderlich.

48. Zu § 75 (Pflicht zur Berichtigung, Löschung sowie Einschränkung der Verarbeitung)

Die Vorschrift dient insbesondere der Umsetzung des Artikels 16 der Richtlinie (EU) 2016/680 in seiner Ausformung als Pflicht des datenschutzrechtlich Verantwortlichen. Systematisch werden hier die eigenständigen Pflichten der Polizei zur Berichtigung und Löschung personenbezogener Daten sowie zur Einschränkung ihrer Verarbeitung geregelt, die unabhängig davon bestehen, ob eine betroffene Person darum ersucht. Die spiegelbildlich bestehenden Rechte der betroffenen Person auf Berichtigung und Löschung personenbezogener Daten sowie auf Einschränkung ihrer Verarbeitung sind in § 92 geregelt. Ferner übernimmt die Vorschrift Elemente des § 38 PolG a.F. hinsichtlich der Erforderlichkeit einer weiteren Datenspeicherung, die einer Löschpflicht entgegensteht.

Zu Absatz 1

In Absatz 1 Satz 1 wird die Pflicht der Polizei zur Berichtigung unrichtiger Daten festgelegt. Diese Pflicht folgt aus dem in Artikel 4 Absatz 1 Buchstabe d) der Richtlinie

(EU) 2016/680 genannten Grundsatz der sachlichen Richtigkeit von Daten sowie im Umkehrschluss aus Artikel 16 Absatz 1 der Richtlinie (EU) 2016/680. Satz 2 dient der Umsetzung von Artikel 16 Absatz 5 der Richtlinie (EU) 2016/680.

Zu Absatz 2

Absatz 2 dient der Umsetzung von Artikel 16 Absatz 2 der Richtlinie (EU) 2016/680, aus dem ausdrücklich sowohl das Recht der betroffenen Person auf Löschung als auch die unabhängig davon bestehende Pflicht des Verantwortlichen zur Löschung hervorgehen. Die Voraussetzungen, unter denen personenbezogene Daten zu löschen sind beziehungsweise ein Anspruch auf deren Löschung besteht, sind dieselben. Zur Erfüllung einer rechtlichen Verpflichtung der Polizei (Alternative 3) müssen Daten insbesondere dann gelöscht werden, wenn in einer Regelung allgemeine oder spezielle Höchstspeicherfristen festgelegt sind, nach deren Ablauf die Daten zu löschen sind.

Der in Satz 2 enthaltene Verweis auf das Landesarchivgesetz mit der dort bestimmten Anbietungspflicht war zuvor in § 23 Absatz 3 LDSG a.F. enthalten.

Zu Absatz 3

Absatz 3 übernimmt hinsichtlich der Speicherung von Daten, also der Aufschiebung der Löschpflicht, den Regelungsgehalt des § 38 Absätze 2 und 3 PolG a.F. und konkretisiert, unter welchen Voraussetzungen und unter welcher Höchstspeicherfrist die Kenntnis von Daten zur vorbeugenden Bekämpfung von Straftaten als erforderlich im Sinne des Absatzes 2 Alternative 2 anzusehen ist. Durch die Aufrechterhaltung der Altregelung soll unter anderem vermieden werden, dass der vorhandene Datenbestand grundlegend neuen Regeln mit der eventuellen Folge eines umfassenden Anpassungsbedarfs unterworfen wird. Wie nach bisheriger Rechtslage dürfen die Daten zwei Jahre gespeichert bleiben, wenn ein Verdacht beziehungsweise ein Resttatverdacht besteht, dass die betroffene Person eine Straftat begangen hat. Über diese zwei Jahre hinaus dürfen die Daten weiter gespeichert bleiben, wenn entweder tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffene Person zukünftig eine Straftat begehen wird (negative Kriminalprognose) oder wenn aufgrund tatsächlicher Anhaltspunkte der Verdacht besteht, dass die betroffene Person während des Laufs dieser zwei Jahre eine weitere Straftat begangen hat.

Zu beachten ist, dass die Regelungen des § 38 Absätze 2 und 3 PolG a.F. lediglich hinsichtlich der Speicherung der Daten, nicht aber hinsichtlich der Veränderung und weiteren Nutzung der Daten übernommen werden können. Diese in der Altregelung ebenfalls erfassten Formen der weiteren Verarbeitung müssen sich künftig am Grundsatz der hypothetischen Datenneuerhebung messen. Ob und unter welchen Voraussetzungen die Daten für welche Zwecke weiter verarbeitet werden dürfen, ist daher anhand der neuen Vorschriften zur Zweckbindung und Zweckänderung zu beurteilen. Hinsichtlich der Veränderung und weiteren Nutzung gespeicherter Daten geht § 38 Absätze 2 und 3 PolG a.F. folglich in § 15 auf. Auch § 38 Absatz 1 PolG a.F., der die weitere Verarbeitung von Daten betrifft, die zu repressiven Zwecken erhoben wurden, geht in § 15 auf.

Zu Absatz 4

Absatz 4 übernimmt weitgehend den Regelungsgehalt des § 38 Absatz 6 PolG a.F. und bestimmt, wie lange die Speicherung von Daten bestimmter Kategorien betroffener Personen höchstens erforderlich ist. Erfasst sind insbesondere Kontaktpersonen, potenzielle Opfer von Straftaten, Zeugen und Hinweisgeber. Die Befugnis zur Erhebung von Daten dieser Personenkategorien zur vorbeugenden Bekämpfung von Straftaten ergibt sich aus § 43.

Entsprechend den Ausführungen zu Absatz 3 gilt, dass die Vorgängervorschrift nur hinsichtlich der Speicherung übernommen werden kann. Die sonstige weitere Verarbeitung der Daten im engeren Sinne, insbesondere die Nutzung zu anderen Zwecken, richtet sich auch hier nach der neuen Vorschrift des § 15.

Zu Absatz 5

In Absatz 5 wird in Umsetzung von Artikel 16 Absatz 3 der Richtlinie (EU) 2016/680 festgelegt, unter welchen Voraussetzungen die Polizei von einer Berichtigung oder Löschung der Daten absehen kann und stattdessen eine Einschränkung der Verarbeitung dieser Daten vornehmen kann beziehungsweise muss.

Satz 1 regelt die Möglichkeit der Einschränkung der Verarbeitung als Alternative zur Berichtigung für den Fall, dass die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet und die Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann. Nach § 46 Absatz 2 PolG a.F. war für die vom Polizeivollzugsdienst zur vorbeugenden Bekämpfung von Straftaten gespeicherten personenbezogenen Daten in solchen Fällen bislang keine Berichtigung oder Sperrung der Daten vorgesehen. Die Anwendung der entsprechenden §§ 22 und 24 des LDSG a.F. war für diese Fälle ausdrücklich ausgenommen. Aufgrund der Vorgaben der Richtlinie (EU) 2016/680 ist das nicht mehr haltbar. Stattdessen ist für diese Fälle nun als Alternative zur Berichtigung die Einschränkung der Verarbeitung vorzusehen. Entgegen dem Wortlaut des Artikels 16 Absatz 3 Satz 1 Buchstabe a) der Richtlinie (EU) 2016/680 handelt es sich nicht um eine Alternative zur Löschung, sondern um eine Alternative zur Berichtigung.

Ist beabsichtigt, die Einschränkung wieder aufzuheben, ist die betroffene Person zuvor zu unterrichten (Satz 2).

Satz 3 regelt die Pflicht zur Einschränkung der Verarbeitung von Daten anstelle ihrer Löschung, wenn ein berechtigter Grund zu der Annahme besteht, dass eine Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigen würde, wenn die Daten noch zu Beweiszwecken erforderlich sind oder wenn die Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich wäre. In Artikel 16 Absatz 3 der Richtlinie (EU) 2016/680 wird die Einschränkung der Verarbeitung zwar für alle Fälle lediglich als Option dargestellt („kann der Verantwortliche deren Verarbeitung einschränken“). Als Alternative zur Löschung, insbesondere, wenn die Daten zu Beweiszwecken weiter aufbewahrt werden müssen, muss die Einschränkung allerdings als Pflicht angesehen werden. Grundsätzlich kommen als Beweiszwecke nur solche in Betracht, die für die Durchführung von Strafverfahren, mithin für Richtlinien-Zwecke, erforderlich sind.

Allerdings müssen auch solche Fälle erfasst sein, die in direktem Zusammenhang mit der Datenspeicherung stehen, wie zum Beispiel wenn anlässlich einer Auskunftserteilung eine unzulässige Speicherung festgestellt wird. Um einerseits zu verhindern,

dass die der Löschpflicht unterliegenden Daten weiter verarbeitet werden, und andererseits der betroffenen Person die Möglichkeit zu belassen, die Datenspeicherung gerichtlich oder durch die Aufsichtsbehörde für den Datenschutz überprüfen zu lassen, muss die Löschung aufgeschoben und die Verarbeitung der Daten eingeschränkt werden.

Satz 4 normiert eine enge Zweckbindung für Daten, deren Verarbeitung eingeschränkt wurde. Als Konsequenz aus der Einschränkung ihrer Verarbeitung dürfen sie ausschließlich zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand. Um dieser Anforderung gerecht werden zu können, bestimmt Satz 5, dass die Einschränkung samt ihren Gründen eindeutig erkennbar festzuhalten ist. Dies hat durch eine entsprechende Kennzeichnung der betroffenen Daten zu erfolgen.

Zu Absatz 6

Absatz 6 legt in Umsetzung von Artikel 16 Absatz 6 der Richtlinie (EU) 2016/680 fest, dass Fälle der Berichtigung, Löschung oder Einschränkung der Verarbeitung den Empfängern mitzuteilen sind, an die die Daten übermittelt wurden. Für die in § 22 Absatz 2, § 24 Absatz 5 LDSG a.F. noch enthaltene Einschränkung, wonach diese Mitteilungspflicht nicht galt, wenn sie einen unverhältnismäßigen Aufwand erfordern würde, gibt es nach der Richtlinie (EU) 2016/680 keine Grundlage mehr.

Die Verpflichtung der Empfänger, nach Erhalt der Mitteilung die Daten ihrerseits zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken, muss sich aus den richtlinienkonformen Vorschriften ergeben, denen die Empfänger unterliegen.

49. Zu § 76 (Überprüfung der Erforderlichkeit der Speicherung personenbezogener Daten)

Im Einklang mit Artikel 5 der Richtlinie (EU) 2016/680 bestimmt die Vorschrift angemessene Höchstfristen für die regelmäßige Überprüfung der Notwendigkeit einer weiteren Speicherung vorhandener personenbezogener Daten und legt fest, wie die Fristen zu berechnen sind.

Zu Absatz 1

Absatz 1 enthält die grundsätzliche Bestimmung, dass in angemessenen regelmäßigen Zeitabständen eine Überprüfung stattzufinden hat, ob gespeicherte personenbezogene Daten noch erforderlich sind oder ob sie zu berichtigen, zu löschen oder in ihrer Verarbeitung einzuschränken sind.

Zu Absatz 2

Absatz 2 bestimmt gesetzliche Höchstfristen für diese Überprüfung. Bezüglich der Höchstfristen für Erwachsene und Jugendliche wird § 38 Absatz 4 PolG a.F. weitgehend unverändert übernommen. Lediglich die fünfjährige Höchstfrist für Erwachsene nach Vollendung des 70. Lebensjahres in Nummer 1 entfällt aufgrund der gegenläufigen Bestimmung in § 5 Absatz 2 DVOPolG, die für Verbrechen und bestimmte Vergehen eine zehnjährige Überprüfungsfrist vorsieht. Die Höchstfrist für Kinder wird auf fünf Jahre hochgesetzt und damit der Höchstfrist für Jugendliche angeglichen. Insbesondere die jüngsten Erfahrungen mit der Bekämpfung des internationalen Terrorismus haben gezeigt, dass verstärkt auch Kinder in die Täterrolle gedrängt werden. Um Zusammenhänge erkennen und kriminellen Entwicklungen frühzeitig entgegenwirken zu können, ist eine längere Speicherfrist für Kinder aus polizeifachlicher Sicht erforderlich. Nach § 75 Absatz 3 ist ohne das Vorliegen einer entsprechenden negativen Kriminalprognose eine Überprüfung der Erforderlichkeit der weiteren Speicherung ohnehin schon nach zwei Jahren erforderlich. Anpassungen redaktioneller Art erfolgen aufgrund von Änderungen der Bezugsvorschriften im StGB. Die einzelnen konkreten Überprüfungsfristen, die teilweise unter den hier normierten Höchstfristen liegen, ergeben sich aus § 5 DVOPolG.

Zu Absatz 3

Absatz 3 übernimmt nahezu unverändert die Regelung des § 38 Absatz 5 PolG a.F. zur Berechnung der Fristen einschließlich des „Mitzieheffekts“ in Satz 2. Lediglich in Satz 5 wird die Frist zur erneuten Überprüfung der Erforderlichkeit der weiteren Speicherung von drei auf zwei Jahre herabgesetzt, um die bislang bestehende Unstimmigkeit zur Höchstfrist bei Kindern (zwei Jahre) zu beseitigen.

Die Einhaltung der festgelegten Überprüfungsfristen ist durch verfahrensrechtliche Vorkehrungen beziehungsweise geeignete technische Maßnahmen sicherzustellen, insbesondere durch automatische Wiedervorlagen in den technischen Systemen.

50. Zu § 77 (Berichtigung und Einschränkung der Verarbeitung in Akten sowie Vernichtung von Akten)
Die Vorschrift orientiert sich an § 78 BKAG. Ferner greift sie Regelungen zur Datenhaltung in Akten auf, die im LDSG a.F. enthalten waren.

Nach Artikel 2 Absatz 2 der Richtlinie (EU) 2016/680 erstreckt sich ihr Anwendungsbereich auf die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie auf die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Der gewährte Schutz soll nach Erwägungsgrund 18 der Richtlinie (EU) 2016/680 technologieneutral sein. Lediglich solche Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, fallen aus dem Anwendungsbereich der Richtlinie (EU) 2016/680 heraus. Der Vorhalt von Akten geht mit der Ausweitung und Verbesserung der technischen Informationssysteme zwar kontinuierlich zurück. Nichtsdestotrotz gibt es noch immer Bereiche, in denen systematisch Akten geführt werden, wenn auch oft lediglich parallel oder ergänzend zu automatisierten Dateisystemen.

Auch die herkömmliche Form der Datenhaltung ist folglich richtlinienkonform auszugestalten. Dabei gelten zwar dieselben Grundsätze, die für die automatisierte Datenverarbeitung Anwendung finden. Hinsichtlich der Verfahrensweise bei der Berichtigung, Löschung und Einschränkung der Verarbeitung bedarf es allerdings einer gesonderten Regelung, die den tatsächlichen und technischen Unterschieden Rechnung trägt.

51. Zu § 78 (Sicherheit der Datenverarbeitung)
Die Vorschrift dient der Umsetzung des Artikels 29 der Richtlinie (EU) 2016/680. Die Pflicht zum Ergreifen technisch-organisatorischer Maßnahmen zur Datensicherheit ergab sich bislang und im Wesentlichen inhaltsgleich aus § 9 LDSG a.F.. Durch den Wegfall dieser Regelung im Anwendungsbereich der Richtlinie (EU) 2016/680 bedarf es einer eigenständigen Vorschrift im Polizeigesetz.

Zu Absatz 1

Die Maßnahmen nach Absatz 1 sollen gewährleisten, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und dass die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können. Konkretisiert werden die Maßnahmen durch die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik sowie die etablierten Informationssicherheitsprozesse der Polizei Baden-Württemberg.

Ein dem Risiko angemessenes Schutzniveau zu gewährleisten bedeutet, dass sich die Schutzbedürftigkeit der personenbezogenen Daten insbesondere an dem Risiko der Beeinträchtigung der Persönlichkeitsrechte der betroffenen Person zu orientieren hat. Mehr als nach bisherigem Recht steht die betroffene Person damit selbst im Fokus der Risikobewertung.

Die Maßnahmen können unter anderem eine möglichst frühe Pseudonymisierung oder die Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind.

Zu Absatz 2
Die Maßnahmen nach den Nummern 1 bis 11 sind Artikel 29 Absatz 2 der Richtlinie (EU) 2016/680 entnommen. Die Maßnahmen nach den Nummern 12 (Auftragskontrolle) und 13 (Verfügbarkeitskontrolle) waren in § 9 LDSG a.F. enthalten. Sie sind auch im BDSG n.F. enthalten, ebenso wie die Nummer 14 (Trennbarkeit). Letztere Maßnahme erscheint sachdienlich, um den Grundsatz der Zweckbindung umzusetzen. Nummer 15 (Organisationskontrolle) wird aus § 9 Absatz 3 Nummer 11 LDSG a.F. überführt.

Werden personenbezogene Daten in nicht automatisierten Dateien oder in Akten verarbeitet, sind ebenfalls Maßnahmen zu treffen, die verhindern, dass Unbefugte bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung auf die Daten zugreifen können (§ 9 Absatz 5 LDSG a.F.).

52. Zu § 79 (Technikgestaltung und datenschutzfreundliche Voreinstellungen)

Die Vorschrift dient der Umsetzung des Artikels 20 der Richtlinie (EU) 2016/680. Sie formuliert Anforderungen an die datenschutzfreundliche Gestaltung von Datenverarbeitungssystemen („Privacy by Design“, Absatz 1) und an die Implementierung datenschutzfreundlicher Grundeinstellungen („Privacy by Default“, Absatz 2).

Die sich aus dieser Vorschrift ergebenden Anforderungen waren bislang nicht im LDSG a.F. geregelt. Es handelt sich um neue, technikorientierte Verpflichtungen, die durch die Richtlinie (EU) 2016/680 auferlegt werden. Der Aufwand zur Erfüllung dieser Anforderungen sollte im Sinne eines effizienten Mitteleinsatzes in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen.

Insbesondere sind die Auswahl und die Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. Eine angemessene Maßnahme zur Erreichung dieses Ziels kann die frühzeitige Pseudonymisierung von Daten sein, soweit sie möglich ist, ohne den Verarbeitungszweck zu gefährden.

53. Zu § 80 (Datenschutz-Folgenabschätzung)
Die Vorschrift dient der Umsetzung des Artikels 27 der Richtlinie (EU) 2016/680.

Zu Absatz 1
Die in Absatz 1 formulierte Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung entspricht inhaltlich im Wesentlichen der bisherigen Vorabkontrolle gemäß § 12 LDSG a.F.. Das Erfordernis einer Datenschutz-Folgenabschätzung gilt für neue Verarbeitungsvorgänge und für wesentliche Veränderungen an bestehenden Verarbeitungsvorgängen und besteht deshalb grundsätzlich nicht, wenn bereits eine Vorabkontrolle gemäß § 12 LDSG a.F. durchgeführt wurde.

Zu Absatz 2
Absatz 2 greift den Gedanken aus Artikel 35 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 auf. Es ist kein triftiger Grund ersichtlich, weshalb die dort ausdrücklich ermöglichte Arbeitserleichterung bei mehreren ähnlichen Verarbeitungsvorgängen nicht auch im Anwendungsbereich der Richtlinie (EU) 2016/680 zum Tragen kommen sollte.

Zu Absatz 3

Absatz 3 legt den Inhalt der Datenschutz-Folgenabschätzung fest und konkretisiert die in Artikel 27 Absatz 2 der Richtlinie (EU) 2016/680 enthaltenen allgemeinen Angaben unter Übernahme von in Artikel 35 Absatz 7 der Verordnung (EU) 2016/679 enthaltenen zusätzlichen Angaben. Die Beschreibung der Zwecke der Datenverarbeitung sowie eine Bewertung der Verhältnismäßigkeit der Verarbeitung in Bezug auf deren Zwecke erscheint als einer der Schwerpunkte einer Folgenabschätzung unerlässlich, weshalb die Anforderungen der Richtlinie (EU) 2016/680 um diese in der Verordnung (EU) 2016/679 enthaltenen Anforderungen ergänzt werden.

54. Zu § 81 (Verzeichnis von Verarbeitungstätigkeiten)

Die Vorschrift dient der Umsetzung des Artikels 24 der Richtlinie (EU) 2016/680. Die Pflicht zum Führen eines Verfahrensverzeichnisses ergab sich bislang aus § 11 LDSG a.F.. Sie gilt auch für einen Auftragsverarbeiter. Die hierzu notwendige Verpflichtung des Auftragsverarbeiters durch die Polizei ist in der Vorschrift über die Auftragsverarbeitung verankert. Durch die neue richtlinienkonforme Bezeichnung als „Verzeichnis von Verarbeitungstätigkeiten“ ergibt sich keine inhaltliche Änderung, weshalb die nach bisherigem Recht erstellten Verfahrensverzeichnisse grundsätzlich weiter Gültigkeit besitzen und lediglich um nach der Neuregelung gegebenenfalls zu ergänzende Angaben fortzuschreiben sind.

Zu Absatz 1

Die in § 11 Absatz 3 LDSG a.F. enthaltene Einschränkung, wonach die Pflicht zum Führen eines Verfahrensverzeichnisses nicht für Verarbeitungstätigkeiten gilt, die allgemeinen Verwaltungszwecken, insbesondere der Textverarbeitung, dienen, wird übernommen.

Die Nummern 1, 3 und 11 des Absatzes 1 werden aus § 11 Absatz 2 LDSG a.F. überführt und ergänzen insoweit die der Richtlinie (EU) 2016/680 entnommenen Angaben, um nicht hinter den bisherigen Anforderungen zurückzubleiben. Die Bezeichnung des jeweiligen Verfahrens (Nummer 1) erscheint zur Konkretisierung und Abgrenzung von anderen Arten oder Kategorien von Verarbeitungstätigkeiten weiterhin

notwendig. Die Benennung der zugriffsberechtigten Personen oder Personengruppen (Nummer 3) ist vor dem Hintergrund der Zugriffskontrolle und des damit in Zusammenhang stehenden Rechte- und Rollenkonzeptes für das jeweilige Verfahren erforderlich. Die Beschreibung der Hardware, der Vernetzung und der Software (Nummer 11) ist insbesondere zur Überprüfung des technischen Datenschutzes erforderlich.

Zu Absatz 2

Im Unterschied zur bisherigen Rechtslage, nach der das Verfahrensverzeichnis zumindest in Teilen auf Antrag jedermann zur Verfügung zu stellen war (§ 11 Absatz 4 LDSG a.F.), besteht nun bei einer entsprechenden Anfrage nur noch die Pflicht zur Vorlage an die Aufsichtsbehörde für den Datenschutz.

55. Zu § 82 (Auftragsverarbeitung)

Die Vorschrift dient der Umsetzung der Artikel 22 und 23 der Richtlinie (EU) 2016/680. Durch den Wegfall der Altregelung in § 7 LDSG a.F. bedarf es einer eigenständigen Vorschrift im Polizeigesetz. Sie enthält Regelungen für den Fall, dass sich die Polizei eines Auftragsverarbeiters bedient, also einer öffentlichen oder privaten Stelle, die im Auftrag der Polizei Daten verarbeitet. Dabei kann es sich um eine Stelle innerhalb oder außerhalb der Polizei handeln. An der bisherigen Rechtslage, nach der es für die Datenübermittlung an einen Auftragsverarbeiter keiner gesonderten Rechtsgrundlage bedarf, ändert sich nichts.

Zu Absatz 1

Da die datenschutzrechtlichen Anforderungen des Polizeigesetzes auch dann gelten, wenn die Polizei die Datenverarbeitung nicht selbst ausführt, sondern sich einer anderen Stelle bedient, hat sie sicherzustellen, dass sie ihren Verpflichtungen trotz der Auftragsverarbeitung in vollem Umfang nachkommen kann. Sie hat deshalb dafür Sorge zu tragen, dass der Auftragsverarbeiter bei seiner Tätigkeit die datenschutzrechtlichen Anforderungen einhält und die Polizei mit allen erforderlichen Informationen versorgt, die sie benötigt, um die ihr selbst obliegenden Verpflichtungen zu erfüllen.

Zu Absatz 2

Vor dem Hintergrund, dass sowohl der Auftragsverarbeiter als auch Personen, die diesem unterstellt sind, nicht direkt durch das Polizeigesetz verpflichtet sind, hat sich die Polizei durch vertragliche Vereinbarung mit dem Auftragsverarbeiter ein umfassendes Weisungsrecht einzuräumen.

Zu Absatz 3
Ferner hat die Polizei die Einhaltung der ihr obliegenden Verpflichtungen vertraglich oder anhand eines sonstigen verbindlichen Rechtsinstruments an den Auftragsverarbeiter „durchzureichen“. In den Nummern 1 bis 11 sind Pflichtbestandteile einer solchen Vereinbarung aufgelistet.

Die in Nummer 9 genannte Pflicht zur Meldung einer Verletzung des Schutzes personenbezogener Daten beruht auf Artikel 30 Absatz 2 der Richtlinie (EU) 2016/680. Sie ist erforderlich, damit die Polizei ihrerseits der auf Artikel 30 Absatz 1 der Richtlinie (EU) 2016/680 beruhenden Meldepflicht nachkommen kann.

Die in Nummer 10 genannte Pflicht zur Zusammenarbeit mit der Aufsichtsbehörde für den Datenschutz beruht auf Artikel 26 der Richtlinie (EU) 2016/680. Diese Pflicht trifft die Polizei und den Auftragsverarbeiter gleichermaßen.

Die in Nummer 11 genannte Pflicht zum Führen eines Verzeichnisses aller Kategorien von Verarbeitungen beruht auf Artikel 24 Absatz 2 der Richtlinie (EU) 2016/680.

Zu Absatz 4
Die dem Auftragsverarbeiter vertraglich aufzuerlegende Verpflichtung, ohne vorherige schriftliche Genehmigung keine weiteren Auftragsverarbeiter hinzuzuziehen, gilt sowohl hinsichtlich privaten als auch öffentlichen Auftragsverarbeitern. Die Genehmigung eines Unterauftragsverarbeiters kann dann in Betracht kommen, wenn gemäß der Vorschrift des § 62 Absatz 4 BDSG dem weiteren Auftragsverarbeiter dieselben Verpflichtungen auferlegt werden („Zieht ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter hinzu, so hat er diesem dieselben Verpflichtungen aus seinem Vertrag mit dem Verantwortlichen nach Absatz 5 aufzuerlegen, die auch für ihn gelten, soweit diese Pflichten für den weiteren Auftragsverarbeiter nicht schon aufgrund an-

derer Vorschriften verbindlich sind.“). Eine Untersagung einer gewünschten Unterauftragsverarbeitung wird hingegen bei Anhaltspunkten dafür in Betracht kommen, dass der Unterauftragsverarbeiter die Pflichten, die die Polizei dem Auftragsverarbeiter auferlegt hat, nicht erfüllen kann oder wird.

56. Zu § 83 (Gemeinsam Verantwortliche)
Die Vorschrift dient der Umsetzung des Artikels 21 der Richtlinie (EU) 2016/680.

Ein Verantwortlicher ist hier stets eine Stelle innerhalb der Polizei, der weitere Verantwortliche kann eine Stelle innerhalb oder außerhalb der Polizei sein. Für betroffene Personen soll transparent sein, wer unter mehreren Verantwortlichen datenschutzrechtlich verantwortlich ist und an welchen Verantwortlichen sich die betroffene Person zur Geltendmachung ihrer Rechte wenden soll. Unabhängig davon bleibt es den betroffenen Personen aber unbenommen, sich an einen anderen Verantwortlichen zu wenden.

Anwendungsfälle sind zum Beispiel projektbezogene gemeinsame Dateien mit dem Landesamt für Verfassungsschutz nach § 46 mit der dort teilweise geregelten Festlegung der Verantwortlichkeiten, ferner der Informationsverbund mit dem Bundeskriminalamt. Hierzu enthält das BKAG Festlegungen bezüglich der Verantwortlichkeiten. So ist in § 31 BKAG die datenschutzrechtliche Verantwortung im polizeilichen Informationsverbund und in § 85 BKAG die Ausübung der Betroffenenrechte im polizeilichen Informationsverbund sowie bei projektbezogenen gemeinsamen Dateien geregelt.

57. Zu § 84 (Automatisierte Entscheidungsfindung im Einzelfall)
Die Vorschrift dient der Umsetzung des Artikels 11 der Richtlinie (EU) 2016/680.

Zu Absatz 1
Absatz 1 bestimmt, dass eine Entscheidungsfindung, die für die betroffene Person eine nachteilige Rechtsfolge hat oder sie sonst erheblich beeinträchtigt, nicht ausschließlich auf einer automatischen Verarbeitung ihrer personenbezogenen Daten

beruhen darf, es sei denn, dies ist ausdrücklich durch eine gesetzliche Regelung erlaubt, die zumindest das Recht auf persönliches Eingreifen seitens der Polizei vorsieht.

Im Regelfall erfolgt im Anschluss an eine automatisierte Überprüfung polizeilicher Daten, zum Beispiel im Rahmen einer Zuverlässigkeitsüberprüfung, eine abschließende Entscheidung des Sachbearbeiters, so dass die Entscheidung selbst nicht automatisiert getroffen wird. Daher dürfte die praktische Relevanz der Vorschrift für die polizeiliche Arbeit derzeit gering sein. Im Hinblick auf eventuelle künftige Verfahrensweisen ist diese Bestimmung der Richtlinie (EU) 2016/680 allerdings aufzunehmen.

Zu Absatz 2
Absatz 2 dient dem strengen Schutz der besonderen Kategorien personenbezogener Daten.

Zu Absatz 3
Absatz 3 sieht vor, dass Profiling, das auf der Grundlage besonderer Kategorien personenbezogener Daten eine Diskriminierung zur Folge hat, verboten ist.

58. Zu § 85 (Allgemeine Informationspflicht)
Die Vorschrift dient der Umsetzung des Artikels 13 Absatz 1 in Verbindung mit Artikel 12 Absatz 1 der Richtlinie (EU) 2016/680.

Die allgemeine Informationspflicht dient der Transparenz gegenüber der betroffenen Person und soll dieser ermöglichen, ihre Rechte auszuüben. Die Pflicht kann durch Übermittlung der Informationen in einer beliebigen geeigneten Form erfüllt werden. Dazu zählt auch die elektronische Übermittlung, zum Beispiel durch Veröffentlichung auf der Website der zuständigen Behörde (Erwägungsgrund 42 der Richtlinie (EU) 2016/680).

59. Zu § 86 (Benachrichtigung bei verdeckten und eingriffsintensiven Maßnahmen)
Die Vorschrift dient der Umsetzung des Artikels 13 Absatz 2 der Richtlinie (EU) 2016/680 sowie der Vorgaben des Bundesverfassungsgerichts, die es im Urteil vom

20. April 2016 an die verhältnismäßige Ausgestaltung eingriffsintensiver Überwachungsmaßnahmen aufgestellt hat (Rn. 136).

Neben der allgemeinen Informationspflicht des Artikels 13 Absatz 1 sieht Artikel 13 Absatz 2 der Richtlinie (EU) 2016/680 eine weitergehende Benachrichtigungspflicht „in besonderen Fällen“ vor, um die Ausübung der Rechte der betroffenen Person zu ermöglichen. Im Einklang mit den Anforderungen des Urteils des Bundesverfassungsgerichts vom 20. April 2016 betrifft dies insbesondere Fälle, in denen die betroffene Person aufgrund verdeckter Maßnahmen gar nicht weiß, dass ihre Daten erhoben und verarbeitet werden, sie sich also mangels Kenntnis der Datenverarbeitung nicht dagegen zur Wehr setzen kann beziehungsweise die Aufsichtsbehörde nicht mit einer Überprüfung beauftragen kann. Verdeckte Maßnahmen sind vielfach eingriffsintensive Maßnahmen, die den Kernbereich privater Lebensgestaltung tangieren können. In diesen Fällen ist es grundsätzlich angezeigt, die betroffene Person zu gegebener Zeit über die erfolgte Datenverarbeitung in Kenntnis zu setzen, um ihr wenigstens nachträglich die Ausübung ihrer Rechte zu ermöglichen. Allerdings kann es auch nach Abschluss der Maßnahmen Konstellationen geben, in denen durch die Benachrichtigung der betroffenen Person der Zweck der Maßnahme oder die Durchführung eines staatsanwaltlichen Ermittlungsverfahrens gefährdet würde oder sonstige Gründe einer Benachrichtigung zumindest teilweise oder zeitweise entgegenstehen.

Zu Absatz 1

In Absatz 1 werden die betroffenen Personen festgelegt, die nach Durchführung der jeweiligen verdeckten Maßnahme zu benachrichtigen sind.

Zu Absatz 2

Absatz 2 legt den Mindestinhalt der Benachrichtigung fest.

Zu Absatz 3

Absatz 3 bestimmt den Zeitpunkt der Benachrichtigung sowie die Voraussetzungen, unter denen eine Benachrichtigung zurückgestellt werden bzw. ganz unterbleiben kann.

Zu Absatz 4

Absatz 4 weist auf die erforderliche Zustimmung des Landesamts für Verfassungsschutz für den Fall hin, dass sich die Benachrichtigung auf eine Übermittlung personenbezogener Daten dorthin bezieht. In diesen Fällen kann es nicht allein in der Entscheidungshoheit der Polizei liegen, ob Gründe vorliegen, die gegen eine Benachrichtigung sprechen.

60. Zu § 87 (Benachrichtigung bei der Verletzung des Schutzes personenbezogener Daten)

Die Vorschrift dient der Umsetzung des Artikels 31 der Richtlinie (EU) 2016/680. Sie bestimmt, dass betroffene Personen unverzüglich zu benachrichtigen sind, wenn eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für ihre Rechtsgüter zur Folge hat.

Ein hohes Risiko für die Rechtsgüter betroffener Personen wird im Regelfall dann vorliegen, wenn Daten aus dem Einwirkungsbereich der Polizei nach außen gelangt sind, so dass die Polizei die Verfügungsgewalt darüber verloren hat. Fälle, in denen personenbezogene Daten innerhalb der Polizei zwar rechtswidrig verarbeitet wurden, aber nicht nach außen gelangt sind, dürften hingegen im Regelfall kein hohes Risiko für die Rechtsgüter der betroffenen Personen darstellen.

Die Benachrichtigung kann entfallen, wenn die Polizei entweder vorab geeignete Maßnahmen getroffen hat, um eine Verletzung zu vermeiden oder sie durch entsprechende nachfolgende Maßnahmen die Auswirkungen der Verletzung so minimiert hat, dass aller Wahrscheinlichkeit nach kein hohes Risiko für die Rechtsgüter betroffener Personen mehr besteht. Geeignete Vorabmaßnahmen können insbesondere Verschlüsselungen sein, durch die die Daten für unbefugte Personen unzugänglich gemacht werden. Wäre die Benachrichtigung einzelner betroffener Personen mit einem unverhältnismäßigen Aufwand verbunden, kann die Benachrichtigung zwar nicht entfallen, jedoch durch eine öffentliche Bekanntmachung oder eine vergleichbare Maßnahme ersetzt werden.

61. Zu § 88 (Meldung bei der Verletzung des Schutzes personenbezogener Daten)

Die Vorschrift dient der Umsetzung des Artikels 30 der Richtlinie (EU) 2016/680. Sie bestimmt, dass die Aufsichtsbehörde für den Datenschutz unverzüglich zu benachrichtigen ist, wenn eine Verletzung des Schutzes personenbezogener Daten voraussichtlich eine Gefahr für die Rechtsgüter betroffener Personen zur Folge hat.

Die Meldepflicht tritt bereits bei einer voraussichtlichen einfachen Gefahr für die Rechtsgüter betroffener Personen ein, während die Pflicht zur Benachrichtigung der betroffenen Personen erst bei einer voraussichtlichen erheblichen Gefahr ausgelöst wird. Dies entspricht den Vorgaben der Richtlinie (EU) 2016/680. Denn in Artikel 30 Absatz 1 der Richtlinie (EU) 2016/680 wird für die Meldepflicht ein voraussichtliches „Risiko für die Rechte und Freiheiten natürlicher Personen“, in Artikel 31 Absatz 1 der Richtlinie (EU) 2016/680 für die Benachrichtigungspflicht hingegen ein voraussichtliches „hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ gefordert. Grundsätzlich entsteht die Meldepflicht damit unter geringeren Voraussetzungen als die Benachrichtigungspflicht. Allerdings setzt auch die Meldepflicht durch die Beschränkung auf Verletzungen, die voraussichtlich eine Gefahr für die Rechtsgüter betroffener Personen zur Folge haben, noch eine gewisse Erheblichkeit voraus. Auch ihr Anwendungsbereich sollte daher regelmäßig auf solche Vorfälle beschränkt sein, bei denen Daten nach außen gelangt sind, so dass die Polizei die Verfügungsgewalt über sie verloren hat.

62. Zu § 89 (Zusammenarbeit mit der Aufsichtsbehörde für den Datenschutz)
Die Vorschrift dient der Umsetzung der Artikel 26 und 28 der Richtlinie (EU) 2016/680. Sie bestimmt die Pflichten der Polizei zur Zusammenarbeit mit der Aufsichtsbehörde für den Datenschutz.

Zu Absatz 1
Absatz 1 normiert die allgemeine Pflicht der Polizei zur Zusammenarbeit mit der Aufsichtsbehörde für den Datenschutz bei der Erfüllung ihrer aufsichtlichen Aufgaben, die in weiteren Vorschriften konkretisiert werden.

Zu Absatz 2

Die sich aus Absatz 2 ergebende Anhörungspflicht im Rahmen der Ausarbeitung von Rechts- und Verwaltungsvorschriften, die die Verarbeitung personenbezogener Daten durch die Polizei betreffen, ist durch das zuständige Ministerium, im Regelfall also durch das Innenministerium, zu erfüllen. Sie ergab sich bislang aus § 31 Absatz 4 Satz 2 LDSG a.F..

Zu Absatz 3
Absatz 3 enthält die Pflicht zur Vorlage der nach § 80 vorzunehmenden Datenschutz-Folgenabschätzung.

Zu Absatz 4
Aus Absatz 4 ergibt sich die Pflicht zur Anhörung der Aufsichtsbehörde für den Datenschutz, bevor neue Dateisysteme in Betrieb genommen werden, wenn diese ein hohes Risiko für die Rechtsgüter der betroffenen Personen zur Folge haben können.

63. Zu § 90 (Berichtspflicht gegenüber dem Landtag)
Das Bundesverfassungsgericht hat in seinem Urteil vom 20. April 2016 (Rn. 142 f.) entschieden, dass es zur Gewährleistung von Transparenz und Kontrolle einer gesetzlichen Regelung von Berichtspflichten für einige eingriffsintensive verdeckte Maßnahmen bedarf. Es hat hierzu festgestellt: „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.>)“.

Auch hinsichtlich der Übermittlung von Daten im internationalen Bereich hat das Bundesverfassungsgericht die Anordnung einer hinreichenden Berichtspflicht zur Übermittlungspraxis gefordert (Rn. 354).

Diesen Anforderungen entsprechend bündelt die Vorschrift bereits bestehende Berichtspflichten und legt hinsichtlich weiterer eingriffsintensiver verdeckter Befugnisse erstmals Berichtspflichten fest. Neu festgelegt wird die Berichtspflicht für die besonderen Mittel der Datenerhebung nach § 49, für den Einsatz des IMSI-Catchers nach § 55 Absatz 1 und für die Datenübermittlung im internationalen Bereich nach § 61.

In welchem zeitlichen Abstand die Berichtspflicht zu erfüllen ist, hat das Bundesverfassungsgericht offen gelassen und lediglich „regelmäßige Berichte“ gefordert. Die Festlegung einer einheitlichen zweijährigen Berichtspflicht erfolgt in Anlehnung an die zweijährige Kontrolle durch die Aufsichtsbehörde für den Datenschutz und gewährleistet ein hohes Maß an Transparenz, ebenso wie die Pflicht, das Ergebnis öffentlich zugänglich zu machen.

64. Zu § 91 (Auskunftsrecht)
Die Vorschrift dient der Umsetzung der Artikel 14 und 15 sowie in Teilen des Artikels 12 der Richtlinie (EU) 2016/680. Sie regelt das Auskunftsrecht der betroffenen Person über die zu ihrer Person gespeicherten Daten, welches sich bislang aus § 45 PolG a.F. in Verbindung mit § 21 LDSG a.F. ergab.

Zu Absatz 1
Absatz 1 bestimmt das Recht jeder Person, auf Antrag Auskunft darüber zu erhalten, ob sie betreffende personenbezogene Daten durch die Polizei verarbeitet werden. Ferner enthält Absatz 1 in Umsetzung von Artikel 14 der Richtlinie (EU) 2016/680 die Angaben, über die der betroffenen Person im Fall einer Verarbeitung Auskunft zu erteilen ist.

In Umsetzung der Anforderung des Artikels 14 Buchstabe g) der Richtlinie (EU) 2016/680 bestimmt Satz 2 Nummer 2, dass grundsätzlich ein Recht auf Auskunft über die verfügbaren Informationen hinsichtlich der Herkunft der Daten besteht. Die Altregelung des § 45 Halbsatz 2 PolG a.F. sah abweichend hiervon keine dementsprechende Auskunftspflicht vor. In der Begründung zu § 31 h des Entwurfs zur Änderung des Polizeigesetzes Baden-Württemberg vom 07.05.1991 (Drucksache

10/5230) heißt es zur Einschränkung des schon damals grundsätzlich umfassend bestehenden Auskunftsanspruchs: „Ein Auskunftsanspruch über die Herkunft von Daten würde zu einer Beeinträchtigung der Aussage- und Hinweisbereitschaft gegenüber der Polizei führen, wodurch die polizeiliche Arbeit erheblich beeinträchtigt werden könnte. Hinter dem öffentlichen Interesse an der Gewinnung polizeilicher Erkenntnisse hat das private Interesse an der Kenntnis der Herkunft von Daten regelmäßig zurückzustehen“. In Erwägungsgrund 43 der Richtlinie (EU) 2016/680 heißt es: „Enthalten solche Mitteilungen Informationen über den Ursprung der personenbezogenen Daten, so sollten die Informationen nicht die Identität natürlicher Personen und insbesondere keine vertraulichen Quellen preisgeben“. Daraus ist zu schließen, dass sich auch die Verfasser der Richtlinie (EU) 2016/680 mit dieser Thematik beschäftigt haben und die Preisgabe der Herkunft der Daten nicht uneingeschränkt festlegen wollten. Mit der Aufnahme des Zusatzes „soweit diese nicht die Identität natürlicher Personen, insbesondere vertraulicher Quellen, preisgeben“ wird damit richtlinienkonform eine zweckwahrende Einschränkung vorgenommen.

Zu Absatz 2

Absatz 2 Satz 1 erfolgt in Umsetzung von Artikel 12 Absatz 3 der Richtlinie (EU) 2016/680. Satz 2 dient der Umsetzung von Artikel 12 Absatz 5 der Richtlinie (EU) 2016/680 und soll sicherstellen, dass tatsächlich nur die betroffene Person Auskunft erhält. Begründete Zweifel an der Identität der antragstellenden Person können zum Beispiel vorliegen, wenn die angegebene Adresse eines schriftlichen Antrags nicht mit der in den polizeilichen Dateien gespeicherten Adresse übereinstimmt. Ebenso können Zweifel entstehen, wenn eine unbekannte Person persönlich auf der Dienststelle erscheint und Auskunft verlangt. Hier kann die Vorlage des Personalausweises bestätigen, dass die erschienene Person tatsächlich die Person ist, zu der Auskunft verlangt wird.

Zu Absatz 3

Absatz 3 erfolgt in Umsetzung von Artikel 12 Absatz 4 der Richtlinie (EU) 2016/680. Die Unentgeltlichkeit der Auskunftserteilung ergab sich bislang aus § 21 Absatz 1 LDSG a.F..

Gemäß Erwägungsgrund 43 der Richtlinie (EU) 2016/680 soll das Auskunftsrecht „in angemessenen Abständen“ bestehen. Dieser Formulierung ist nicht zu entnehmen, ab wann von einem exzessiven, also einem auf Grund der Häufigkeit missbräuchlichen, Antrag auszugehen ist. Wenn einem Auskunftsinteresse der betroffenen Person zeitnah und hinreichend umfassend nachgekommen wurde, keine Anhaltspunkte dafür vorliegen, dass sich seit der letzten Auskunftserteilung wesentliche Änderungen ergeben haben und die betroffene Person kein schützenswertes Interesse an einer weiteren Auskunftserteilung vorgebracht hat, muss die erneute Auskunft verweigert werden können. Die Polizei hat im Zweifel den Nachweis zu erbringen, dass es sich um einen offenkundig missbräuchlichen oder exzessiven Antrag handelt.

Zu Absatz 4

Absatz 4 setzt Artikel 15 Absatz 1 der Richtlinie (EU) 2016/680 um, der die Möglichkeiten zur teilweisen oder vollständigen Einschränkung des Auskunftsrechts an bestimmte Zwecke bindet, die konkrete Ausgestaltung jedoch offen lässt. Die gewählten Einschränkungs- und Verweigerungsgründe sind § 21 Absatz 5 LDSG a.F. entnommen.

Zu Absatz 5

Absatz 5 übernimmt die Regelung des § 21 Absatz 4 LDSG a.F. und bestimmt, dass in Fällen, in denen sich die Auskunftserteilung auf die Übermittlung von Daten an andere Behörden bezieht, die Zustimmung der betroffenen Behörde einzuholen ist.

Zu Absatz 6

Mit Absatz 6 wird Artikel 15 Absätze 3 und 4 der Richtlinie (EU) 2016/680 umgesetzt. Er enthält Regelungen zum Verfahren im Fall der Einschränkung oder Verweigerung einer Auskunft.

Zu Absatz 7

Absatz 7 ist rein deklaratorischer Natur und stellt klar, dass Rechtsvorschriften über die Akteneinsicht im Verwaltungsverfahren unberührt bleiben.

Zu Absatz 8

Absatz 8 enthält eine Verordnungsermächtigung zugunsten des Innenministeriums, um die Zuständigkeit zur Auskunftserteilung abweichend regeln zu können.

Zu Absatz 9

Absatz 9 verweist auf zwei Vorschriften des Bundeskriminalamtgesetzes, die Besonderheiten der Betroffenenrechte bezüglich solcher Daten regeln, die im polizeilichen Informationsverbund mit dem Bundeskriminalamt gespeichert sind.

65. Zu § 92 (Recht auf Berichtigung, Löschung sowie Einschränkung der Verarbeitung)

Die Vorschrift dient der Umsetzung des Artikels 16 der Richtlinie (EU) 2016/680 in seiner Ausformung als Recht der betroffenen Person. Systematisch werden hier die Rechte der betroffenen Person auf Berichtigung und Löschung der sie betreffenden personenbezogenen Daten sowie auf Einschränkung ihrer Verarbeitung normiert, die spiegelbildlich zu den Pflichten der Polizei zur Berichtigung, Löschung sowie Einschränkung der Verarbeitung bestehen, die in § 75 geregelt sind.

Zu Absatz 1

Absatz 1 enthält das Recht auf Berichtigung unrichtiger Daten sowie das Recht auf Vervollständigung unvollständiger Daten. In Satz 2 wird klargestellt, dass der Inhalt einer Zeugenaussage vom Recht auf Berichtigung unberührt bleibt. Hintergrund hierfür ist, dass Zeugenaussagen oft nicht auf Tatsachen, sondern auf persönlichen Einschätzungen beruhen, die einem Richtigkeitsbeweis nicht zugänglich sind. Die Frage der Richtigkeit der Daten betrifft im Fall von Zeugenaussagen deshalb nicht den Inhalt der Aussage, sondern allein die Tatsache, dass die Aussage so erfolgt ist.

Zu Absatz 2

Absatz 2 enthält das Recht auf Löschung personenbezogener Daten. Es ist an die gleichen Voraussetzungen geknüpft wie die eigenständige Pflicht der Polizei zur Löschung ohne Ersuchen der betroffenen Person.

Zu Absatz 3

Absatz 3 verweist hinsichtlich der Einschränkung der Verarbeitung und der Mitteilung an Empfänger auf die Parallelvorschrift zur Pflicht der Polizei sowie hinsichtlich der Verfahrensregelungen auf die Vorschrift zum Auskunftsrecht.

Zu Absatz 4
Absatz 4 legt in Umsetzung von Artikel 16 Absatz 4 der Richtlinie (EU) 2016/680 fest, dass die betroffene Person unter Angabe der Gründe schriftlich zu unterrichten ist, wenn von der ersuchten Berichtigung, Löschung oder Einschränkung der Verarbeitung abgesehen wird. Unter Verweis auf die entsprechenden Bestimmungen der Vorschrift zum Auskunftsrecht bestimmt Satz 4, inwiefern diese Unterrichtung verweigert oder eingeschränkt werden kann.

Zu Absatz 5
Absatz 5 verweist auf zwei Vorschriften des Bundeskriminalamtgesetzes, die Besonderheiten der Betroffenenrechte bezüglich solcher Daten regeln, die im polizeilichen Informationsverbund mit dem Bundeskriminalamt gespeichert sind.

66. Zu § 93 (Anrufung der Aufsichtsbehörde für den Datenschutz)
Die Vorschrift dient der Umsetzung sowohl des Artikels 52 als auch des Artikels 17 der Richtlinie (EU) 2016/680. Sie regelt das Recht der betroffenen Person zur Anrufung der Aufsichtsbehörde für den Datenschutz. Dieses Recht wird in zwei unterschiedlichen Ausformungen gewährt, im Beschwerderecht nach Absatz 1 und im Recht auf Ausübung der Betroffenenrechte durch die Aufsichtsbehörde nach Absatz 2. Der Unterschied besteht darin, dass im Rahmen einer Beschwerde nach Absatz 1 die Rechtmäßigkeit einer polizeilichen Datenverarbeitung überprüft wird, wohingegen sich die Überprüfung nach Absatz 2 auf die Rechtmäßigkeit einer bestimmten Entscheidung der Polizei bezieht, das Recht der betroffenen Person auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung ihrer Daten zu verweigern oder einzuschränken.

Die Pflicht der Aufsichtsbehörde für den Datenschutz, die betroffene Person in angemessener Frist über das Ergebnis der Überprüfung zu unterrichten, folgt aus Artikel 46 Absatz 1 Buchstaben f) und g) der Richtlinie (EU) 2016/680, der die Aufgaben der Aufsichtsbehörde für den Datenschutz konkretisiert.

Zu Absatz 1

Absatz 1 setzt Artikel 52 der Richtlinie (EU) 2016/680 um und normiert das Recht der betroffenen Person, bei der Aufsichtsbehörde für den Datenschutz Beschwerde einzulegen, wenn sie der Auffassung ist, dass die Verarbeitung ihrer personenbezogenen Daten durch die Polizei gegen dieses Gesetz verstößt.

Es handelt sich dabei nicht um eine förmliche Art der Beschwerde, wie sie im Prozessrecht ausgestaltet ist, sondern um eine formlose Art der Beschwerde ähnlich der Fachaufsichtsbeschwerde. Die betroffene Person muss daher nicht durch eine Ausgangsentscheidung beschwert sein.

Das Beschwerderecht besteht unbeschadet anderweitiger Rechtsbehelfe, insbesondere unbeschadet der Rechtsbehelfe, mit denen die betroffene Person unmittelbar gegen die Polizei vorgehen kann. Gegen die Entscheidung der Aufsichtsbehörde für den Datenschutz über die Beschwerde kann die betroffene Person ebenfalls einen Rechtsbehelf einlegen, worauf sie von der Aufsichtsbehörde hinzuweisen ist.

Zu Absatz 2

Absatz 2 setzt Artikel 17 der Richtlinie (EU) 2016/680 um und normiert das Recht der betroffenen Person, eine Entscheidung der Polizei über die Verweigerung oder Einschränkung einer Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung von Daten durch die Aufsichtsbehörde für den Datenschutz überprüfen zu lassen.

Der Wortlaut des Artikels 17 Absatz 1 der Richtlinie (EU) 2016/680 sieht vor, dass „die Rechte der betroffenen Person auch über die zuständige Aufsichtsbehörde ausgeübt werden können“. Allerdings darf auch die mittelbare Ausübung der Rechte nicht dazu führen, dass die betroffene Person durch die Aufsichtsbehörde für den Datenschutz die begehrte Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung von Daten erhält, wenn dieser nach wie vor sachliche oder rechtliche Gründe entgegenstehen. Vielmehr muss die Aufsichtsbehörde anhand der von der Polizei darzulegenden Gründe überprüfen, ob die Entscheidung zur Verweigerung oder Einschränkung der Auskunft, Berichtigung, Löschung oder Einschränkung der

Verarbeitung von Daten rechtmäßig war und der betroffenen Person und der Polizei im Anschluss das Überprüfungsergebnis mitteilen. In Erwägungsgrund 48 der Richtlinie (EU) 2016/680 heißt es entsprechend: „sollte die betroffene Person die nationale Aufsichtsbehörde ersuchen können, die Rechtmäßigkeit der Verarbeitung zu überprüfen“. Wird festgestellt, dass die Entscheidung unrechtmäßig ergangen ist, hat die Polizei die Gelegenheit zur Abhilfe, andernfalls kann die betroffene Person einen Rechtsbehelf einlegen. Wird festgestellt, dass die Entscheidung rechtmäßig ergangen ist, hat die betroffene Person lediglich Anspruch auf Mitteilung dieses Ergebnisses, nicht aber auf die begehrte Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, und auch nicht auf die Mitteilung der die Entscheidung tragenden Gründe, wenn diese Auskunft dem Zweck der Verweigerung oder Einschränkung entgegensteht. Die diesbezügliche Formulierung, dass die Mitteilung keine Rückschlüsse auf den Erkenntnisstand der Polizei zulassen darf, sofern diese keiner weitergehenden Auskunft zustimmt, war nahezu wortgleich in § 27 Absatz 2 LDSG a.F. enthalten.

Die Aufsichtsbehörde für den Datenschutz hat die betroffene Person auf die Möglichkeit zur Einlegung eines Rechtsbehelfs hinzuweisen. Aus Gründen des Rechtsschutzbedürfnisses ist dieser Rechtsbehelf gegen die Entscheidung der Polizei zur Verweigerung oder Einschränkung der Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung von Daten zu richten.

67. Zu § 94 (Benennung eines Datenschutzbeauftragten)
Die Vorschrift dient der Umsetzung des Artikels 32 der Richtlinie (EU) 2016/680. Sie enthält Regelungen zur Benennung eines Datenschutzbeauftragten.

Die zur Benennung eines Datenschutzbeauftragten verpflichtete Stelle wird in Absatz 1 konkretisiert. Die Organisation der Polizei umfasst die Polizeibehörden und den Polizeivollzugsdienst, der seinerseits in Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst aufgeteilt ist. Grundsätzlich hat jede dieser Stellen einen Datenschutzbeauftragten zu benennen, wobei mehrere zuständige Stellen auch einen gemeinsamen Datenschutzbeauftragten benennen können. Im Einklang mit Artikel 32 Absatz 3 der Richtlinie (EU) 2016/680 ist der Organisationsstruktur und Größe der zuständigen Stellen Rechnung zu tragen.

68. Zu § 95 (Stellung des Datenschutzbeauftragten)
Die Vorschrift regelt die Stellung des Datenschutzbeauftragten. Absatz 1 übernimmt Regelungen des § 10 Absätze 2 und 3 LDSG a.F.. Die Absätze 2 und 3 dienen der Umsetzung des Artikels 33 der Richtlinie (EU) 2016/680.

69. Zu § 96 (Aufgaben des Datenschutzbeauftragten)
Die Vorschrift dient der Umsetzung des Artikels 34 der Richtlinie (EU) 2016/680. Sie bestimmt die Aufgaben, die dem Datenschutzbeauftragten obliegen.

Zu Absatz 1
Zusätzlich zu den sich aus der Richtlinie (EU) 2016/680 ergebenden Aufgaben greift Absatz 1 in Nummer 1 (Unterstützung der zuständigen Stelle), Nummer 4 (Hinwirken auf die Einhaltung der Datenschutzvorschriften bei der Planung, Einführung und Anwendung von Verfahren, mit denen personenbezogene Daten automatisiert verarbeitet werden) und Nummer 5 (Beratung beim Führen des Verzeichnisses von Verarbeitungstätigkeiten) Elemente aus § 10 LDSG a.F. auf.

Zu Absatz 2
Absatz 2 stellt klar, dass dem Datenschutzbeauftragten außerhalb des Anwendungsbereichs dieses Gesetzes die in der Verordnung (EU) 2016/679 und im Landesdatenschutzgesetz genannten Aufgaben obliegen.

70. Zu § 97 (Aufsichtsbehörde für den Datenschutz)
Mit der Vorschrift wird von der durch Artikel 41 Absatz 3 der Richtlinie (EU) 2016/680 eingeräumten Möglichkeit Gebrauch gemacht, die gemäß der Verordnung (EU) 2016/679 errichtete und im Landesdatenschutzgesetz bestimmte Aufsichtsbehörde zugleich als Aufsichtsbehörde für den Datenschutz im Anwendungsbereich dieses Gesetzes festzulegen. Dafür wird auf die Bestimmungen des Landesdatenschutzgesetzes verwiesen, die die Errichtung, die Organisation sowie die grundsätzlichen Rechte und Pflichten der gemeinsamen Aufsichtsbehörde näher festlegen.

71. Zu § 98 (Aufgaben der Aufsichtsbehörde für den Datenschutz)

Die Vorschrift dient insbesondere der Umsetzung des Artikels 46 der Richtlinie (EU) 2016/680. Sie legt fest, welche Aufgaben der Aufsichtsbehörde für den Datenschutz im Anwendungsbereich des Polizeigesetzes zukommen.

Zu Absatz 1
Absatz 1 enthält eine Auflistung der konkreten Aufgaben.

Die in Nummer 1 enthaltene Aufgabe, die Anwendung der datenschutzrechtlichen Regelungen durchzusetzen, erfolgt anhand der in § 99 Absatz 1 Nummern 4 und 5 genannten Befugnisse.

Nummer 6 setzt die Artikel 17 und 52 der Richtlinie (EU) 2016/680 in ihrer Ausgestaltung als Pflicht der Aufsichtsbehörde um, sich mit dem jeweiligen Ersuchen der betroffenen Person zu befassen. Die weiteren sich aus Artikel 46 Absatz 1 Buchstaben f) und g) der Richtlinie (EU) 2016/680 ergebenden diesbezüglichen Pflichten der Aufsichtsbehörde sind in § 93 enthalten.

Mit Nummer 12 wird Artikel 48 der Richtlinie (EU) 2016/680 umgesetzt.

Mit Nummer 13 wird Artikel 49 der Richtlinie (EU) 2016/680 umgesetzt. Künftig hat die Aufsichtsbehörde für den Datenschutz jährlich einen Tätigkeitsbericht vorzulegen.

Mit Nummer 14 wird der im Urteil des Bundesverfassungsgerichts vom 20. April 2016 aufgestellten Anforderung an die Gewährleistung einer wirksamen aufsichtlichen Kontrolle bezüglich heimlicher Überwachungsmaßnahmen Rechnung getragen (Rn. 140 f.). Nach den Ausführungen des Bundesverfassungsgerichts kommt der regelmäßigen Durchführung einer aufsichtlichen Kontrolle angesichts deren Kompensationsfunktion für den schwach ausgestalteten Individualrechtsschutz in diesem Zusammenhang eine besondere Bedeutung zu. Solche Kontrollen sind in angemessenen Abständen, deren Dauer ein gewisses Höchstmaß von etwa zwei Jahren nicht überschreiten darf, durchzuführen (Rn. 141). Um Wiederholungen bei den einzelnen Befugnisnormen zu vermeiden, wird diese Aufgabe der Aufsichtsbehörde für den Datenschutz hier einheitlich geregelt.

Zu Absatz 2

Absatz 2 sieht vor, dass die Aufsichtsbehörde für den Datenschutz durch die Bereitstellung entsprechender Formulare das Einreichen von Beschwerden erleichtern soll.

Zu Absatz 3

Absatz 3 bestimmt, dass die Aufsichtsbehörde für den Datenschutz ihre Aufgaben unentgeltlich zu erfüllen hat. Ferner wird der Aufsichtsbehörde die Möglichkeit eingeräumt, die Bearbeitung einer Anfrage abzulehnen, wenn diese offenkundig missbräuchlich oder exzessiv gestellt ist. Dies entspricht den Voraussetzungen, unter denen die Polizei einen Antrag auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung von Daten ablehnen kann.

Zu Absatz 4

Absatz 4 stellt klar, dass der Aufsichtsbehörde für den Datenschutz außerhalb des Anwendungsbereichs dieses Gesetzes die in der Verordnung (EU) 2016/679 und im Landesdatenschutzgesetz genannten Aufgaben obliegen.

72. Zu § 99 (Befugnisse der Aufsichtsbehörde für den Datenschutz)

Die Vorschrift dient der Umsetzung des Artikels 47 der Richtlinie (EU) 2016/680. Sie legt fest, welche Befugnisse der Aufsichtsbehörde für den Datenschutz im Anwendungsbereich des Polizeigesetzes zustehen.

Nach Artikel 47 Absätze 1 bis 3 der Richtlinie (EU) 2016/680 sind der Aufsichtsbehörde für den Datenschutz wirksame Untersuchungs-, Abhilfe- und Beratungsbefugnisse einzuräumen. Aus Erwägungsgrund 82 der Richtlinie (EU) 2016/680 geht ausdrücklich hervor, dass bei der Ausübung der Befugnisse der Grundsatz der Verhältnismäßigkeit zu wahren ist. Danach sollte jede Maßnahme im Hinblick auf die Gewährleistung der Einhaltung der Richtlinie geeignet, erforderlich und verhältnismäßig sein, wobei die Umstände des jeweiligen Einzelfalls zu berücksichtigen sind. Dementsprechend hat die Aufsichtsbehörde als mildestes Mittel stets jene Befugnis zu wählen, die die geringste Intensität aufweist, solange diese zur Zielerreichung, der Einhaltung der Vorschriften dieses Gesetzes, geeignet ist.

Zu Absatz 1

Absatz 1 enthält eine Auflistung der konkreten Befugnisse.

In Nummer 1 werden wirksame Untersuchungsbefugnisse eingeräumt, indem der Aufsichtsbehörde Zugang zu allen personenbezogenen Daten gewährt wird, die einer Verarbeitung unterliegen, sowie Zugang zu allen Informationen, die sie zur Aufgabenerfüllung benötigt. Dabei stellt die Durchführung von Untersuchungen und die damit verbundene Prüfungstätigkeit regelmäßig die am wenigsten einschneidende Maßnahme dar.

In den Nummern 2 und 3 werden unter Bezugnahme auf die Pflicht der Polizei zur Zusammenarbeit mit der Aufsichtsbehörde wirksame Beratungsbefugnisse eingeräumt, die regelmäßig von höherer Intensität sein dürften als die in Nummer 1 geregelten Untersuchungsbefugnisse.

In den Nummern 4 und 5 werden wirksame Abhilfebefugnisse geschaffen, die sich an den Beispielen des Artikels 47 Absatz 2 der Richtlinie (EU) 2016/680 orientieren. Die Abhilfebefugnisse sind gegenüber den Untersuchungs- und Beratungsbefugnissen als schärferes Mittel anzusehen, da sie auf ein bestimmtes Ziel, nämlich die Abwendung eines konkreten datenschutzrechtlichen Verstoßes, gerichtet sind. Auch innerhalb der Abhilfebefugnisse hat die Aufsichtsbehörde zur Wahrung des Verhältnismäßigkeitsgrundsatzes zu differenzieren.

Nummer 4 bestimmt, dass die Aufsichtsbehörde die Polizei vor einem möglicherweise drohenden Verstoß gegen datenschutzrechtliche Bestimmungen warnen kann.

Nach Nummer 5 kann die Aufsichtsbehörde die Polizei auffordern, Verarbeitungsvorgänge mit diesem Gesetz in Einklang zu bringen. Die Aufforderung kann mit einer Frist und einer bestimmten Weise der Abhilfe verbunden werden, insbesondere der Berichtigung oder Löschung personenbezogener Daten oder der vorübergehenden oder endgültigen Einschränkung ihrer Verarbeitung. Die Aufsichtsbehörde kann damit von der Polizei konkrete Maßnahmen fordern, die ihr erforderlich erscheinen, um einen Verstoß gegen datenschutzrechtliche Bestimmungen zu verhindern oder abzu-

stellen. Dies entspricht einer konkretisierten Rügebefugnis, die nicht allein problembezogen, sondern zugleich lösungsorientiert ist und der Polizei die Gelegenheit zur Abhilfe gibt.

In Umsetzung von Artikel 47 Absatz 5 der Richtlinie (EU) 2016/680 bestimmt Satz 2, dass der Aufsichtsbehörde für Verstöße gegen dieses Gesetz der Verwaltungsrechtsweg offen steht.

Zu Absatz 2
Absatz 2 stellt klar, dass der Aufsichtsbehörde für den Datenschutz außerhalb des Anwendungsbereichs dieses Gesetzes die in der Verordnung (EU) 2016/679 und im Landesdatenschutzgesetz genannten Befugnisse zustehen.

73. Zu §§ 100 bis 102 (Voraussetzungen bis Ersatz)
Die Regelungen entsprechen den §§ 55 bis 57 des bisherigen PolG. Die Verweise werden aufgrund der neuen Nummerierung des Gesetzes angepasst.

74. Zu § 103 (Rechtsweg)
Satz 1 entspricht unter Anpassung der Verweise der Regelung des § 58 des bisherigen PolG. Mit dem neuen Satz 2 wird klargestellt, dass die Bestimmungen des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit für Ansprüche nach §§ 100 bis 102 keine Anwendung finden.

75. Zu § 104 (Allgemeines)
Die Regelung entspricht § 59 des bisherigen PolG.

76. Zu § 105 (Zuständigkeitsabgrenzung)
Die Regelung entspricht weitestgehend § 60 des bisherigen PolG. Allerdings wird die Aufzählung in Absatz 3 um § 29 und § 42 ergänzt. Damit wird geregelt, dass der Polizeivollzugsdienst neben den Polizeibehörden originär für die Durchführung von Gefährderansprachen / -anschreiben bzw. Gefährdetenansprachen und für die Verarbeitung personenbezogener Daten aufgrund einer Einwilligung zuständig ist. Bezüglich der Gefährderansprachen ist die Ergänzung eine Folge des Urteils des Verwaltungsgerichtshofs Baden-Württemberg vom 7. Dezember 2017 (Az. 1 S 2526/16),

nach welchem dem Polizeivollzugsdienst nach der bisherigen Rechtslage lediglich eine Eilfallkompetenz zukam. Im Übrigen werden die Verweise aufgrund der neuen Nummerierung des Gesetzes angepasst.

77. Zu §§ 106 bis 129 (Arten der Polizeibehörden bis Zurückbehaltungsbefugnis)
Die Regelungen entsprechen den §§ 61 bis 83a des bisherigen PolG. Die Verweise werden aufgrund der neuen Nummerierung des Gesetzes angepasst.

78. Zu § 130 (Durchführungsvorschriften)
Die Regelung entspricht weitgehend § 84 des bisherigen PolG. Die Verweise werden aufgrund der neuen Nummerierung des Gesetzes angepasst.

Zu Absatz 1 Nummer 1
Mit der Umsetzung der Vorgaben des Bundesverfassungsgerichts vom 20. April 2016 haben auch die bisher bestehenden Berechtigungen zur Übertragung von Antrags- oder Anordnungsbefugnissen hinsichtlich verdeckter Überwachungsmaßnahmen Änderungen erfahren. Daher wird die entsprechende Verordnungsermächtigung an die nunmehr bestehenden Delegationsbefugnisse im Polizeigesetz angepasst. Danach kann die Übertragung der Antragsbefugnis nach § 49 Absatz 4 Satz 4 und § 53 Absatz 2 Satz 3 sowie die Anordnungsbefugnis nach § 49 Absatz 4 Satz 6, § 53 Absatz 5 Satz 2 und Absatz 7 Satz 2, § 55 Absatz 1 Satz 3, § 56 Absatz 2 Satz 1 sowie § 69 Absatz 3 Satz 2 durch Rechtsverordnung näher geregelt werden.

Zu Absatz 1 Nummer 6
Die bisher in § 6 DVO PolG geregelte Anordnungsbefugnis für eine nach § 40 Absatz 4 PolG a.F. vorzunehmende Löschung von Daten bzw. Vernichtung von Unterlagen ist mit der Änderung des § 48 Absatz 4 Sätze 2 und 3 nunmehr unmittelbar im Polizeigesetz geregelt. Die bisherige Verordnungsermächtigung in Nummer 6 wird daher gestrichen.

Zu Absatz 1 Nummer 7

Da die polizeilichen Protokollierungspflichten im Zusammenhang mit der Verarbeitung personenbezogener Daten nach §§ 73 und 74 nunmehr vollumfänglich im Polizeigesetz geregelt sind, bedarf es keiner entsprechenden Verordnungsermächtigung mehr. Daher wird Nummer 7 ebenfalls gestrichen.

Zu Absatz 1 Nummern 8 und 9
Die bisherigen Nummern 8 und 9 werden zu den Nummern 6 und 7.

79. Zu § 131 (Schadenersatz - Datenverarbeitung)
Die Vorschrift dient der Umsetzung des Artikels 56 der Richtlinie (EU) 2016/680. Gleichzeitig schließt sie die durch den Wegfall der Geltung des § 25 LDSG a.F. entstandene Lücke. Sie regelt die Pflicht der Polizei zum Ersatz des Schadens, der durch eine rechtswidrige Verarbeitung personenbezogener Daten unter Verstoß gegen die Vorschriften dieses Gesetzes entstanden ist. Umfasst sind wie von der Altregelung des § 25 LDSG sowohl materielle als auch immaterielle Schäden.

Nach Erwägungsgrund 88 der Richtlinie (EU) 2016/680 sollten betroffene Personen einen vollständigen und wirksamen Schadenersatz für den durch eine rechtswidrige Verarbeitung personenbezogener Daten erlittenen Schaden erhalten. Darüber hinaus sollte der Schadensbegriff im Lichte der Rechtsprechung des Europäischen Gerichtshofs weit und auf eine Art und Weise ausgelegt werden, die den Zielen der Richtlinie (EU) 2016/680 in vollem Umfang entspricht, unbeschadet etwaiger weiterer Schadenersatzansprüche. Die bisherige Regelung des § 25 Absatz 3 LDSG a.F., wonach eine Höchstgrenze für die Zahlung eines entsprechenden Schadenersatzes in Höhe von 130.000 € festgesetzt war, genügt diesen Anforderungen, insbesondere nach einem vollständigen Schadenersatz, nicht mehr.

Der in Absatz 3 Satz 2 enthaltene Verweis auf § 86 BKAG betrifft eine Sonderregelung für den Schadenersatz im polizeilichen Informationsverbund, nach der das Bundeskriminalamt bei der Datenverarbeitung im polizeilichen Informationsverbund gegenüber einer betroffenen Person als allein Verantwortlicher gilt, der Schaden im Innenverhältnis jedoch auszugleichen ist, soweit er der datenschutzrechtlichen Verantwortung einer anderen Stelle zuzurechnen ist.

80. Zu § 132 (Gerichtliche Zuständigkeiten, Verfahren)

Mit der Umsetzung der Vorgaben des Bundesverfassungsgerichts vom 20. April 2016 sind zu den im Polizeigesetz bereits enthaltenen Richtervorbehalten noch weitere hinzugekommen. Damit stößt die bislang im Polizeigesetz geübte Technik, hinsichtlich der gerichtlichen Zuständigkeiten und der anwendbaren Verfahrensvorschriften innerhalb des Gesetzes zu verweisen, an die Grenzen der Verständlichkeit und Lesbarkeit des Gesetzestextes. Es empfiehlt sich daher, in Bezug auf die Bestimmungen über die gerichtlichen Zuständigkeiten und das gerichtliche Verfahren von der bislang geübten Verweisungstechnik abzurücken. An die Stelle der bisherigen Verweisungen tritt nun in § 132 eine zentrale Vorschrift, mit der grundsätzlich für sämtliche Richtervorbehalte im Polizeigesetz Regelungen über die gerichtlichen Zuständigkeiten und über das zu beachtende Verfahrensrecht getroffen werden. Die Regelungen in § 132 sind damit für sämtliche polizeigesetzliche Richtervorbehalte zentral „vor die Klammer gezogen“. Sie sind zu beachten, sofern der Gesetzgeber nicht unmittelbar im Zusammenhang mit dem jeweiligen Richtervorbehalt spezielle Regelungen zur gerichtlichen Zuständigkeit oder zum Verfahren getroffen hat. Diese gehen den allgemeinen Bestimmungen in § 132 vor.

Eine konkrete Umsetzung der Artikel 53 und 54 der Richtlinie (EU) 2016/680, die das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen die Aufsichtsbehörde für den Datenschutz und gegen den Verantwortlichen, also die Polizei, vorsehen, wird nicht für erforderlich erachtet. In beiden Fällen dürften die bestehenden Regelungen der Verwaltungsgerichtsordnung ausreichend sein, um entsprechende Rechtsbehelfe geltend zu machen. Eine Umsetzung von Artikel 55 der Richtlinie (EU) 2016/680, der das Recht der betroffenen Person vorsieht, sich durch eine bestimmte Einrichtung, Organisation oder Vereinigung vertreten zu lassen, müsste, sofern erforderlich, durch eine bundesgesetzliche Änderung der Verwaltungsgerichtsordnung erfolgen. Diesbezüglich trifft das Prozessrecht in § 67 Verwaltungsgerichtsordnung eine abschließende Regelung. Den Ländern verbleibt hier keine eigene Gesetzgebungskompetenz.

Zu Absatz 1

Absatz 1 regelt, dass für gerichtliche Entscheidungen aufgrund des Polizeigesetzes grundsätzlich das Amtsgericht zuständig ist, in dessen Bezirk die zuständige Polizeidienststelle ihren Sitz hat, soweit nichts anderes bestimmt ist. Davon abweichende Regelungen sind beispielsweise in § 31 Absatz 3 Satz 6, § 32 Absatz 5 Satz 6, § 33 Absatz 4 Satz 1, § 36 Absatz 5, § 38 Absatz 5 Satz 2, § 50 Absatz 2 Satz 1 sowie § 54 Absatz 4 Satz 4 vorgesehen.

Zu Absatz 2
Satz 1 verweist für gerichtliche Entscheidungen aufgrund des Polizeigesetzes grundsätzlich auf das Verfahrensrecht im Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG). Dieses kommt aufgrund des Verweises im vorliegenden Zusammenhang als Landesrecht zur Anwendung. Auch hier gilt allerdings, dass im unmittelbaren Zusammenhang mit den einzelnen Richtervorbehalten bestehende spezielle Verfahrensvorschriften der allgemeinen Bestimmung des § 132 vorgehen. Dies betrifft beispielsweise die speziellen Verfahrensvorschriften zum Gewahrsam (§ 33 Absatz 4).

Nach Satz 2 bedürfen gerichtliche Entscheidungen zu ihrer Wirksamkeit nicht der Bekanntmachung an den Betroffenen. Der in Satz 1 enthaltene Verweis auf das Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit wird hierdurch eingeschränkt (vgl. § 40 FamFG).

Die Sätze 3 und 4 stellen klar, dass gegen eine richterliche Entscheidung die Beschwerde gegeben ist (vgl. § 58 FamFG) und dass diese keine aufschiebende Wirkung entfaltet (vgl. § 64 Absatz 3 FamFG). Die sachliche Zuständigkeit für die Beschwerdeentscheidung liegt beim Oberlandesgericht, sofern sich aus speziellen Vorschriften des Polizeigesetzes nichts anderes ergibt (zu einem solchen Ausnahmefall vgl. § 33 Absatz 4 Satz 7). Nach Satz 5 ist die Rechtsbeschwerde nicht statthaft. Diese Vorschrift trägt dem Umstand Rechnung, dass in der Regel das Oberlandesgericht zur Entscheidung über die Beschwerde berufen ist und dass es um die Anwendung von Landesrecht geht.

Mit Satz 6 wird klarstellend geregelt, dass der Polizeivollzugsdienst im Rahmen der gerichtlichen Verfahren nicht verpflichtet ist, Urkunden oder Akten vorzulegen, elektronische Dokumente zu übermitteln oder Auskünfte zu erteilen, wenn das Bekanntwerden des Inhalts dieser Urkunden, Akten, elektronischen Dokumente oder Auskünfte dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder wenn die Vorgänge nach einem Gesetz oder ihrem Wesen nach geheim gehalten werden müssen. Dies gilt sowohl bei der originären Antragstellung, als auch im Rahmen eines etwaigen Beschwerdeverfahrens. Die Vorschrift ist angelehnt an vergleichbare Regelungen wie beispielsweise in §§ 5 Absatz 2, 29 Absatz 2 LVwVfG. Der in Satz 1 enthaltene Verweis auf das Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit wird diesbezüglich klarstellend konkretisiert, da dieses keine ausdrücklichen Regelungen hierzu enthält.

Zu Absatz 3

Mit Absatz 3 wird die im Verwaltungsrechtsweg zu erhebende Anfechtungsklage (§§ 40, 42 VwGO) ausgeschlossen, wenn eine richterliche Entscheidung nach dem Polizeigesetz ergangen ist. Damit wird zugleich die Fortsetzungsfeststellungsklage (§ 113 Absatz 1 Satz 4 VwGO <analog>) vor dem Verwaltungsgericht ausgeschlossen, wenn sich die Maßnahme nach Erlass einer richterlichen Entscheidung erledigt, die nach dem Polizeigesetz getroffen worden ist. Die Vorschrift greift damit die bislang für den Gewahrsam getroffene Regelung des § 28 Absatz 4 Satz 8 PolG a.F. auf und überträgt sie auf alle Maßnahmen, die nach dem Polizeigesetz einem Richtervorbehalt unterliegen.

81. Zu § 133 (Ordnungswidrigkeiten)

Die Regelung entspricht § 84a des bisherigen PolG. Die Verweise werden aufgrund der neuen Nummerierung des Gesetzes angepasst.

82. Zu § 134 (Strafvorschriften)

Zu Absatz 1

Absatz 1 entspricht § 84b des bisherigen PolG. Die Verweise werden aufgrund der neuen Nummerierung des Gesetzes angepasst.

Zu Absatz 2
Absatz 2 verweist hinsichtlich der Strafbarkeit von datenschutzrechtlichen Verstößen im Anwendungsbereich dieses Gesetzes auf die Regelung des § 29 LDSG.

83. Zu § 135 (Übergangsregelung - Datenverarbeitung)
Absatz 1 der Vorschrift bestimmt, dass die Übergangsregelung in § 72 Absatz 4 Satz 2 nur zeitlich befristet bis Ende des Jahres 2029 anwendbar bleibt und dann außer Kraft tritt.

Die in Bezug genommene Übergangsregelung legt fest, dass sowohl die Pflicht zur Kennzeichnung neu zu speichernder Daten einschließlich der Hinweispflicht im Fall einer Übermittlung als auch das Verbot zur Weiterverarbeitung und Übermittlung solcher Daten, die die Anforderungen an eine Kennzeichnung nicht erfüllen, keine Anwendung finden, solange eine Kennzeichnung technisch noch nicht möglich ist oder einen unverhältnismäßigen Aufwand erfordern würde.

Dadurch wird eine ressourcenaufwendige Nachkennzeichnung der Altdatenbestände vermieden und gleichzeitig die Möglichkeit der rechtssicheren weiteren Verarbeitung auch von Altdatenbeständen geschaffen, ohne die Funktionsfähigkeit der Polizei zu beeinträchtigen. Die Altdatenbestände unterliegen der regulären Aussonderungsprüfung und Löschung, so dass sich ihr Bestand und damit auch das Anwendungsfeld der Übergangsregelung sukzessive reduzieren wird bei gleichzeitigem Anwachsen des Datenbestandes, der die Anforderungen an eine Kennzeichnung vollumfänglich erfüllt. Die Übergangsregelung lässt die Möglichkeit unberührt, Altdaten durch eine nachträgliche Kennzeichnung entsprechend den Vorgaben vollständig in das neue Datenschutzregime zu überführen.

Da eine vollständige technische Umsetzung der Kennzeichnungsmöglichkeit in den polizeilichen Systemen nur sukzessive erfolgen kann und sich über einen längeren Zeitraum erstrecken wird, bezieht sich die Übergangsregelung auch auf künftig zu erhebende Datenbestände, bei denen im Zeitpunkt ihrer Speicherung eine Kennzeichnung aus technischen Gründen noch nicht möglich ist.

Die Befristung bis Ende 2029 erscheint notwendig und angemessen, um einerseits ausreichend Zeit zur Ertüchtigung der technischen Systeme zu belassen und andererseits sicherzustellen, dass die Kennzeichnungspflicht und das Weiterverarbeitungsverbot in absehbarer Zukunft vollumfänglich eingehalten werden.

Absatz 2 enthält in Umsetzung von Artikel 63 Absatz 2 der RL (EU) 2016/680 eine Übergangsregelung bis 6. Mai 2023 für solche automatisierten Verarbeitungssysteme, die vor dem 6. Mai 2016 eingerichtet wurden und die technisch die Anforderungen an die Protokollierungspflicht noch nicht erfüllen, so dass deren Einhaltung mit einem unverhältnismäßigen Aufwand verbunden wäre.

Die Übergangsbestimmungen des § 85 PolG a.F. gehen in den neuen Regelungen auf und sind daher nicht mehr erforderlich.

II. Zu Artikel 2

Mit Artikel 2 wird ein neuer § 13a in das AGGVG eingefügt. Hierdurch können Gerichtsvollzieherinnen und Gerichtsvollzieher in bestimmten Fällen zur Abschätzung der konkreten Gefährdungssituation bei einer beabsichtigten Vollstreckungsmaßnahme Informationen über die Schuldnerin oder den Schuldner bei der zuständigen Polizeidienststelle einholen. Dies dient der Vermeidung von Gefährdungssituationen sowie der Stärkung des Eigenschutzes der Gerichtsvollzieherinnen und Gerichtsvollzieher.

Der neue § 13a AGGVG steht dabei sowohl mit der Verordnung (EU) 2016/679 als auch mit dem nationalen Verfassungsrecht in Einklang.

Zu Absatz 1
Absatz 1 enthält für die dort näher geregelten Fälle eine Ermächtigungsgrundlage für die Übermittlung personenbezogener Daten seitens einer Gerichtsvollzieherin oder eines Gerichtsvollziehers an die zuständige Polizeidienststelle, damit diese anschließend einen Abgleich mit den Daten in ihrem Dateienbestand nach § 47 PolG vornehmen kann.

Zu Absatz 2
Nach Absatz 2 kann eine Gerichtsvollzieherin oder ein Gerichtsvollzieher in den im Absatz 1 Satz 1 geregelten Fällen bei der zuständigen Polizeidienststelle Daten über die Schuldnerin oder den Schuldner erheben und speichern, soweit dies zur Abschätzung der Gefährdungslage erforderlich ist. Die Ermächtigungsgrundlage ist notwendig, damit eine Gerichtsvollzieherin oder ein Gerichtsvollzieher das Ergebnis des seitens der zuständigen Polizeidienststelle durchgeführten Datenabgleichs gemäß § 47 PolG bei dieser erheben sowie hiernach speichern kann, solange die erlangten Informationen für die Abschätzung der Gefährdungslage erforderlich sind. Die korrespondierende Übermittlungsbefugnis der zuständigen Polizeidienststelle findet sich in § 59 Absatz 3 PolG.

III. Zu Artikel 3

1. Zu Artikel 3 Nummer 1

Es handelt sich um eine redaktionelle Folgeänderung zur neuen Nummerierung des Polizeigesetzes (Artikel 1).

2. Zu Artikel 3 Nummer 2

Es handelt sich um eine redaktionelle Änderung.

3. Zu Artikel 3 Nummer 3

Mit den angepassten Regelungen zur Übertragung der Antrags- und Anordnungsbefugnis wird vor allem den Änderungen des Polizeigesetzes Rechnung getragen.

Zu Absatz 1
Absatz 1 regelt, dass die Leitung eines regionalen Polizeipräsidiums die Antrags- bzw. Anordnungsbefugnisse nach § 49 Absatz 4 Sätze 4 und 6 und § 69 Absatz 3 Satz 2 PolG auf die Leitung des Führungs- und Einsatzstabes und die Leitung der Kriminalpolizeidirektion übertragen kann. Die Leitung des Polizeipräsidiums Einsatz kann die genannten Befugnisse auf die Leitung des Führungs- und Einsatzstabes

und die Leitung der Wasserschutzpolizeidirektion übertragen, die Leitung des Landeskriminalamtes auf Abteilungsleiter.

Zu Absatz 2
Absatz 2 regelt, dass die Leitung eines regionalen Polizeipräsidiums die Antrags- bzw. Anordnungsbefugnisse nach § 53 Absatz 2 Satz 3, Absatz 5 Satz 2, Absatz 7 Satz 2 sowie § 55 Absatz 1 Satz 3 PolG auf die Leitung des Führungs- und Einsatzstabes, die Leitung der Direktion Polizeireviere und die Leitung der Kriminalpolizeidirektion sowie im Fall des § 53 Absatz 7 Satz 2 PolG zusätzlich auf den Polizeiführer vom Dienst übertragen kann. In diesem Zusammenhang werden die bisherigen Delegationsbefugnisse maßvoll erweitert. Zum einen kann die Antrags- bzw. Anordnungsbefugnis künftig für sämtliche in §§ 53 und 55 PolG genannten Fälle auch auf die Leitung der Direktion Polizeireviere übertragen werden. Darüber hinaus kann die Anordnungsbefugnis nach § 53 Absatz 7 Satz 2 PolG künftig auch auf den Polizeiführer vom Dienst in den Führungs- und Lagezentren der Polizeipräsidien übertragen werden.

Die Leitung des Landeskriminalamts kann die genannten Antrags- bzw. Anordnungsbefugnisse auf Abteilungsleiter übertragen.

4. Zu Artikel 3 Nummer 4

Die bisherige Regelung des § 5 DVO PolG wird in einigen Punkten geändert.

Zu Absatz 1
Die bislang enthaltene Beschränkung der Überprüfungsfristen auf zum Zweck der vorbeugenden Bekämpfung von Straftaten gespeicherte personenbezogene Daten wird entsprechend der neuen Regelung in § 76 Absatz 2 aufgehoben.

Die Überprüfungsfristen nach § 76 Absatz 2 werden einheitlich für Erwachsene, Jugendliche und Kinder auf fünf Jahre festgesetzt.

Zudem wird der bisherige zweite Halbsatz in Absatz 1 Nummer 2 ersatzlos gestrichen. Aus fachlicher Sicht sprechen gute Gründe dafür, auf die einschränkende Bedingung zu verzichten, dass personenbezogene Daten von Kindern nur dann gespeichert werden dürfen, wenn „kein kindstypisches entwicklungsbedingtes Fehlverhalten“ vorliegt. Denn ohne die Einschränkung kann mehrfache Delinquenz bei Kindern leichter erkannt und negativen Entwicklungen frühzeitiger entgegengetreten werden.

Zu Absatz 2

Auf Anregung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit wird die Vorschrift in Absatz 2 Nummer 3 mit den Rahmenrichtlinien für den Kriminalaktennachweis (KAN) harmonisiert.

Zu Absatz 3

Aufgrund des Wegfalls der Differenzierung zwischen Erwachsenen, Jugendlichen und Kindern in Absatz 1 werden auch die verkürzten Überprüfungsfristen einheitlich auf drei Jahre festgesetzt. In Satz 2 werden die Worte „in der Regel“ gestrichen. Dadurch soll eine unverhältnismäßig lange Speicherung von „Bagatelldelikten“ verhindert werden. Soweit eine längere Speicherung solcher Delikte im Einzelfall dennoch geboten sein sollte, ist dies künftig allein anhand der Kriterien in § 5 Absatz 4 zu bewerten. Die Änderung geht ebenfalls auf eine Anregung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit zurück.

Zu Absatz 4

Durch die Ergänzung der Wörter „aus sexuellen Motiven“ wird klargestellt, dass insbesondere die Tatbestände der Beleidigung (§ 185 StGB), der üblen Nachrede (§ 186 StGB), der Verleumdung (§ 187 StGB), der vorsätzlichen Körperverletzung (§ 223 StGB) und der Nötigung (§ 240 StGB) keine Fälle von geringer Bedeutung sind, wenn die Begehung aus sexuellen Motiven erfolgt.

5. Zu Artikel 3 Nummer 5

a) Die bisher in § 6 DVO PolG geregelte Anordnungsbefugnis für eine nach § 40 Absatz 4 PolG a.F. vorzunehmende Löschung von Daten bzw. Vernichtung von Unterlagen ist mit der Änderung des Polizeigesetzes (Artikel 1) nunmehr unmittelbar in § 48 Absatz 4 Sätze 2 und 3 geregelt. Daher wird § 6 DVO PolG gestrichen.

b) Da die polizeilichen Protokollierungspflichten im Zusammenhang mit der Verarbeitung personenbezogener Daten im Zuge der Änderungen des Polizeigesetzes (Artikel 1) vollumfänglich in den neuen §§ 73, 74 PolG geregelt sind, wird § 7 DVO PolG gestrichen.

6. Zu Artikel 3 Nummer 6
Mit der Ergänzung wird noch einmal klargestellt, dass die Polizeidienststellen auch beim Austausch von personenbezogenen Daten untereinander die allgemeinen Regeln für die weitere Verarbeitung (insbesondere die Grundsätze der hypothetischen Datenneuerhebung) zu beachten haben.

7. Zu Artikel 3 Nummer 7
Mit der Änderung wird die Regelung begrifflich an die neuen Vorschriften des Polizeigesetzes zur Berichtigung, Löschung sowie Einschränkung einer Datenverarbeitung angepasst, insbesondere §§ 75 und 92 PolG.

8. Zu Artikel 3 Nummer 8
Es handelt sich um eine redaktionelle Folgeänderung zur neuen Nummerierung des Polizeigesetzes (Artikel 1).

9. Zu Artikel 3 Nummer 9
Es handelt sich um eine redaktionelle Folgeänderung zur neuen Nummerierung des Polizeigesetzes (Artikel 1).

10. Zu Artikel 3 Nummer 10
Es handelt sich um eine redaktionelle Folgeänderung zur neuen Nummerierung des Polizeigesetzes (Artikel 1).

11. Zu Artikel 3 Nummer 11

Mit der Änderung wird die Regelung begrifflich an die neuen Vorschriften des Polizeigesetzes zur Berichtigung, Löschung sowie Einschränkung einer Datenverarbeitung angepasst, insbesondere §§ 75 und 92 PolG.

IV. Zu Artikel 4

Bereits die bisherige Fassung des Polizeigesetzes enthielt Befugnisse zum Einsatz besonderer Mittel der Datenerhebung (§ 22 Absätze 2 und 3), zum Einsatz eines IMSI-Catchers (§ 23a Absatz 6) sowie zur Rasterfahndung (§ 40 Absatz 1). Allerdings war für die Anordnung solcher Maßnahmen bislang keine richterliche Entscheidung erforderlich. Mit der Übergangsregelung wird aus Gründen der Rechtssicherheit klargestellt, dass solche vor Inkrafttreten dieses Gesetzes angeordnete Maßnahmen, deren Durchführung sich über den Zeitpunkt des Inkrafttretens dieses Gesetzes hinaus erstreckt, keiner nachträglichen richterlichen Entscheidung im Sinne der neuen Regelungen (§ 48 Absatz 3, § 49 Absatz 4 sowie § 55 Absatz 1 in Verbindung mit § 53 Absatz 2 PolG) bedürfen.

V. Zu Artikel 5

Die Bestimmung regelt das Inkrafttreten des Gesetzes und das gleichzeitige Außerkrafttreten des bisherigen Polizeigesetzes für Baden-Württemberg. Da die neuen Vorschriften einen erheblichen Anpassungsbedarf bei vorhandenen untergesetzlichen Regelungen und Formularen auslösen, wird eine Übergangsfrist für das Inkrafttreten von drei Monaten festgelegt.