

Gesetzentwurf

der CDU-Fraktion

Zwölftes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes

Gesetzentwurf

der CDU-Fraktion

Zwölftes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes

A. Problem

In den vergangenen Jahren hat sich die polizeiliche Gefahrenlage in Deutschland und auch in Brandenburg hinsichtlich bestimmter Kriminalitätsphänomene wie dem Terrorismus und der Politisch motivierten Kriminalität, der Organisierten und Grenzüberschreitenden Kriminalität sowie der Wirtschafts- und Cyberkriminalität verschärft. Das Internet und andere technische Innovationen haben neben ihrem positiven Mehrwert für die Menschen auch zu neuen Formen und Methoden der Kriminalität geführt. Kriminalität kann sich unter Verwendung dieser modernen Mittel verdeckter, schneller und schlagkräftiger ausbreiten.

Zur effektiveren Abwehr dieser Gefahren müssen notwendige polizeiliche Befugnisse unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichtes, der Bundes- und anderen Länderpolizeigesetze sowie der Vorgaben durch die Europäische Union im brandenburgischen Landesrecht umgesetzt und bestehende Sicherheitslücken zum Schutz der Bevölkerung geschlossen werden. So bedarf es einer dem Stand der Technik entsprechenden Ergänzung wichtiger polizeilicher Befugnisnormen. Gleichzeitig müssen auch die Eingriffsbefugnisse der Polizei mit den persönlichen Freiheitsrechten der Menschen in einen angemessenen Ausgleich gebracht werden.

Das Bundesverfassungsgericht hat – insbesondere in seinem Urteil vom 20. April 2016 zum Bundeskriminalamtgesetz (1 BvR 966/09 und 1 BvR 1140/09) – seine Rechtsprechung zu den verfassungsgerichtlichen Anforderungen an die Ausgestaltung polizeilicher Eingriffsbefugnisse weiterentwickelt und präzisiert (z. B. zum Gefahrenbegriff, zur Einführung von weiteren Richtervorbehalten, zu expliziten Regelungen betreffend Vertrauenspersonen, zu verstärkten Anforderungen an die Zweckbindung und an die weitere Verarbeitung von Daten, zum Schutz des Kernbereichs privater Lebensgestaltung, zur Protokollierung, zu den Benachrichtigungspflichten sowie zur parlamentarischen und öffentlichen Kontrolle).

Die Richtlinie (EU) 2016/680 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 (EU-Datenschutzrichtlinie für den Bereich der Polizei) ist im Land Brandenburg in nationales Recht umzusetzen. So heißt es in Artikel 63 der Richtlinie, dass die Mitgliedstaaten bis zum 6. Mai 2018 die Rechts- und Verwaltungsvorschriften, die erforderlich sind, um dieser Richtlinie nachzukommen, erlassen und veröffentlichen. Sie teilen der Kommission unverzüglich den Wortlaut dieser Vorschriften mit und wenden diese Vorschriften ab dem 6. Mai 2018 an.

B. Lösung

Durch diesen Gesetzentwurf wird das Brandenburgische Polizeigesetz umfassend geändert:

1. Die Polizeiarbeit hat sich in den vergangenen Jahrzehnten erheblich verändert. Insbesondere die oben aufgeführten Kriminalitätsphänomene haben dazu geführt, dass die Polizei im Bereich der selektiven Kriminalprävention verstärkt strategisch auf Grundlage kriminalpräventiver Handlungskonzepte und operativ durch Präventionsplanungen, in denen bestimmte polizeitaktische Maßnahmen auf die Verhütung oder vorbeugende Bekämpfung von Straftaten oder Kriminalitätsphänomenen ausgerichtet werden, handelt. Um diese Entwicklung im Polizeigesetz nachzuvollziehen, werden
 - das Merkmal „Kriminalitätsphänomen“ in das Polizeigesetz eingeführt und definiert,
 - die schwerwiegenden Kriminalitätsphänomene des Terrorismus und der Politisch motivierten Kriminalität, der Organisierten und schwerwiegenden Grenzüberschreitenden Kriminalität sowie der schwerwiegenden Wirtschafts- und Cyberkriminalität definiert und in den Befugnisnormen verankert,
 - polizeiliche Maßnahmen zur „Verhütung oder vorbeugenden Bekämpfung von Straftaten oder Kriminalitätsphänomenen“ an kriminalpräventive Handlungskonzepte und operative Präventionsplanungen gebunden und
 - die Gefahrenabwehr im digitalen Raum ausdrücklich als polizeiliche Aufgabe geregelt.
2. Wichtige Begriffe werden zusammengefasst vorne im Gesetz definiert. So wird der polizeiliche Gefahrenbegriff konkretisiert. In der Entscheidung des Bundesverfassungsgerichtes zum Bundeskriminalamtgesetz wurden die Kriterien des Begriffs der „konkreten Gefahr“ hinsichtlich der Online-Durchsuchung fortentwickelt, der die maßgebliche Eingriffsvoraussetzung in den Polizeigesetzen bildet. Eine konkrete Gefahr kann schon zu einem sehr frühen Zeitpunkt des Kausalverlaufs angenommen werden, wenn auf Grundlage der polizeilichen Prognoseentscheidung zwar noch kein abschließendes Wahrscheinlichkeitsurteil zum Schadenseintritt getroffen werden kann, aber im Einzelfall von konkreten Personen innerhalb eines absehbaren Zeitraums und der Art nach konkretisierten Weise oder aufgrund ihres individuellen Verhaltens in überschaubarer Zukunft mit konkreter Wahrscheinlichkeit schwere Schädigungshandlungen gegen bedeutsame Rechtsgüter zu erwarten sind. Weiterhin werden im Gesetz die abstrakte und die erhöhte abstrakte Gefahr definiert. Frühzeitige Anhaltspunkte einer konkreten Gefahr lassen sich nämlich nur aus dem Schatten der abstrakten Gefahr erhellen, wenn die Polizei bereits zu einem solchen Zeitpunkt weniger eingriffsintensive Aufklärungs- und Erforschungsmaßnahmen ergreifen kann. Beispielsweise wird im Gesetz entsprechend der Rechtsprechung im Freistaat Bayern die Identitätsfeststellung durch die Schleierfahndung bereits zum Zeitpunkt der abstrakten Gefahr zugelassen. Darüber hinaus werden auch Definitionen der EU-Datenschutzrichtlinie für den Bereich der Polizei übernommen.

3. Die EU-Datenschutzrichtlinie für den Bereich der Polizei und die Rechtsprechung des Bundesverfassungsgerichtes werden im Polizeigesetz in Kapitel 2 Abschnitt 2 zur Datenverarbeitung als neuer Unterabschnitt 1 „Allgemeine Vorschriften zur Datenverarbeitung und zum Datenschutz“ geregelt und durch einen Verweis im Ordnungsbehördengesetz entsprechend auf die gefahrenabwehrrechtlichen Maßnahmen der Ordnungsbehörden angewendet. Der Unterabschnitt 1 hat die folgenden Regelungsinhalte:
 - Grundsätze der Verarbeitung personenbezogener Daten und besonders geschützte Datenkategorien,
 - Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung,
 - Benachrichtigungspflichten,
 - Auskunftsrecht und Akteneinsicht,
 - Verzeichnis von Verarbeitungstätigkeiten, Protokollierung und Kontrolle durch die oder den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht,
 - automatisierte Verfahren der Datenverarbeitung,
 - Errichtungsanordnung für Dateien und Datenschutz-Folgenabschätzung,
 - Anwendung des Brandenburgischen Datenschutzgesetzes und
 - parlamentarische Kontrolle.
4. Weiterhin werden die polizeilichen Befugnisnormen im Sinne der Nummern 1 bis 3 angepasst und insbesondere der folgende Katalog an Maßnahmen umgesetzt, die zum Teil je nach Schwere des Eingriffs an einen Richtervorbehalt gebunden sowie ministeriellen und parlamentarischen Kontrollsystemen unterworfen werden:
 - a) Anpassung der Regelung zur Videoüberwachung:
 - Möglichkeit der Übersichtsaufzeichnungen bei Veranstaltungen und Ansammlungen,
 - Ausweitung der Videoüberwachung im öffentlichen Raum auf sogenannte „weiche Ziele“ (beispielsweise öffentliche Plätze, Busbahnhöfe usw.),
 - Einbeziehung intelligenter Videoüberwachungssysteme mit automatisierter und sensorischer Erkennungs- und Auswertungsfunktion einschließlich der automatischen Systemsteuerung und des Abgleichs mit biometrischen Daten von Straftätern und Gefährdern,
 - Verlängerung der Datenspeicherfrist;
 - b) Regelung des Einsatzes von Bodycams mit Pre-Recording-Funktion einschließlich der Verwendung in Wohnungen;

- c) Ermöglichung sogenannter verdachts- und anlassunabhängiger Kontrollen („Schleierfahndung“) im gesamten öffentlichen Verkehrsraum des Landes Brandenburg;
- d) Ausweitung der Frist des Polizeigewahrsams auf einen Monat mit der Möglichkeit, bei einem weiteren Vorliegen der Tatbestandsvoraussetzungen Verlängerungen herbeizuführen;
- e) Einführung von Rechtsgrundlagen
 - zur elektronischen Aufenthaltsüberwachung (elektronische Fußfessel) einschließlich einer Strafvorschrift für Maßnahmenverstöße sowie
 - zur Verhängung eines Aufenthaltsgebotes und Kontaktverbotes
 insbesondere für als Gefährder eingestufte Personen;
- f) Kodifizierung der Meldeauflage mit einem hinreichend weiten zeitlichen Aufgabenspielraum;
- g) Regelung der Identitätsfeststellung durch die Erhebung genetischer Daten (DNA-Identifizierungsmuster und Geschlecht sowie bei DNA-Spuren unbekannter Personen auch die Augen-, Haar- und Hautfarbe, das biologische Alter und die biogeographische Herkunft);
- h) Ermöglichung der Durchsuchung räumlich getrennter elektronischer Speichermedien;
- i) Kodifizierung der Sicherstellung von Forderungen und anderen Vermögensrechten durch Pfändung sowie der Postsicherstellung;
- j) Schaffung einer klaren Rechtsgrundlage für
 - die Telekommunikationsüberwachung unter Eingriff in informationstechnische Systeme einschließlich sogenannter Messenger-Dienste (Quellen-Telekommunikationsüberwachung) sowie
 - den verdeckten Zugriff auf informationstechnische Systeme zur Erhebung von Daten (Online-Durchsuchung);
- k) Regelungen
 - zur präventiven Öffentlichkeitsfahndung,
 - zum Einsatz und zur Abwehr unbemannter Luftfahrtsysteme und
 - zur Möglichkeit des zielgerichteten Einwirkens auf Straftäter mit Sprengmitteln in Fällen des Terrorismus oder sonstiger schwerer Kriminalität;
- l) Konkretisierung des Einsatzes von Vertrauenspersonen als Folge verfassungsrechtlicher Rechtsprechung und der NSU-Erkenntnisse;

- m) Ermöglichung projektbezogener gemeinsamer Dateien mit dem Verfassungsschutz Brandenburg im Bereich Terrorismus und geheimdienstlicher Tätigkeit;
 - n) Regelung der in der EU-Datenschutzrichtlinie für den Bereich der Polizei niedergelegten Voraussetzungen für das sogenannte „Profiling“;
 - o) Opfer- und Zeugenschutzregelung zur Herstellung und Veränderung von Urkunden und sonstigen Dokumenten für den Aufbau und die Aufrechterhaltung einer vorübergehend geänderten Identität.
5. Im Ordnungsbehördengesetz werden die Verweise auf das Polizeigesetz angepasst:
- a) Bestimmte Maßnahmenerweiterungen insbesondere bei der Frist des Polizeigewahrsams und bei der Videoüberwachung im Polizeigesetz werden für die Ordnungsbehörden nicht übernommen.
 - b) Der Einsatz von Bodycams wird nach der Zustimmung des für Inneres zuständigen Ministeriums und einer Pilotphase in den betroffenen Kommunen auch den Ordnungsbehörden ermöglicht, wenn dieser erforderlich ist.

C. Rechtsfolgenabschätzung

I. Erforderlichkeit

Die Entwicklungen bei den oben genannten Kriminalitätsphänomenen machen es notwendig die angeführten Gesetzesänderungen vorzunehmen. Die Vorgaben der Europäischen Union und des Bundesverfassungsgerichtes sind umzusetzen. Außerdem dienen die Änderungen dazu, ein Auseinanderfallen des Normenbestandes im Polizeirecht zu den Regelungen des Bundes (BKAG) und anderer Bundesländer zu verhindern.

II. Zweckmäßigkeit

Die beabsichtigten Regelungen sind für diesen Zweck unverzichtbar.

III. Auswirkungen auf Bürgerinnen und Bürger, Wirtschaft und Verwaltung

Die Bürgerinnen und Bürger sowie die Unternehmen im Land Brandenburg erhalten durch die verbesserten Handlungsbefugnisse der Polizei zur Abwehr von Gefahren, Straftaten und Kriminalitätsphänomenen mehr Sicherheit.

Für die Wirtschaft entsteht durch die Einführung der Regelung zur Postsicherung wegen der zu erwartenden wohl eher geringen Fallzahlen wohl ein geringer Erfüllungsaufwand.

Kosten bei der Polizei entstehen insbesondere beim Personal, das aufgestockt und fortlaufend weitergebildet werden muss, und bei der Sachausstattung der

Polizei, damit die Rechtsvorschriften im Rahmen der täglichen Polizeiarbeit effektiv ausgefüllt werden können. Etwaige Mehrkosten für den Landeshaushalt lassen sich zum aktuellen Zeitpunkt noch nicht verlässlich beziffern. Jedoch sind die folgenden Kostenfaktoren zu berücksichtigen:

1. Anpassung und Betreuung der IT-Infrastruktur und der polizeilichen Fachverfahren (z. B. Vorgangs-, Fallbearbeitungs- und Fahndungssystem) auf Grundlage der erweiterten Datenschutz-, Kennzeichnungs-, Dokumentations-, Protokollierungs-, Prüf-, Berichts-, Berichtigungs-, Hinweis- und Benachrichtigungspflichten nach den Entscheidungen des Bundesverfassungsgerichtes und der EU-Datenschutzrichtlinie für den Bereich der Polizei;
2. Schnittstellenanpassungen und Verbindung zu externen bundesweiten Verfahren nach dem neugefassten Bundeskriminalamtgesetz (umfangreicher Planungs-, Abstimmungs- und Realisierungsaufwand);
3. Mehrkosten (insbesondere Personal und Fortbildung) bei Polizei und Justiz durch erweiterte Vorlagen zur Entscheidung durch die Richterin oder den Richter und die Sichtung kernbereichsrelevanter Daten für bestimmte Fälle;
4. Beispiele zu Beschaffungskosten für Ausrüstung und Verbrauchsmaterialien:
 - Materialkosten pro DNA-Analyse von ca. 25 Euro,
 - Einzelkosten für ein Bodycam-System von ca. 1.500 bis 2.000 Euro zuzüglich 1.000 Euro pro Dienststelle für ein Auslesesystem,
 - Kosten des Einsatzes eines intelligenten Kamerasystems im sechsstelligen Bereich und
 - Beschaffungskosten für geeignete unbemannte Luftfahrtsysteme zur Datenerhebung pro Stück von 20.000 bis 25.000 Euro.

D. Zuständigkeiten

Zuständig ist der Minister des Innern und für Kommunales.

Gesetzentwurf für ein

Zwölftes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes

Vom ...

Der Landtag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des Brandenburgischen Polizeigesetzes

Das Brandenburgische Polizeigesetz vom 19. März 1996 (GVBl. I S. 74), das zuletzt durch Artikel 14 des Gesetzes vom 25. Januar 2016 (GVBl. I Nr. 5 S. 18) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

a) Nach der Angabe zu § 2 werden die folgenden Angaben eingefügt:

„§ 3 Begriffsbestimmungen

§ 4 Allgemeine Voraussetzungen selektiver Kriminalprävention“.

b) Die Angaben zu den bisherigen §§ 3 bis 6 werden die Angaben zu den §§ 5 bis 8.

c) Nach der Angabe zu § 8 wird die folgende Angabe eingefügt:

„§ 9 Unmittelbare Ausführung einer Maßnahme“.

d) Die Angaben zu den bisherigen §§ 7 bis 13 werden die Angaben zu den §§ 10 bis 16 und in der Angabe zum neuen § 13 das Komma und das Wort „Begriffsbestimmung“ gestrichen.

e) Die Angabe zum bisherigen § 14 wird durch die folgende Angabe ersetzt:

„§ 17 Prüfung von Berechtigungsscheinen und sonstigen Urkunden“.

f) Die Angabe zum bisherigen § 15 wird die Angabe zu § 18.

g) Die Angaben zu den bisherigen §§ 16 und 16a werden durch die folgenden Angaben ersetzt:

„§ 19 Meldeauflage

§ 20 Platzverweisung, Kontaktverbot, Aufenthaltsanordnung und Wohnungsaufenthaltsverbot“.

h) Die Angaben zu den bisherigen §§ 17 bis 28 werden die Angaben zu den §§ 21 bis 32.

- i) Die Angaben zu Kapitel 2 Abschnitt 2 werden wie folgt gefasst:

„Abschnitt 2

Datenverarbeitung

Unterabschnitt 1

Allgemeine Vorschriften zur Datenverarbeitung und zum Datenschutz

§ 33 Grundsätze der Datenverarbeitung

§ 34 Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung

§ 35 Benachrichtigungspflichten

§ 36 Auskunftrecht, Akteneinsicht

§ 37 Verzeichnis von Verarbeitungstätigkeiten, Protokollierung, Kontrolle durch die oder den Landesbeauftragten

§ 38 Automatisierte Verfahren der Datenverarbeitung

§ 39 Errichtungsanordnung für Dateien, Datenschutz-Folgenabschätzung

§ 40 Anwendung des Brandenburgischen Datenschutzgesetzes

§ 41 Parlamentarische Kontrolle

Unterabschnitt 2

Datenerhebung

§ 42 Grundsätze der Datenerhebung

§ 43 Allgemeine Befugnis zur Datenerhebung

§ 44 Offene Bild- und Tonaufnahmen oder -aufzeichnungen

§ 45 Elektronische Aufenthaltsüberwachung, Strafvorschrift

§ 46 Postsicherstellung

§ 47 Einsatz besonderer Mittel der Datenerhebung

§ 48 Einsatz technischer Mittel zur Überwachung von Wohnungen

§ 49 Eingriffe in die Telekommunikation und in informationstechnische Systeme, Verkehrs- und Nutzungsdatenauskunft

§ 50 Bestandsdatenauskunft

§ 51 Datenerhebung durch den Einsatz von Vertrauenspersonen

§ 52 Datenerhebung durch den Einsatz verdeckt ermittelnder Personen

§ 53 Polizeiliche Ausschreibung

§ 54 Anlassbezogene automatische Kennzeichenfahndung

§ 55 Einsatz und Abwehr unbemannter Luftfahrtsysteme

Unterabschnitt 3

Datenspeicherung, Datenveränderung und Datennutzung

§ 56 Allgemeine Regeln über die Dauer der Datenspeicherung

§ 57 Zweckbindung bei der Datenspeicherung, Datenveränderung und Datennutzung

§ 58 Speicherung, Veränderung und Nutzung von Daten

§ 59 Datenabgleich

Unterabschnitt 4

Datenübermittlung

§ 60 Allgemeine Regeln der Datenübermittlung

§ 61 Datenübermittlung zwischen Polizeibehörden

§ 62 Datenübermittlung an öffentliche Stellen, an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen

§ 63 Datenübermittlung an Personen oder an Stellen außerhalb des öffentlichen Bereichs, Bekanntgabe an die Öffentlichkeit

§ 64 Datenübermittlung an die Polizei

§ 65 Rasterfahndung, Profiling

§ 66 Projektbezogene gemeinsame Dateien mit dem Verfassungsschutz Brandenburg

Unterabschnitt 5

Datenberichtigung, Datenlöschung und Datensperrung

§ 67 Berichtigung, Löschung und Sperrung von Daten“.

j) Die Angaben zu den bisherigen §§ 50 bis 65 werden die Angaben zu den §§ 68 bis 83.

k) Die Angaben zu den bisherigen §§ 66 bis 69 werden durch die folgenden Angaben ersetzt:

„§ 84 Allgemeine Vorschriften für den Schusswaffengebrauch

§ 85 Schusswaffengebrauch gegen Personen

§ 86 Schusswaffengebrauch gegen Personen in einer Menschenmenge

§ 87 Sprengmittel“.

- l) Die Angabe zum bisherigen § 70 wird die Angabe zu § 88.
- m) Die Angaben zu den Kapiteln 6 bis 8 werden durch die folgenden Angaben ersetzt:

„Kapitel 6

Organisation und Zuständigkeit der Polizei, Polizeibeiräte

Abschnitt 1

Organisation der Polizei

§ 89 Polizeibehörde und -einrichtungen

Abschnitt 2

Zuständigkeit der Polizei

§ 90 Amtshandlungen von Polizeivollzugsbediensteten außerhalb Brandenburgs

§ 91 Amtshandlungen von Polizeivollzugsbediensteten anderer Länder und des Bundes sowie von Bediensteten ausländischer Staaten im Land Brandenburg

§ 92 Zuständigkeit des Polizeipräsidiums, des Zentraldienstes der Polizei mit seiner Zentralen Bußgeldstelle und der Polizeivollzugsbediensteten

Abschnitt 3

Polizeibeiräte

§ 93 Polizeibeiräte

§ 94 Wahl der Mitglieder

§ 95 Verordnungsermächtigung

Kapitel 7

Schlussvorschriften

§ 96 Verwaltungsabkommen

§ 97 Verwaltungsvorschriften

§ 98 Opferschutz, Zeugenschutz“.

- 2. § 1 wird wie folgt geändert:

- a) Absatz 1 wird wie folgt gefasst:

„(1) Die Polizei hat die Aufgabe, die allgemein oder im Einzelfall bestehenden Gefahren für die öffentliche Sicherheit oder Ordnung abzuwehren (Gefahrenabwehr). Sie hat im Rahmen dieser Aufgabe auch

1. die freiheitliche demokratische Grundordnung zu schützen und die ungehinderte Ausübung der Grundrechte und der staatsbürgerlichen Rechte zu gewährleisten (Schutz wichtiger Verfassungsgüter),
2. die erforderlichen Vorbereitungen für die Hilfeleistungen und das Handeln in Gefahrenfällen zu treffen (Vorbereitungshandlungen),
3. Straftaten und Kriminalitätsphänomene zu verhüten und vorbeugend zu bekämpfen (selektive Kriminalprävention),
4. zur Vermeidung strafbarer Verhaltensweisen beizutragen (universelle Kriminalprävention) und
5. Gefahrenabwehr im digitalen Raum zu betreiben, soweit ein Bezug zum Land Brandenburg besteht.“

b) Absatz 3 wird wie folgt gefasst:

„(3) Die Polizei leistet anderen Behörden und den Gerichten Vollzugshilfe (§§ 68 bis 70).“

c) In Absatz 5 werden die Wörter „§§ 11 bis 15 sowie den §§ 29 bis 49“ durch die Wörter „§§ 14 bis 18 sowie den §§ 33 bis 67“ ersetzt.

3. § 2 wird wie folgt geändert:

a) In Satz 1 wird die Angabe „Abs.“ durch das Wort „Absatz“ ersetzt.

b) Nach Satz 1 wird folgender Satz 2 eingefügt:

„Darüber hinaus ist die Polizei zur vernetzten Zusammenarbeit mit anderen Sicherheitsbehörden (Polizei, Verfassungsschutz, Staatsanwaltschaften und Ordnungsbehörden) verpflichtet, soweit dies rechtlich möglich ist.“

c) In dem neuen Satz 3 werden nach den Wörtern „allen Vorgängen“ die Wörter „und übermittelt Daten“ eingefügt.

4. Nach § 2 werden die folgenden §§ 3 und 4 eingefügt:

„§ 3

Begriffsbestimmungen

Im Sinne dieses Gesetzes sind

1. öffentliche Sicherheit die Unverletzlichkeit der Rechtsordnung, der subjektiven Rechte und Rechtsgüter des einzelnen sowie der Einrichtungen und Veranstaltungen des Staates oder sonstiger Träger der Hoheitsgewalt;

2. öffentliche Ordnung die Gesamtheit der ungeschriebenen Ordnungsvorstellungen, deren Befolgung nach der herrschenden sozialen und ethischen Anschauung als unerlässliche Voraussetzung eines geordneten menschlichen Zusammenlebens anzusehen sind;
3. bedeutsames Rechtsgut das Leben, die Gesundheit, die Freiheit der Person, der Bestand oder die Sicherheit des Bundes oder eines Landes, die sexuelle Selbstbestimmung, eine bedeutende Sach- oder Vermögensposition oder eine Sache, deren Erhalt im besonderen öffentlichen Interesse liegt;
4. konkrete Gefahr eine Sachlage, bei der im Einzelfall auf Grundlage einer Prognoseentscheidung die hinreichende Wahrscheinlichkeit besteht, dass bei ungehindertem Geschehensablauf in absehbarer Zeit ein Schaden für die öffentliche Sicherheit oder Ordnung eintreten wird;
 - a. je größer der zu erwartende Schaden für ein betroffenes Schutzgut und je höher dessen Rang auch im Vergleich zu anderen durch eine polizeiliche Maßnahme betroffenen Rechtsgütern ist, desto geringere Anforderungen sind an die Wahrscheinlichkeit zu stellen, so dass die Polizei eine bestimmte Maßnahme zu einem frühen Zeitpunkt des Kausalverlaufs ergreifen kann;
 - b. eine konkrete Gefahr kann bereits zu einem sehr frühen Zeitpunkt des Kausalverlaufs vor der Feststellung der hinreichenden Wahrscheinlichkeit eines Schadenseintritts angenommen werden, wenn im Einzelfall bestimmte Tatsachen die Annahme rechtfertigen, dass von konkreten Personen
 - aa. innerhalb eines absehbaren Zeitraums und der Art nach konkretisierten Weise oder
 - bb. aufgrund ihres individuellen Verhaltens in überschaubarer Zukunft mit konkreter Wahrscheinlichkeit
 eine schwere Schädigungshandlung gegen ein bedeutsames Rechtsgut zu erwarten ist, insbesondere bei Anhaltspunkten auf Planungs- oder Vorbereitungshandlungen;
5. gegenwärtige konkrete Gefahr eine Sachlage, bei der die Einwirkung des schädigenden Ereignisses bereits begonnen hat oder bei der diese Einwirkung unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorsteht;
6. erhebliche konkrete Gefahr eine Sachlage, bei der ein Schaden für ein bedeutsames Rechtsgut droht;
7. dringende konkrete Gefahr eine Sachlage, bei der die hohe Wahrscheinlichkeit eines Schadens für ein bedeutsames Rechtsgut besteht;
8. konkrete Gefahr für Leib oder Leben eine Sachlage, bei der eine nicht unerhebliche Körperverletzung oder der Tod einzutreten droht;

9. abstrakte Gefahr eine nach polizeilicher Erfahrung und nach allgemeinen Lageerkenntnissen vorliegende Sachlage, bei der allgemein ein Schaden für die öffentliche Sicherheit oder Ordnung möglich erscheint;
10. erhöhte abstrakte Gefahr eine nach polizeilicher Erfahrung und nach hinreichend greifbaren Lageerkenntnissen vorliegende Sachlage, bei der allgemein mit einem Schaden für die öffentliche Sicherheit oder Ordnung gerechnet werden kann;
11. Gefahr im Verzug eine Sachlage, bei der ein Schaden eintreten würde, wenn nicht an Stelle der zuständigen Behörde oder Person die Polizei oder eine im Polizeivollzugsdienst tätige Person eine Maßnahme der Gefahrenabwehr ergreift;
12. Kriminalitätsphänomen ein bestimmtes Kriminalitätsfeld, das die öffentliche Sicherheit oder Ordnung in nicht unbeträchtlicher Weise beeinträchtigt;
13. schwerwiegendes Kriminalitätsphänomen
 - a. Organisierte Kriminalität die von Gewinn- oder Machtstreben bestimmte planmäßige Begehung, Veranlassung oder Unterstützung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei beteiligte Personen auf längere oder unbestimmte Dauer arbeitsteilig
 - aa. unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen,
 - bb. unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder
 - cc. unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken;
 - b. schwerwiegende Grenzüberschreitende Kriminalität die Begehung, Veranlassung oder Unterstützung von Straftaten von erheblicher Bedeutung, deren Begehungsweisen, Tatörtlichkeiten, Tatelemente, Täter oder Tätergruppen über die staatlichen Grenzen eines Nationalstaates hinweg aufgeteilt sind;
 - c. Politisch motivierte Kriminalität die Begehung, Veranlassung oder Unterstützung von Staatsschutzdelikten nach den §§ 80a bis 109h, 129a, 129b, 234a oder 241a des Strafgesetzbuches oder von Straftaten, bei denen die Tatumstände oder die TäterEinstellung Anhaltspunkte dafür bieten, dass diese
 - aa. den demokratischen Willensbildungsprozess beeinflussen sollen,
 - bb. der Erreichung oder Verhinderung politischer, religiöser oder ideologischer Ziele dienen; einschließlich des Terrorismus mit den Gefahren der physischen oder psychischen Gewalt zur Erreichung solcher Ziele, insbesondere

- aaa. die Einschüchterung der Bevölkerung auf erhebliche Weise,
 - bbb. das Rekrutieren von Personen zu terroristischen Zwecken,
 - ccc. die rechtswidrige Nötigung einer Behörde oder einer über- oder zwischenstaatlichen Stelle mit Gewalt oder durch Drohung mit Gewalt oder
 - ddd. die Beseitigung oder erhebliche Beeinträchtigung der politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates, eines Landes oder einer über- oder zwischenstaatlichen Stelle,
- und die durch die Art ihrer Begehung oder ihrer Auswirkungen einen Staat, ein Land oder eine über- und zwischenstaatliche Stelle erheblich schädigen können,
- cc. sich gegen die Realisierung politischer Entscheidungen richten,
 - dd. sich gegen die freiheitlich demokratische Grundordnung oder eines ihrer Wesensmerkmale richten,
 - ee. sich gegen den Bestand und die Sicherheit des Bundes oder eines Landes richten,
 - ff. eine ungesetzliche Beeinträchtigung der Amtsführung von Mitgliedern der Verfassungsorgane des Bundes oder eines Landes zum Ziel haben,
 - gg. durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden oder
 - hh. gegen eine Person wegen ihrer politischen Einstellung, Nationalität, Volkszugehörigkeit, Hautfarbe, Religion, Weltanschauung, Herkunft, ihres Erscheinungsbildes, aufgrund rassistischer Gründe, wegen ihrer Behinderung, sexuellen Orientierung oder ihres gesellschaftlichen Status gerichtet sind und die Tathandlung damit im Kausalzusammenhang steht oder sich in diesem Zusammenhang gegen eine Institution, eine Sache oder ein Objekt richtet;
- d. schwerwiegende Wirtschaftskriminalität die Begehung, Veranlassung oder Unterstützung
- aa. der in § 74c Absatz 1 Satz 1 Nummer 1 bis 6b des Gerichtsverfassungsgesetzes aufgeführten Straftaten mit wirtschaftlichem Bezug oder
 - bb. von staatlich gelenkter oder gestützter illegaler Ausforschung (Wirtschaftsspionage) oder von konkurrierenden Unternehmen gelenkte oder gestützte illegale Ausforschung (Konkurrenzspionage) im Zielbereich Wirtschaft,

die im Einzelfall oder in ihrer Gesamtheit schwer wiegen;

- e. schwerwiegende Cyberkriminalität die Begehung, Veranlassung oder Unterstützung von Straftaten, die sich gegen das Internet, das Internet der Dinge, Datennetze, andere informationstechnische Systeme oder deren Daten richten oder die mittels Informationstechnik begangen werden, einschließlich der Cyberspionage und Cybersabotage, und die im Einzelfall oder in ihrer Gesamtheit schwer wiegen;
14. verfassungsfeindliche Handlung eine Handlung, die den objektiven Tatbestand einer Störung oder Abänderung der verfassungsmäßigen Ordnung der Bundesrepublik Deutschland oder eines ihrer Länder in verfassungswidriger Weise verwirklicht und weder eine Straftat noch eine Ordnungswidrigkeit ist;
 15. Ordnungswidrigkeit eine rechtswidrige Tat, die den objektiven Tatbestand eines Ordnungswidrigkeitsgesetzes verwirklicht;
 16. Ordnungswidrigkeit von erheblicher Bedeutung eine rechtswidrige Tat, die den objektiven Tatbestand eines Ordnungswidrigkeitsgesetzes verwirklicht, und nach den Umständen des Einzelfalls
 - a. ein Schaden für ein bedeutsames Rechtsgut,
 - b. für andere Rechtsgüter in erheblichem Umfang oder
 - c. hinsichtlich ihrer Art und Dauer die nachhaltige Beeinträchtigung des Rechtsfriedens droht;
 17. Straftat eine rechtswidrige Tat, die den objektiven Tatbestand eines Strafgesetzes verwirklicht;
 18. Straftaten von erheblicher Bedeutung:
 - a. Verbrechen im Sinne des § 12 Absatz 1 des Strafgesetzbuches,
 - b. aus dem Strafgesetzbuch:
 - aa. Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80a bis 82, 84 bis 86, 87 bis 89a, 89c Absatz 1 bis 4, 94 bis 100a,
 - bb. Bestechlichkeit und Bestechung von Mandatsträgern nach § 108e,
 - cc. Straftaten gegen die Landesverteidigung nach den §§ 109d bis 109h,
 - dd. Straftaten gegen die öffentliche Ordnung nach den §§ 129 bis 130,

- ee. Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Absatz 3 und § 152b Absatz 1 bis 4,
- ff. Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176a, 176b und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,
- gg. Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften nach § 184b Absatz 1 und 2, § 184c Absatz 2,
- hh. Mord und Totschlag nach den §§ 211 und 212,
- ii. Straftaten gegen die persönliche Freiheit nach den §§ 232, 232a Absatz 1 bis 5, den §§ 232b, 233 Absatz 2, den §§ 233a, 234, 234a, 239a und 239b,
- jj. Bandendiebstahl nach § 244 Absatz 1 Nummer 2 und schwerer Bandendiebstahl nach § 244a,
- kk. Straftaten des Raubes und der Erpressung nach den §§ 249 bis 255,
- ll. gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260 und 260a,
- mm. Geldwäsche und Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 Absatz 1, 2 und 4; beruht die Strafbarkeit darauf, dass die Straflosigkeit nach § 261 Absatz 9 Satz 2 gemäß § 261 Absatz 9 Satz 3 ausgeschlossen ist, jedoch nur dann, wenn der Gegenstand aus einer der in den Buchstaben a bis m genannten schweren Straftaten herrührt,
- nn. Betrug und Computerbetrug unter den in § 263 Absatz 3 Satz 2 genannten Voraussetzungen und im Falle des § 263 Absatz 5, jeweils auch in Verbindung mit § 263a Absatz 2,
- oo. Subventionsbetrug unter den in § 264 Absatz 2 Satz 2 genannten Voraussetzungen und im Falle des § 264 Absatz 3 in Verbindung mit § 263 Absatz 5,
- pp. Sportwettbetrug und Manipulation von berufssportlichen Wettbewerben unter den in § 265e Satz 2 genannten Voraussetzungen,
- qq. Straftaten der Urkundenfälschung unter den in § 267 Absatz 3 Satz 2 genannten Voraussetzungen und im Falle des § 267 Absatz 4, jeweils auch in Verbindung mit § 268 Absatz 5 oder § 269 Absatz 3, sowie nach § 275 Absatz 2 und § 276 Absatz 2,
- rr. Bankrott unter den in § 283a Satz 2 genannten Voraussetzungen,
- ss. Straftaten gegen den Wettbewerb nach § 298 und, unter den in § 300 Satz 2 genannten Voraussetzungen, nach § 299,

- tt. gemeingefährliche Straftaten in den Fällen der §§ 306 bis 306c, 307 Absatz 1 bis 3, des § 308 Absatz 1 bis 3, des § 309 Absatz 1 bis 4, des § 310 Absatz 1, der §§ 313, 314, 315 Absatz 3, des § 315b Absatz 3 sowie der §§ 316a und 316c,
- uu. Bestechlichkeit und Bestechung nach den §§ 332 und 334,
- c. aus der Abgabenordnung:
 - aa. Steuerhinterziehung unter den in § 370 Absatz 3 Satz 2 Nummer 5 genannten Voraussetzungen,
 - bb. gewerbsmäßiger, gewaltsamer und bandenmäßiger Schmuggel nach § 373,
 - cc. Steuerhehlerei im Falle des § 374 Absatz 2,
- d. aus dem Anti-Doping-Gesetz: Straftaten nach § 4 Absatz 4 Nummer 2 Buchstabe b,
- e. aus dem Asylgesetz:
 - aa. Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Absatz 3,
 - bb. gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a,
- f. aus dem Aufenthaltsgesetz:
 - aa. Einschleusen von Ausländern nach § 96 Absatz 2,
 - bb. Einschleusen mit Todesfolge und gewerbs- und bandenmäßiges Einschleusen nach § 97,
- g. aus dem Außenwirtschaftsgesetz: vorsätzliche Straftaten nach den §§ 17 und 18 des Außenwirtschaftsgesetzes,
- h. aus dem Betäubungsmittelgesetz:
 - aa. Straftaten nach einer in § 29 Absatz 3 Satz 2 Nummer 1 in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen,
 - bb. Straftaten nach den §§ 29a, 30 Absatz 1 Nummer 1, 2 und 4 sowie den §§ 30a und 30b,
- i. aus dem Grundstoffüberwachungsgesetz: Straftaten nach § 19 Absatz 1 unter den in § 19 Absatz 3 Satz 2 genannten Voraussetzungen,
- j. aus dem Gesetz über die Kontrolle von Kriegswaffen:
 - aa. Straftaten nach § 19 Absatz 1 bis 3 und § 20 Absatz 1 und 2 sowie § 20a Absatz 1 bis 3, jeweils auch in Verbindung mit § 21,

- bb. Straftaten nach § 22a Absatz 1 bis 3,
 - k. aus dem Neue-psychoaktive-Stoffe-Gesetz: Straftaten nach § 4 Absatz 3 Nummer 1 Buchstabe a,
 - l. aus dem Völkerstrafgesetzbuch:
 - aa. Völkermord nach § 6,
 - bb. Verbrechen gegen die Menschlichkeit nach § 7,
 - cc. Kriegsverbrechen nach den §§ 8 bis 12,
 - dd. Verbrechen der Aggression nach § 13,
 - m. aus dem Waffengesetz:
 - aa. Straftaten nach § 51 Absatz 1 bis 3,
 - bb. Straftaten nach § 52 Abs. 1 Nr. 1 und 2 Buchstabe c und d sowie Absatz 5 und 6;
19. besonders schwere Straftaten:
- a. aus dem Strafgesetzbuch:
 - aa. Straftaten des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 81, 82, 89a, 89c Absatz 1 bis 4, nach den §§ 94, 95 Absatz 3 und § 96 Absatz 1, jeweils auch in Verbindung mit § 97b, sowie nach den §§ 97a, 98 Absatz 1 Satz 2, § 99 Absatz 2 und den §§ 100, 100a Absatz 4,
 - bb. Bildung krimineller Vereinigungen nach § 129 Absatz 1 in Verbindung mit Absatz 5 Satz 3 und Bildung terroristischer Vereinigungen nach § 129a Absatz 1, 2, 4, 5 Satz 1 erste Alternative, jeweils auch in Verbindung mit § 129b Absatz 1,
 - cc. Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Absatz 3 und § 152b Absatz 1 bis 4,
 - dd. Straftaten gegen die sexuelle Selbstbestimmung in den Fällen des § 176a Absatz 2 Nummer 2 oder Absatz 3 und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,
 - ee. Verbreitung, Erwerb und Besitz kinderpornografischer Schriften in den Fällen des § 184b Absatz 2,
 - ff. Mord und Totschlag nach den §§ 211, 212,
 - gg. Straftaten gegen die persönliche Freiheit in den Fällen der §§ 234, 234a Absatz 1, 2, der §§ 239a, 239b und Menschenhandel nach § 232 Absatz 3, Zwangsprostitution und Zwangsarbeit nach

§ 232a Absatz 3, 4 oder 5 zweiter Halbsatz, § 232b Absatz 3 oder 4 in Verbindung mit § 232a Absatz 4 oder 5 zweiter Halbsatz und Ausbeutung unter Ausnutzung einer Freiheitsberaubung nach § 233a Absatz 3 oder 4 zweiter Halbsatz,

- hh. Bandendiebstahl nach § 244 Absatz 1 Nummer 2 und schwerer Bandendiebstahl nach § 244a,
 - ii. schwerer Raub und Raub mit Todesfolge nach § 250 Absatz 1 oder Absatz 2, § 251,
 - jj. räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Absatz 4 Satz 2 genannten Voraussetzungen,
 - kk. gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260, 260a,
 - ll. besonders schwerer Fall der Geldwäsche, Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 unter den in § 261 Absatz 4 Satz 2 genannten Voraussetzungen; beruht die Strafbarkeit darauf, dass die Straflosigkeit nach § 261 Absatz 9 Satz 2 gemäß § 261 Absatz 9 Satz 3 ausgeschlossen ist, jedoch nur dann, wenn der Gegenstand aus einer der in den Buchstaben a bis g genannten besonders schweren Straftaten herrührt,
 - mm. gemeingefährliche Straftaten nach § 306b, § 306c, § 307 Absatz 1 bis 3, § 308 Absatz 1 bis 3, § 309 Absatz 1 bis 4, § 310 Absatz 1 Nummer 1, § 313 Absatz 1, § 313 Absatz 2 in Verbindung mit § 308 Absatz 2 und 3, § 314, § 315 Absatz 3, § 315b Absatz 3, § 316a oder § 316c Absatz 1 bis 3,
 - nn. besonders schwerer Fall der Bestechlichkeit und Bestechung nach § 335 Absatz 1 unter den in § 335 Absatz 2 Nummer 1 bis 3 genannten Voraussetzungen,
- b. aus dem Asylgesetz:
- aa. Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Absatz 3,
 - bb. gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a Absatz 1,
- c. aus dem Aufenthaltsgesetz:
- aa. Einschleusen von Ausländern nach § 96 Absatz 2,
 - bb. Einschleusen mit Todesfolge oder gewerbs- und bandenmäßiges Einschleusen nach § 97,
- d. aus dem Betäubungsmittelgesetz:

- aa. besonders schwerer Fall einer Straftat nach § 29 Absatz 1 Satz 1 Nummer 1, 5, 6, 10, 11 oder 13, Absatz 3 unter der in § 29 Absatz 3 Satz 2 Nummer 1 genannten Voraussetzung,
 - bb. eine Straftat nach den §§ 29a, 30 Absatz 1 Nummer 1, 2, 4, § 30a,
 - e. aus dem Gesetz über die Kontrolle von Kriegswaffen:
 - aa. eine Straftat nach § 19 Absatz 2 oder § 20 Absatz 1, jeweils auch in Verbindung mit § 21,
 - bb. besonders schwerer Fall einer Straftat nach § 22a Absatz 1 in Verbindung mit Absatz 2,
 - f. aus dem Völkerstrafgesetzbuch:
 - aa. Völkermord nach § 6,
 - bb. Verbrechen gegen die Menschlichkeit nach § 7,
 - cc. Kriegsverbrechen nach den §§ 8 bis 12,
 - dd. Verbrechen der Aggression nach § 13,
 - g. aus dem Waffengesetz:
 - aa. besonders schwerer Fall einer Straftat nach § 51 Absatz 1 in Verbindung mit Absatz 2,
 - bb. besonders schwerer Fall einer Straftat nach § 52 Absatz 1 Nummer 1 in Verbindung mit Absatz 5;
20. öffentlicher Verkehrsraum eine Verkehrsfläche oder Verkehrseinrichtung (z.B. Straßen, Plätze, Brücken, Fußwege, Flughäfen, Bahnhöfe, Züge, Tank- und Rastanlagen),
- a. die nach dem Wegerecht des Bundes, der Länder oder der Kommunen dem allgemeinen Verkehr gewidmet ist oder
 - b. die ohne Rücksicht auf eine Widmung und ungeachtet der Eigentumsverhältnisse entweder ausdrücklich oder mit stillschweigender Duldung der verfassungsberechtigten natürlichen oder juristischen Person für jedermann oder aber zumindest für eine allgemein bestimmte größere Personengruppe zur Benutzung zugelassen ist und auch tatsächlich so genutzt wird;
21. digitaler Raum das Internet, Intranets und sonstige elektronische Verbindungen einschließlich der mit diesen verbundenen informationstechnischen Systeme und sonstigen Geräte;
22. Wohnung jeder umschlossene Raum, der zum Wohnen oder Schlafen benutzt wird, einschließlich Wohn- und Nebenräume, Arbeits-, Betriebs- und Geschäftsräume sowie anderes befriedetes Besitztum;

23. personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;
24. Kernbereichsdaten alle dem Kernbereich privater Lebensgestaltung zuzurechnende Daten;
25. besondere Kategorien personenbezogener Daten alle Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung;
26. genetische Daten einer Person das DNA-Identifizierungsmuster, das Geschlecht, die Augen-, Haar- und Hautfarbe, das biologische Alter und die biogeographische Herkunft;
27. biometrische Daten alle mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie beispielsweise Gesichtsbilder oder daktyloskopische Daten;
28. Gesundheitsdaten alle personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;
29. Datenverarbeitung jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Daten, insbesondere die Erhebung, Erfassung, Organisation, das Ordnen, die Speicherung, Anpassung oder Veränderung, das Auslesen, Abfragen, die Auswertung, Nutzung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich, die Verknüpfung, Einschränkung, Berichtigung, Sperrung, Löschung oder die Vernichtung;
30. Pseudonymisierung die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

31. informationstechnisches System alle elektronischen datenverarbeitenden Systeme, beispielsweise Computer, Großrechner, Hochleistungsrechner, verteilte Systeme einschließlich Serversysteme, Computer-Grids und Cloud Computing, sowie Datenbanksysteme, Informationssysteme, Prozessrechner, digitale Messsysteme, DSP-Systeme, Mikrocontroller-Systeme, Kompaktregler, eingebettete Systeme, Mobiltelefone, Handgeräte, digitale Anrufbeantworter, Videokonferenzsysteme und sonstige Kommunikationssysteme sowie das Internet in seiner Gesamtheit;
32. Datei jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;
33. Behördenleitung die Polizeipräsidentin oder der Polizeipräsident, ihre oder seine Stellvertreterinnen und Stellvertreter und durch diese beauftragte Bedienstete;
34. Landesbeauftragte die oder der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht;
35. Kontakt- oder Begleitperson eine Person, die mit einer anderen
 - a. für die Gefahr nach §§ 7 oder 8 verantwortlichen oder nach § 10 notstandspflichtigen Person oder
 - b. Person, von der hinreichend sichere Anhaltspunkte die Annahme rechtfertigen, dass diese Straftaten von erheblicher Bedeutung begangen, veranlassen oder unterstützen wird oder einem schwerwiegenden Kriminalitätsphänomen zuzuordnen ist,

in einer Weise in Verbindung steht, die es erwarten lässt, dass durch sie Hinweise über die Gefahrenlage, die angenommenen Straftaten oder das Kriminalitätsphänomen gewonnen werden können; Amts- und Berufsgeheimnisträger gehören, soweit das geschützte Vertrauensverhältnis reicht, nicht zu den Kontakt- oder Begleitpersonen;
36. postdiensteanbietende Person eine natürliche oder juristische Person, die ganz oder teilweise geschäftsmäßig Post- oder Telekommunikationsdienste erbringt oder daran mitwirkt;
37. telediensteanbietende Person eine natürliche oder juristische Person, die ganz oder teilweise geschäftsmäßig Telekommunikations- oder Telemediendienste erbringt oder daran mitwirkt;
38. Vertrauensperson eine Person, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist;
39. verdeckt ermittelnde Person eine unter einer ihr verliehenen, auf Dauer angelegten Legende eingesetzte Person, die eine Polizeivollzugsbedienstete oder ein Polizeivollzugsbediensteter ist.

Allgemeine Voraussetzungen selektiver Kriminalprävention

(1) Die Polizei kann Maßnahmen zur Verhütung oder vorbeugenden Bekämpfung von Straftaten oder Kriminalitätsphänomenen ergreifen und die personenbezogenen Daten verarbeiten, soweit dies durch die Vorschriften des Kapitels 2 erlaubt ist. Die Reichweite selektiver Kriminalprävention richtet sich nach den Gefahrenbegriffen, die den jeweiligen Vorschriften zugrunde liegen.

(2) Den Maßnahmen nach Absatz 1 muss eine schriftliche operative Präventionsplanung zugrunde liegen, in der Anlass, Ziele, Mittel und Ort der jeweiligen Maßnahme vor dem Hintergrund polizeilicher Erfahrung und den Lageerkennnissen beschrieben werden. Die operative Präventionsplanung umfasst eine Gefahrenprognose sowie eine Abwägung der Verhältnismäßigkeit der Maßnahmen und die Gründe für die Ermessensausübung.

(3) Der operativen Präventionsplanung nach Absatz 2 muss ein schriftliches kriminalpräventives Handlungskonzept der Polizei zugrunde liegen, das unter der Federführung der Behördenleitung und in Abstimmung mit dem für Inneres zuständigen Mitglied der Landesregierung erstellt wurde. Kriminalpräventiven Handlungskonzepten kommt in Bezug auf die operative Präventionsplanung und die zu ergreifenden Maßnahmen eine strategische Ausrichtungs-, Eingrenzungs- und Leitfunktion zu.

(4) Maßnahmen nach Absatz 1, die diesen zugrunde liegende operative Präventionsplanung nach Absatz 2 und das dieser zugrunde liegende kriminalpräventive Handlungskonzept nach Absatz 3 sind im verwaltungsgerichtlichen Verfahren überprüfbar.

(5) Das für Inneres zuständige Mitglied der Landesregierung erstattet dem Landtag und dessen für Inneres zuständigen Ausschuss entsprechend § 41 jährlich einen Bericht über die Maßnahmen, Präventionsplanungen, Handlungskonzepte und die verwaltungsgerichtlichen Verfahren nach den Absätzen 1 bis 4.“

5. Der bisherige § 3 wird § 5 und wie folgt geändert:

a) In Absatz 1 werden die Wörter „den einzelnen“ durch die Wörter „die betroffene Person“ ersetzt.

b) In Absatz 3 wird das Wort „daß“ durch das Wort „dass“ ersetzt.

6. Der bisherige § 4 wird § 6 und in Absatz 2 Satz 2 werden die Wörter „Dem Betroffenen“ durch die Wörter „Der betroffenen Person“ ersetzt.

7. Der bisherige § 5 wird § 7 und Absatz 2 Satz 2 und 3 wie folgt gefasst:

„Ist für die Person eine Betreuerin oder ein Betreuer bestellt, so können die Maßnahmen auch gegen die Betreuerin oder den Betreuer im Rahmen ihres oder seines Aufgabenkreises gerichtet werden. Dies gilt auch, wenn der Aufgabenkreis der Betreuerin oder des Betreuers die in § 1896 Absatz 4 und § 1905 des Bürgerlichen Gesetzbuches bezeichneten Angelegenheiten nicht erfasst.“

8. Der bisherige § 6 wird § 8 und wie folgt geändert:

a) In Absatz 1 Satz 1 werden vor den Wörtern „den Inhaber“ die Wörter „die Inhaberin oder“ eingefügt.

b) Absatz 2 wird wie folgt gefasst:

„(2) Maßnahmen können auch gegen die Eigentümerin, den Eigentümer oder eine andere berechnigte Person gerichtet werden. Das gilt nicht, wenn die Inhaberin oder der Inhaber der tatsächlichen Gewalt diese ohne den Willen der Eigentümerin, des Eigentümers oder der berechtigten Person ausübt.“

c) In Absatz 3 werden die Wörter „gegen denjenigen gerichtet werden, der“ durch die Wörter „gegen eine Person gerichtet werden, die“ ersetzt.

d) In Absatz 4 wird die Angabe „§ 5 Abs. 4“ durch die Angabe „§ 7 Absatz 4“ ersetzt.

9. Nach dem neuen § 8 wird folgender § 9 eingefügt:

„§ 9

Unmittelbare Ausführung einer Maßnahme

(1) Die Polizei kann eine Maßnahme selbst oder durch beauftragte Personen ausführen, wenn der Zweck der Maßnahme durch Inanspruchnahme der nach den §§ 7 oder 8 verantwortlichen Personen nicht oder nicht rechtzeitig erreicht werden kann. Die von der Maßnahme betroffene Person ist unverzüglich zu unterrichten.

(2) Entstehen der Polizei durch die unmittelbare Ausführung einer Maßnahme Kosten, so werden diese von den nach §§ 7 oder 8 verantwortlichen Personen erhoben.“

10. Der bisherige § 7 wird § 10 und wie folgt geändert:

a) In Absatz 1 werden die Wörter „§§ 5 oder 6 Verantwortlichen“ durch die Wörter „§§ 7 oder 8 verantwortlichen Personen“ ersetzt.

b) In Absatz 3 wird die Angabe „§ 5 Abs. 4“ durch die Angabe „§ 7 Absatz 4“ ersetzt.

11. Der bisherige § 8 wird § 11 und wie folgt gefasst:

„§ 11

Einschränkung von Grundrechten

Durch dieses Gesetz werden die Grundrechte auf

1. Leben und körperliche Unversehrtheit (Artikel 2 Absatz 2 Satz 1 des Grundgesetzes, Artikel 8 Absatz 1 Satz 1 der Verfassung des Landes Brandenburg),
2. Freiheit der Person (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes, Artikel 9 Absatz 1 Satz 1 der Verfassung des Landes Brandenburg),
3. Unverletzlichkeit des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 Absatz 1 des Grundgesetzes, Artikel 16 Absatz 1 der Verfassung des Landes Brandenburg),
4. Freizügigkeit (Artikel 11 des Grundgesetzes, Artikel 17 der Verfassung des Landes Brandenburg),
5. Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes, Artikel 15 der Verfassung des Landes Brandenburg),
6. Datenschutz (Artikel 11 der Verfassung des Landes Brandenburg) und
7. Eigentum (Artikel 14 des Grundgesetzes, Artikel 41 Absatz 1 Satz 1 der Verfassung des Landes Brandenburg)

eingeschränkt.“

12. Der bisherige § 9 wird § 12 und in Absatz 1 werden die Wörter „des von einer Maßnahme Betroffenen“ durch die Wörter „der von einer Maßnahme betroffenen Person“ ersetzt.
13. Der bisherige § 10 wird § 13 und wie folgt geändert:
 - a) In der Überschrift werden das Komma und das Wort „Begriffsbestimmung“ gestrichen.
 - b) Absatz 1 wird wie folgt gefasst:

„(1) Die Polizei kann die notwendigen Maßnahmen treffen, um eine konkrete Gefahr abzuwehren, soweit nicht die §§ 14 bis 67 die Befugnisse der Polizei besonders regeln. Maßnahmen im Sinne des Satzes 1 kann die Polizei insbesondere treffen, um Straftaten, Kriminalitätsphänomene, Ordnungswidrigkeiten oder verfassungsfeindliche Handlungen zu verhüten, vorbeugend zu bekämpfen oder zu unterbinden.“
 - c) In Absatz 2 Satz 1 wird die Angabe „Abs.“ durch das Wort „Absatz“ ersetzt.
 - d) Absatz 3 wird aufgehoben.
14. Der bisherige § 11 wird § 14 und wie folgt geändert:
 - a) In Absatz 1 wird das Wort „daß“ durch das Wort „dass“ ersetzt.
 - b) Absatz 2 wird wie folgt geändert:

aa) In Satz 3 werden die Wörter „der Betroffene hierauf, sonst auf die Freiwilligkeit seiner“ durch die Wörter „die betroffene Person hierauf, sonst auf die Freiwilligkeit ihrer“ ersetzt.

bb) Folgende Sätze werden angefügt:

„Wird die Auskunft nach Satz 1 oder 2 unberechtigterweise verweigert, so kann ein Zwangsgeld festgesetzt werden. Dieses ist zuvor in bestimmter Höhe anzudrohen.“

c) Absatz 3 wird aufgehoben.

15. Der bisherige § 12 wird § 15 und wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Nummer 1 wird dem Wort „Gefahr“ das Wort „konkreten“ vorangestellt.

bb) Nummer 2 wird wie folgt gefasst:

„2. wenn sie sich an einem Ort aufhält,

a. von dem Tatsachen die Annahme rechtfertigen, dass

aa. dort Personen Straftaten verabreden, vorbereiten oder verüben,

bb. sich dort Personen treffen, die gegen aufenthaltsrechtliche Strafvorschriften verstoßen,

cc. sich dort gesuchte Straftäter verbergen oder

dd. dort Ordnungswidrigkeiten von erheblicher Bedeutung begangen werden, oder

b. an dem Personen der Prostitution nachgehen,“

cc) In Nummer 3 wird das Wort „daß“ durch das Wort „dass“ ersetzt.

dd) Nummer 4 wird wie folgt gefasst:

„4. an einer Kontrollstelle, die von der Polizei eingerichtet worden ist, um Straftaten von erheblicher Bedeutung oder nach § 27 des Versammlungsgesetzes oder schwerwiegende Kriminalitätsphänomene zu verhüten oder vorbeugend zu bekämpfen, sofern diesbezüglich zumindest eine erhöhte abstrakte Gefahr besteht,“

ee) In Nummer 5 wird das Wort „Flugplatzbereichen“ durch die Wörter „Grenz- und Flugplatzbereichen“ ersetzt.

ff) Nummer 6 wird wie folgt gefasst:

„6. im öffentlichen Verkehrsraum zur Verhütung oder vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung oder von

schwerwiegenden Kriminalitätsphänomenen, sofern diesbezüglich zumindest eine abstrakte Gefahr besteht,“

gg) In Nummer 7 wird die Angabe „Abs.“ durch das Wort „Absatz“ und der Punkt am Ende durch ein Komma ersetzt.

hh) Folgende Nummern 8 und 9 werden angefügt:

„8. wenn dies zur Leistung von Vollzugshilfe (§ 1 Absatz 3) erforderlich ist oder

9. wenn sie sich im räumlichen Umfeld einer anderen Person aufhält, die in besonderem Maße als gefährdet erscheint, und Tatsachen die Maßnahme zum Schutz der Person rechtfertigen.“

b) Absatz 2 wird wie folgt gefasst:

„(2) Die Polizei kann die zur Feststellung der Identität erforderlichen Maßnahmen treffen. Sie kann die betroffene Person insbesondere anhalten, diese nach ihren Personalien befragen und verlangen, dass diese Angaben zur Feststellung ihrer Identität macht, mitgeführte Ausweispapiere zur Prüfung aushändigt und Kleidungsstücke sowie Gegenstände, die eine Identitätsfeststellung verhindern oder erschweren, abnimmt. Die betroffene Person kann festgehalten, ihre Person sowie die von ihr mitgeführten Sachen können durchsucht und sie kann zur Dienststelle gebracht werden, wenn die Identität auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann.“

16. Der bisherige § 13 wird § 16 und wie folgt geändert:

a) Absatz 2 wird wie folgt gefasst:

„(2) Die Polizei kann erkennungsdienstliche Maßnahmen vornehmen, wenn

1. dies zur Abwehr einer konkreten Gefahr erforderlich ist,
2. eine nach § 15 zulässige Identitätsfeststellung auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist,
3. trotz einer nach § 15 getroffenen Maßnahme der Identitätsfeststellung Zweifel über die Person oder die Staatsangehörigkeit bestehen,
4. dies zur Verhütung oder vorbeugenden Bekämpfung von Straftaten oder von Kriminalitätsphänomenen erforderlich ist, weil die betroffene Person
 - a. verdächtig ist, eine Straftat begangen, veranlasst oder unterstützt zu haben, und wegen der Art und Ausführung der Tat die Gefahr der Wiederholung besteht oder
 - b. einem Kriminalitätsphänomen zugeordnet werden kann.“

b) Nach Absatz 2 wird folgender Absatz 3 eingefügt:

„(3) Sind eine Identitätsfeststellung und andere erkennungsdienstliche Maßnahmen nicht hinreichend, kann die Polizei einer betroffenen Person Körperzellen entnehmen oder DNA-Material in sonstiger Weise sicherstellen und zur Feststellung des DNA-Identifizierungsmusters und des Geschlechts der Person eine molekulargenetische Untersuchung durchführen, wenn

1. dies zur Abwehr einer erheblichen konkreten Gefahr erforderlich ist,
2. die Person vermisst wird,
3. es sich bei dieser Person um einen unbekannten Toten handelt oder
4. sich die Person erkennbar in einem die freie Willensbestimmung ausschließenden Zustand oder sich sonst in einer hilflosen Lage befindet.

Durch eine molekulargenetische Untersuchung von aufgefundenem Spurenmaterial unbekannter Herkunft dürfen genetische Daten des Spurenverursachers festgestellt werden, wenn die Abwehr einer erheblichen konkreten Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre. Ein körperlicher Eingriff darf nur von einer Ärztin oder einem Arzt vorgenommen werden. Für die Durchführung der molekulargenetischen Untersuchungen gilt § 81f Absatz 2 der Strafprozessordnung entsprechend. Die entnommenen Körperzellen und das in sonstiger Weise sichergestellte DNA-Material sind unverzüglich nach der Untersuchung zu vernichten, soweit diese nicht nach anderen Rechtsvorschriften aufbewahrt werden dürfen. Eine Maßnahme nach Satz 1 oder 2 darf nur durch die Richterin oder den Richter angeordnet werden, bei Gefahr im Verzug auch durch die Behördenleitung; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen. Zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.“

- c) Die bisherigen Absätze 3 und 4 werden die Absätze 4 und 5 und wie folgt gefasst:

„(4) Für Maßnahmen nach den Absätzen 2 und 3 gilt § 15 Absatz 2 Satz 3 entsprechend. Die Daten der erkennungsdienstlichen Unterlagen und die genetischen Daten können zum Zweck des Abgleichs in einer Datei gespeichert und ausschließlich für die Gefahrenabwehr verwendet werden. Die erkennungsdienstlichen Unterlagen, die genetischen Daten und die angelegte Datei sind unverzüglich zu vernichten und zu löschen, wenn die Voraussetzungen nach Absatz 2 oder 3 entfallen sind.

(5) Die betroffene Person ist bei Vornahme einer Maßnahme nach Absatz 2 oder 3 darüber zu belehren, dass sie die Vernichtung und Löschung der erkennungsdienstlichen Unterlagen, der genetischen Daten und der angelegten Datei verlangen kann, wenn die Voraussetzungen für ihre weitere Aufbewahrung entfallen sind. Sind die erkennungsdienstlichen Unterlagen, die genetischen Daten und die angelegte Datei ohne Wissen der betroffenen Person angefertigt worden, ist ihr mitzuteilen, welche Unterlagen und

Daten aufbewahrt werden, sobald dies ohne Gefährdung des Zwecks der Maßnahme geschehen kann.“

17. Der bisherige § 14 wird § 17 und wie folgt gefasst:

„§ 17

Prüfung von Berechtigungsscheinen und sonstigen Urkunden

Die Polizei kann verlangen, dass Berechtigungsscheine, Bescheinigungen, Nachweise oder sonstige Urkunden zur Prüfung ausgehändigt werden, wenn die betroffene Person aufgrund einer Rechtsvorschrift oder einer vollziehbaren Auflage in einem Erlaubnisbescheid verpflichtet ist, diese mitzuführen. Die betroffene Person kann für die Dauer der Maßnahme angehalten werden.“

18. Der bisherige § 15 wird § 18 und wie folgt geändert:

- a) In Absatz 1 Nummer 1 und Absatz 3 Satz 2 wird jeweils das Wort „daß“ durch das Wort „dass“ ersetzt.
- b) In Absatz 1 Nummer 2 werden nach den Wörtern „erkennungsdienstlicher Maßnahmen“ die Wörter „oder einer elektronischen Aufenthaltsüberwachung“ eingefügt.
- c) In Absatz 2 Satz 2 werden die Wörter „des Betroffenen“ durch die Wörter „der betroffenen Person“ ersetzt.
- d) Absatz 3 Satz 1 wird wie folgt geändert:
 - aa) In dem Satzteil vor Nummer 1 werden die Wörter „ein Betroffener“ durch die Wörter „eine betroffene Person“ ersetzt.
 - bb) In Nummer 1 werden die Wörter „Gefahr für Leib, Leben oder Freiheit einer Person“ durch die Wörter „konkreten Gefahr“ ersetzt.
 - cc) In Nummer 2 werden nach den Wörtern „erkennungsdienstlicher Maßnahmen“ die Wörter „oder einer elektronischen Aufenthaltsüberwachung“ eingefügt.

19. Die bisherigen §§ 16 und 16a werden durch die folgenden §§ 19 und 20 ersetzt:

„§ 19

Meldeauflage

(1) Die Polizei kann gegenüber einer Person anordnen, sich an bestimmten Tagen zu bestimmten Zeiten bei einer bestimmten Dienststelle zu melden (Meldeauflage)

- 1. zur Abwehr einer konkreten Gefahr oder

2. zur Verhütung oder vorbeugenden Bekämpfung von Ordnungswidrigkeiten von erheblicher Bedeutung, Straftaten oder Kriminalitätsphänomenen.

(2) Die Meldeauflage ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Anordnungsvoraussetzungen weiterhin vorliegen. Die Verlängerung darf nur durch die RichterIn oder den Richter angeordnet werden, bei Gefahr im Verzug auch durch die Behördenleitung; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen. Zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Bestimmungen des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Sobald die Anordnungsvoraussetzungen weggefallen sind, ist die Maßnahme unverzüglich zu beenden und das anordnende Gericht davon zu unterrichten.

§ 20

Platzverweisung, Kontaktverbot, Aufenthaltsanordnung und Wohnungsaufenthaltsverbot

(1) Die Polizei kann eine Person vorübergehend von einem Ort verweisen oder ihr vorübergehend das Betreten eines Ortes verbieten (Platzverweisung)

1. zur Abwehr einer konkreten Gefahr oder
2. zur Verhütung oder vorbeugenden Bekämpfung von Ordnungswidrigkeiten, Straftaten oder Kriminalitätsphänomenen.

Die Platzverweisung kann ferner gegen Personen angeordnet werden, die den Einsatz der Feuerwehr oder von Hilfs- oder Rettungsdiensten behindern.

(2) Die Polizei kann zur Abwehr einer konkreten Gefahr oder zur Verhütung oder vorbeugenden Bekämpfung von Straftaten oder von Kriminalitätsphänomenen einer Person untersagen,

1. zu bestimmten Personen oder zu Personen einer bestimmten Gruppe Kontakt zu suchen oder aufzunehmen (Kontaktverbot),
2. bestimmte Orte oder ein bestimmtes Gebiet zu betreten (Aufenthaltsverbot) oder
3. ihren Wohn- oder Aufenthaltsort oder ein bestimmtes Gebiet zu verlassen (Aufenthaltsgebot).

Die betroffene Person ist verpflichtet, der Polizei zum Zwecke der Zustellung der Anordnungen unverzüglich eine Anschrift oder eine zustellungsbevollmächtigte Person zu benennen. Die Polizei übermittelt diese Angaben an gefährdete Personen. Die Wahrnehmung berechtigter Interessen der betroffenen Person und Dritter ist zu berücksichtigen. Die Anordnungen nach Satz 1 dürfen die Dauer von drei Monaten nicht überschreiten und können um jeweils längstens einen Monat verlängert werden. Die Vorschriften des Versammlungsrechts bleiben unberührt.

(3) Die Polizei kann einer Person zur Abwehr einer von dieser ausgehenden erheblichen konkreten Gefahr untersagen, eine Wohnung oder bestimmte Wohn- und Nebenräume zu betreten (Wohnungsaufenthaltsverbot). Absatz 2 Satz 2 bis 4 gelten entsprechend. Die Anordnungen nach Satz 1 dürfen die Dauer von einem Monat nicht überschreiten. Stellt die gefährdete Person während der Dauer des Wohnungsaufenthaltsverbots einen Antrag auf zivilrechtlichen Schutz vor Gewalt oder Nachstellungen mit dem Ziel des Erlasses einer einstweiligen Anordnung, endet das Wohnungsaufenthaltsverbot mit dem Tag der gerichtlichen Entscheidung, spätestens jedoch mit Ablauf der festgelegten Frist. Das Gericht hat der Polizei die Beantragung zivilrechtlichen Schutzes sowie die gerichtliche Entscheidung unverzüglich mitzuteilen; die §§ 18 bis 22 des Einführungsgesetzes zum Gerichtsverfassungsgesetz bleiben unberührt. Die Polizei hat gefährdete Personen und die betroffene Person unverzüglich über die Dauer des Wohnungsaufenthaltsverbots in Kenntnis zu setzen.“

20. Der bisherige § 17 wird § 21 und Absatz 1 wie folgt gefasst:

„(1) Die Polizei kann eine Person in Gewahrsam nehmen, wenn dies unerlässlich ist

1. zum Schutz der Person gegen eine konkrete Gefahr für Leib oder Leben, insbesondere weil die Person sich erkennbar in einem die freie Willensbestimmung ausschließenden Zustand oder sonst in hilfloser Lage befindet,
2. zur Verhinderung der unmittelbar bevorstehenden Begehung oder Fortsetzung einer Straftat oder einer Ordnungswidrigkeit von erheblicher Bedeutung; die Annahme, dass eine Person eine solche Tat begehen oder zu ihrer Begehung beitragen wird, kann sich insbesondere darauf stützen, dass
 - a. sie die Begehung der Tat angekündigt oder dazu aufgefordert hat oder entsprechende Transparente oder sonstige Gegenstände mit sich führt; dies gilt auch für Flugblätter solchen Inhalts, soweit sie in einer Menge mitgeführt werden, die zur Verteilung geeignet ist,
 - b. bei ihr Waffen, Werkzeuge oder sonstige Gegenstände aufgefunden werden, die ersichtlich zur Tatbegehung bestimmt sind oder erfahrungsgemäß bei derartigen Taten verwendet werden, oder ihre Begleitperson solche Gegenstände mit sich führt und sie den Umständen nach hiervon Kenntnis haben musste oder
 - c. sie bereits in der Vergangenheit aus vergleichbarem Anlass bei der Begehung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung als Störer betroffen worden und nach den Umständen eine Wiederholung dieser Verhaltensweise zu erwarten ist,
3. zur Durchsetzung von Maßnahmen und Anordnungen nach den §§ 19, 20 und 45,
4. zur Abwehr einer erheblichen konkreten Gefahr oder
5. zum Schutz privater Rechte, wenn eine Festnahme und Vorführung der Personen nach den §§ 229, 230 Absatz 3 des Bürgerlichen Gesetzbuches zulässig ist.“

21. Der bisherige § 18 wird § 22 und wie folgt geändert:

- a) Absatz 1 wird wie folgt geändert:
 - aa) In Satz 1 werden die Wörter „§ 12 Abs. 2 Satz 3, § 15 Abs. 3 oder § 17“ durch die Wörter „§ 15 Absatz 2 Satz 3, § 16 Absatz 4 Satz 1, § 18 Absatz 3 oder § 21“ ersetzt.
 - bb) In Satz 2 werden die Wörter „daß die Entscheidung des Richters und die Anhörung durch den Richter“ durch die Wörter „dass die Entscheidung der Richterin oder des Richters und die Anhörung durch die Richterin oder den Richter“ ersetzt.
- b) In Absatz 2 Satz 2 wird nach den Wörtern „freiwilligen Gerichtsbarkeit“ das Wort „entsprechend“ eingefügt.

22. Der bisherige § 19 wird § 23 und wie folgt geändert:

- a) In Absatz 1 Satz 1 werden die Wörter „§ 12 Abs. 2 Satz 3, § 15 Abs. 3 oder § 17“ durch die Wörter „§ 15 Absatz 2 Satz 3, § 16 Absatz 4 Satz 1, § 18 Absatz 3 oder § 21“ ersetzt.
- b) In Absatz 2 Satz 4 werden den Wörtern „ein Betreuer“ die Wörter „eine Betreuerin oder“ vorangestellt und die Wörter „derjenige zu benachrichtigen, dem“ durch die Wörter „diejenige Person zu benachrichtigen, der“ ersetzt.
- c) In Absatz 4 werden die Wörter „der Betroffene“ durch die Wörter „die betroffene Person“ ersetzt.

23. Der bisherige § 20 wird § 24 und Absatz 1 wie folgt gefasst:

- „(1) Die festgehaltene Person ist zu entlassen,
1. sobald der Grund für die Maßnahme der Polizei weggefallen ist,
 2. wenn die Fortdauer der Freiheitsentziehung durch richterliche Entscheidung für unzulässig erklärt wird oder
 3. in jedem Fall spätestens bis zum Ende des Tages nach dem Ergreifen, wenn nicht vorher die Fortdauer der Freiheitsentziehung aufgrund dieses oder eines anderen Gesetzes durch richterliche Entscheidung angeordnet ist. In der Entscheidung ist die Dauer der Freiheitsentziehung zu bestimmen. Sie darf nicht mehr als einen Monat betragen und kann jeweils um längstens einen Monat verlängert werden.“

24. Der bisherige § 21 wird § 25 und wie folgt geändert:

- a) Absatz 1 wird wie folgt geändert:
 - aa) In dem Satzteil vor Nummer 1 wird die Angabe „§ 12 Abs. 2 Satz 4“ durch die Wörter „§ 15 Absatz 2 Satz 3“ ersetzt.
 - bb) In Nummer 1 werden nach den Wörtern „festgehalten werden kann“ ein Komma sowie die Wörter „im Falle des § 15 Absatz 1 Nummer 4

oder 6 bereits bei Bestehen einer erhöhten abstrakten Gefahr“ eingefügt.

- cc) In Nummer 2 wird das Wort „daß“ durch das Wort „dass“ ersetzt.
- dd) In Nummer 4 wird die Angabe „§ 12 Abs. 1 Nr. 2“ durch die Wörter „§ 15 Absatz 1 Nummer 2“ ersetzt.
- ee) In Nummer 5 wird die Angabe „§ 12 Abs. 1 Nr. 3“ durch die Wörter „§ 15 Absatz 1 Nummer 3“, das Wort „daß“ durch das Wort „dass“ und das Wort „oder“ am Ende durch ein Komma ersetzt.
- ff) Nach Nummer 5 wird folgende Nummer 6 eingefügt:

„6. eine konkrete Gefahr vorliegt oder“.
- gg) Die bisherige Nummer 6 wird Nummer 7.
- b) In Absatz 2 Satz 1 und Absatz 3 wird jeweils dem Wort „Gefahr“ das Wort „konkrete“ vorangestellt.

25. Der bisherige § 22 wird § 26 und wie folgt geändert:

- a) Absatz 1 wird wie folgt geändert:
 - aa) In dem Satzteil vor Nummer 1 wird die Angabe „§ 12 Abs. 2 Satz 4“ durch die Wörter „§ 15 Absatz 2 Satz 3“ ersetzt.
 - bb) In Nummer 1 wird die Angabe „§ 21“ durch die Angabe „§ 25“ ersetzt.
 - cc) In den Nummern 2 und 3 wird jeweils das Wort „daß“ durch das Wort „dass“ ersetzt.
 - dd) In Nummer 4 wird die Angabe „§ 12 Abs. 1 Nr. 2“ durch die Wörter „§ 15 Absatz 1 Nummer 2“ ersetzt.
 - ee) In Nummer 5 wird die Angabe „§ 12 Abs. 1 Nr. 3“ durch die Wörter „§ 15 Absatz 1 Nummer 3“ und das Wort „daß“ durch das Wort „dass“ ersetzt.
 - ff) Nummer 6 wird wie folgt gefasst:

„6. es sich um ein Land-, Wasser- oder Luftfahrzeug handelt, in dem sich eine Person befindet, deren Identität nach § 15 Absatz 1 Nummer 4 oder 6 festgestellt werden darf, bereits bei Bestehen einer erhöhten abstrakten Gefahr; die Durchsuchung kann sich auch auf die in dem Fahrzeug enthaltenen oder die mit diesem in einem räumlichen Zusammenhang stehenden Sachen erstrecken.“
- b) Nach Absatz 1 wird folgender Absatz 2 eingefügt:

„(2) Betrifft die Durchsuchung ein elektronisches Speichermedium, können auch vom Durchsuchungsobjekt räumlich getrennte Speichermedien durchsucht werden, soweit von diesem aus auf sie zugegriffen werden

kann. Personenbezogene Daten dürfen darüber hinaus nur dann weiterverarbeitet werden, wenn dies gesetzlich zugelassen ist.“

- c) Der bisherige Absatz 2 wird Absatz 3 und wie folgt geändert:
 - aa) In Satz 1 werden den Wörtern „der Inhaber“ die Wörter „die Inhaberin oder“ vorangestellt.
 - bb) Satz 2 wird wie folgt gefasst:

„Ist sie oder er abwesend, so soll ihre oder seine Vertreterperson oder eine andere Zeugenperson hinzugezogen werden.“
 - cc) In Satz 3 wird das Wort „Dem“ durch die Wörter „Der Inhaberin oder dem“ ersetzt.

26. Der bisherige § 23 wird § 27 und wie folgt geändert:

- a) In Absatz 1 Satz 1 Nummer 1 und 2 und Absatz 3 Nummer 1 wird jeweils das Wort „daß“ durch das Wort „dass“ ersetzt.
- b) Absatz 1 wird wie folgt geändert:
 - aa) Satz 1 wird wie folgt geändert:
 - aaa) In dem Satzteil vor Nummer 1 werden den Wörtern „des Inhabers“ die Wörter „der Inhaberin oder“ vorangestellt.
 - bbb) In Nummer 1 wird die Angabe „§ 15 Abs. 3“ durch die Angabe „§ 18 Absatz 3“ und die Angabe „§ 17“ durch die Angabe „§ 21“ ersetzt.
 - ccc) In Nummer 2 wird die Angabe „§ 25 Nr. 1“ durch die Wörter „§ 29 Absatz 1 Nummer 1 und 2“ ersetzt.
 - ddd) In Nummer 3 wird am Ende das Wort „oder“ gestrichen.
 - eee) In Nummer 4 werden die Wörter „gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person oder für Sachen von bedeutendem Wert“ durch die Wörter „erheblichen konkreten Gefahr“ und der Punkt am Ende durch das Wort „oder“ ersetzt.
 - fff) Folgende Nummer 5 wird angefügt:

„5. dies zur Durchführung eines Eingriffs in informationstechnische Systeme nach § 49 Absatz 2 erforderlich ist.“
 - bb) Satz 2 wird aufgehoben.
- c) In Absatz 2 werden die Angabe „Abs.“ durch das Wort „Absatz“ und die Wörter „Absatzes 1 Satz 1 Nr. 3 und 4“ durch die Wörter „Absatzes 1 Nummer 3 und zur Abwehr einer dringenden konkreten Gefahr“ ersetzt.
- d) Absatz 3 wird wie folgt geändert:

- aa) In dem Satzteil vor Nummer 1 wird dem Wort „Gefahren“ das Wort „konkreter“ vorangestellt.
- bb) In Nummer 1 Buchstabe a wird die Angabe „(§ 10 Abs. 3 Satz 1)“ gestrichen.
- cc) In Nummer 2 werden den Wörtern „der Prostitution“ die Wörter „einem schwerwiegenden Kriminalitätsphänomen oder“ vorangestellt.
- e) In Absatz 4 wird die Angabe „Abs.“ durch das Wort „Absatz“ ersetzt.

27. Der bisherige § 24 wird § 28 und wie folgt geändert:

- a) In Absatz 1 Satz 1 werden nach dem Wort „Durchsuchungen“ die Wörter „von Wohnungen“ eingefügt und den Wörtern „den Richter“ die Wörter „die Richterinnen oder“ vorangestellt.
- b) Absatz 2 wird wie folgt geändert:
 - aa) In Satz 1 werden den Wörtern „der Wohnungsinhaber“ die Wörter „die Wohnungsinhaberin oder“ vorangestellt.
 - bb) Satz 2 wird wie folgt gefasst:

„Ist sie oder er abwesend, so ist, wenn möglich, ihre oder seine Vertreterperson, eine erwachsene Angehörigenperson, eine Mitbewohnerin oder ein Mitbewohner oder eine Nachbarin oder ein Nachbar zuzuziehen.“
 - cc) Folgender Satz wird angefügt:

„Das Anwesenheitsrecht gilt nicht in den Fällen des § 27 Absatz 1 Satz 1 Nummer 5.“
- c) In Absatz 3 werden die Wörter „Dem Wohnungsinhaber oder seinem Vertreter“ durch die Wörter „Der Wohnungsinhaberin, dem Wohnungsinhaber oder der Vertreterperson“ ersetzt.
- d) Absatz 4 wird wie folgt geändert:
 - aa) In Satz 3 werden die Wörter „einem durchsuchenden Beamten und dem Wohnungsinhaber“ durch die Wörter „einer oder einem durchsuchenden Bediensteten und der Wohnungsinhaberin oder dem Wohnungsinhaber“ ersetzt.
 - bb) In Satz 5 werden die Wörter „Dem Wohnungsinhaber oder seinem Vertreter“ durch die Wörter „Der Wohnungsinhaberin, dem Wohnungsinhaber oder der Vertreterperson“ ersetzt.
- e) In Absatz 5 werden die Wörter „dem Betroffenen“ durch die Wörter „der betroffenen Person“ ersetzt.
- f) In Absatz 6 werden die Wörter „Der Wohnungsinhaber ist darüber zu belehren, daß er“ durch die Wörter „Die Wohnungsinhaberin oder der Wohnungsinhaber ist darüber zu belehren, dass sie oder er“ ersetzt.

28. Der bisherige § 25 wird § 29 und wie folgt geändert:

a) Der Wortlaut wird Absatz 1 und wie folgt geändert:

aa) Nummer 1 wird wie folgt gefasst:

„1. zur Abwehr einer gegenwärtigen oder erheblichen konkreten Gefahr,“

bb) Nach Nummer 1 wird die folgende Nummer 2 eingefügt:

„2. zur Verhütung oder vorbeugenden Bekämpfung von Straftaten, Ordnungswidrigkeiten oder Kriminalitätsphänomenen, wenn Tatsachen die Annahme rechtfertigen, dass sie

a. zur Begehung, Veranlassung oder Unterstützung von Straftaten oder Ordnungswidrigkeiten oder

b. für ein Kriminalitätsphänomen gebraucht oder verwertet werden soll,“

cc) Die bisherige Nummer 2 wird Nummer 3 und die Wörter „den Eigentümer oder den rechtmäßigen Inhaber“ werden durch die Wörter „die Eigentümerin oder den Eigentümer oder die rechtmäßige Inhaberin oder den rechtmäßigen Inhaber“ ersetzt.

dd) Die bisherige Nummer 3 wird Nummer 4 und in Buchstabe d werden den Wörtern „die Flucht“ die Wörter „sich oder anderen“ vorangestellt.

b) Folgende Absätze 2 und 3 werden angefügt:

„(2) Unter den Voraussetzungen des Absatzes 1 kann die Polizei durch Pfändung eine Forderung sowie sonstige Vermögensrechte sicherstellen. Die Vorschriften der Zivilprozessordnung über die Zwangsvollstreckung in Forderungen und andere Vermögensrechte sind sinngemäß anzuwenden.

(3) Unter den Voraussetzungen des Absatzes 1 kann die Polizei auch Daten sicherstellen und erforderlichenfalls den weiteren Zugriff auf diese ausschließen, wenn andernfalls

1. die Abwehr der gegenwärtigen oder erheblichen konkreten Gefahr,
2. die Verhütung oder vorbeugende Bekämpfung von Straftaten, Ordnungswidrigkeiten oder Kriminalitätsphänomenen,
3. der Schutz vor Verlust oder
4. die Verhinderung der Verwendung

aussichtslos oder wesentlich erschwert wäre. § 26 Absatz 2 Satz 1 und § 34 gelten entsprechend. Die Daten sind besonders zu kennzeichnen. Daten, die nach diesen Vorschriften nicht weiterverarbeitet werden dürfen, sind zu löschen, soweit es sich nicht um Daten handelt, die zusammen mit dem Datenträger sichergestellt wurden, auf dem sie gespeichert sind; Lö-

sungen sind zu dokumentieren. Die Bestimmungen in den §§ 30, 31 Absatz 4 und § 32 Absatz 1 hinsichtlich Verwahrung, Benachrichtigung, Vernichtung und Herausgabe gelten unter Berücksichtigung der unkörperlichen Natur von Daten sinngemäß.“

29. Der bisherige § 26 wird § 30 und wie folgt geändert:

- a) In Absatz 1 Satz 2 wird das Wort „Läßt“ durch das Wort „Lässt“ ersetzt.
- b) Absatz 2 wird wie folgt geändert:
 - aa) In den Sätzen 1 und 2 wird jeweils das Wort „läßt“ durch das Wort „lässt“ ersetzt.
 - bb) In Satz 1 werden die Wörter „Dem Betroffenen“ durch die Wörter „Der betroffenen Person“ ersetzt.
 - cc) In Satz 3 werden die Wörter „Der Eigentümer oder der rechtmäßige Inhaber“ durch die Wörter „Die Eigentümerin oder der Eigentümer oder die rechtmäßige Inhaberin oder der rechtmäßige Inhaber“ ersetzt.
- c) In Absatz 3 Satz 2 werden die Wörter „eines Berechtigten“ durch die Wörter „einer berechtigten Person“ ersetzt.
- d) In Absatz 4 wird das Wort „daß“ durch das Wort „dass“ ersetzt.

30. Der bisherige § 27 wird § 31 und wie folgt geändert:

- a) Absatz 1 wird wie folgt geändert:
 - aa) In den Nummern 3 bis 5 wird jeweils das Wort „daß“ durch das Wort „dass“ ersetzt.
 - bb) In Nummer 3 werden die Wörter „weitere Gefahren für die öffentliche Sicherheit“ durch die Wörter „weitere konkrete Gefahren“ ersetzt.
 - cc) In Nummer 4 werden die Wörter „einen Berechtigten“ durch die Wörter „eine berechtigte Person“ ersetzt.
 - dd) In Nummer 5 werden die Wörter „der Berechtigte“ durch die Wörter „die berechtigte Person“ und das Wort „ihm“ durch das Wort „ihr“ ersetzt.
- b) In Absatz 2 Satz 1 werden die Wörter „Der Betroffene, der Eigentümer“ durch die Wörter „Die betroffene Person, die Eigentümerin oder der Eigentümer“ ersetzt.
- c) Absatz 3 wird wie folgt geändert:
 - aa) In Satz 1 wird die Angabe „§ 979 Abs. 1“ durch die Wörter „§ 979 Absatz 1 bis 1 Buchstabe b“ ersetzt.

bb) In Satz 4 wird das Wort „Lässt“ durch das Wort „Lässt“ ersetzt und den Wörtern „kein Käufer“ werden die Wörter „keine Käuferin oder“ vorangestellt.

cc) Folgende Sätze werden angefügt:

„Bei der Verwertung von Datenträgern ist sicherzustellen, dass zuvor personenbezogene Daten dem Stand der Technik entsprechend gelöscht wurden. Ein Zuschlag bei der öffentlichen oder der im Internet allgemein zugänglichen Versteigerung, der freihändige Verkauf oder die Zuführung zu einem gemeinnützigen Zweck, durch die die Voraussetzungen der Sicherstellung erneut eintreten würden, ist zu versagen.“

d) In Absatz 4 Satz 1 werden nach den Wörtern „unbrauchbar gemacht“ ein Komma sowie das Wort „eingezogen“ eingefügt.

31. Der bisherige § 28 wird § 32 und wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Satz 1 werden die Wörter „denjenigen herauszugeben, bei dem“ durch die Wörter „diejenige Person herauszugeben, bei der“ ersetzt.

bb) In Satz 2 werden die Wörter „ihn nicht möglich, können sie an einen anderen herausgegeben werden, der seine“ durch die Wörter „diese nicht möglich, können sie an eine andere Person herausgegeben werden, die ihre“ ersetzt.

b) Nach Absatz 1 wird folgender Absatz 2 eingefügt:

„(2) Die Sicherstellung im Sinne des § 29 Absatz 2 darf nicht länger als ein Jahr aufrechterhalten werden. Kann das Vermögensrecht nicht freigegeben werden, ohne dass die Voraussetzungen der Sicherstellung erneut eintreten, kann die Sicherstellung mit gerichtlicher Zustimmung um jeweils ein weiteres Jahr verlängert werden.“

c) Der bisherige Absatz 2 wird Absatz 3 und in Satz 2 werden die Wörter „ein Berechtigter“ durch die Wörter „eine berechtigte Person“ ersetzt.

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

aa) In Satz 1 werden die Wörter „und Verwahrung fallen den nach den §§ 5 oder 6 Verantwortlichen“ durch ein Komma sowie die Wörter „Verwahrung, Verwertung, Unbrauchbarmachung, Einziehung und Vernichtung fallen den nach den §§ 7 oder 8 verantwortlichen Personen“ ersetzt.

bb) In Satz 2 wird die Angabe „§ 25 Nr. 2“ durch die Angabe „§ 29 Absatz 1 Nummer 3“ ersetzt.

cc) In Satz 3 wird das Wort „Verantwortliche“ durch die Wörter „verantwortliche Personen“ ersetzt.

e) Der bisherige Absatz 4 wird Absatz 5.

32. Kapitel 2 Abschnitt 2 wird wie folgt gefasst:

„Abschnitt 2 Datenverarbeitung

Unterabschnitt 1

Allgemeine Vorschriften zur Datenverarbeitung und zum Datenschutz

§ 33

Grundsätze der Datenverarbeitung

(1) Vorbehaltlich abweichender Regelungen gelten die Vorschriften dieses Abschnitts für alle Datenverarbeitungen der Polizei nach diesem Gesetz, unabhängig davon, ob diese in Akten, Dateien oder anderer Form erfolgen. Die Polizei darf personenbezogene Daten nur verarbeiten, soweit dies durch dieses Gesetz oder andere Rechtsvorschriften über die Datenverarbeitung der Polizei zugelassen ist.

(2) Personenbezogene Daten

1. werden auf rechtmäßige Weise und nach Treu und Glauben verarbeitet, soweit dies für die Erfüllung einer Aufgabe nach § 1 erforderlich ist oder bei nicht gefahren- oder tatbezogenen Merkmalen sowie über Erkrankungen oder besondere Verhaltensweisen der betroffenen Person nur für Identifizierungszwecke oder zum Schutz der betroffenen Person, von Polizeivollzugsbediensteten oder Dritten,
2. werden für festgelegte, eindeutige oder zumindest bestimmbar und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet,
3. entsprechen dem Verarbeitungszweck und sind diesbezüglich maßgeblich und nicht übermäßig,
4. sind sachlich richtig und erforderlichenfalls auf dem neuesten Stand; dies ist durch Berichtigung, Vervollständigung oder Löschung unrichtiger oder unvollständiger Daten unverzüglich sicherzustellen, wobei die Qualität der personenbezogenen Daten, soweit durchführbar und zumutbar durch die Polizeibehörde überprüft werden soll,
5. werden nicht länger als für den Verarbeitungszweck erforderlich, in einer Form gespeichert, die die Identifizierung der betroffenen Personen ermöglicht,
6. werden in einer Weise verarbeitet, die eine angemessene Sicherheit der personenbezogenen Daten durch geeignete technische und organisatorische Maßnahmen gewährleistet, einschließlich des Schutzes vor unbefug-

ter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust sowie unbeabsichtigter Zerstörung oder Schädigung.

Die Einhaltung der Grundsätze in Satz 1 muss nachgewiesen werden können.

(3) Bei einer Datenverarbeitung im Zusammenhang mit einer begangenen oder drohenden Straftat soll, soweit dies möglich ist, unterschieden werden, ob personenbezogene Daten

1. verdächtige Personen,
2. verurteilte Personen,
3. Opfer oder
4. andere Personen

betreffen.

(4) Soweit möglich soll erkennbar werden, ob personenbezogene Daten auf Tatsachen oder persönlichen Einschätzungen beruhen.

(5) Die Polizei darf folgende Grunddaten einer Person stets verarbeiten, um die Identität der Person festzustellen: Familiennamen, Vornamen, Geburtsnamen, sonstige Namen und andere Namensschreibweisen, Geschlecht, Geburtsdatum, Geburtsort, Geburtsstaat, derzeitige und frühere Staatsangehörigkeiten, gegenwärtige und frühere Aufenthaltsorte, Wohnanschrift sowie Sterbedatum.

(6) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist zulässig,

1. soweit andernfalls die Erfüllung polizeilicher Aufgaben, insbesondere die Verhütung, vorbeugende Bekämpfung oder Unterbindung von Straftaten, Ordnungswidrigkeiten von erheblicher Bedeutung oder Kriminalitätsphänomenen, gefährdet oder wesentlich erschwert wird,
2. zur Abwehr von konkreten Gefahren,
3. wenn die betroffene Person der Datenverarbeitung schriftlich zugestimmt hat und die Daten nur für den Zweck verarbeitet werden, zu dem die Zustimmung erteilt wurde; vor Erteilung der Zustimmung ist die betroffene Person über den Zweck der Verarbeitung sowie darüber aufzuklären, dass sie die Zustimmung verweigern sowie jederzeit widerrufen kann,
4. wenn die betroffene Person sie bereits offensichtlich öffentlich gemacht hat oder
5. wenn dies zu Zwecken der Eigensicherung oder des Schutzes Dritter erforderlich ist.

Solche Daten sollen besonders gekennzeichnet und der Zugriff darauf besonders ausgestaltet werden, wenn und soweit dies der Schutz der betroffenen Person erfordert.

(7) Der Einsatz von Systemen der automatischen Datenverarbeitung zur automatisierten Entscheidungsfindung, an den sich eine nachteilige Rechtsfolge für die betroffene Person knüpft oder der diese erheblich beeinträchtigt, kann durch Regelungen in diesem Gesetz erlaubt werden, wenn die Entscheidung durch den zuständigen Entscheidungsträger überprüft und im Rahmen einer umfassenden und schriftlich zu dokumentierenden Abwägung die Rechte und Freiheiten der betroffenen Person hinreichend berücksichtigt werden. Bei Gefahr im Verzug kann zunächst eine dokumentierte summarische Abwägung vorgenommen werden; die Abwägung nach Satz 1 wird unverzüglich nachgeholt.

§ 34

Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung

(1) Ist oder wird bei Maßnahmen der Datenverarbeitung erkennbar, dass in ein durch ein Berufsgeheimnis nach den §§ 53, 53a der Strafprozessordnung geschütztes Vertrauensverhältnis eingegriffen wird, ist die Datenverarbeitung insoweit unzulässig, es sei denn, die Maßnahmen richten sich gegen den Berufsgeheimnisträger selbst oder in diesem Gesetz werden abweichende Regelungen getroffen. Eine bereits laufende Datenverarbeitung ist unverzüglich und solange erforderlich zu unterbrechen oder zu beenden. Erlangte Erkenntnisse dürfen nicht weiter verarbeitet werden.

(2) Ist oder wird bei Maßnahmen der Datenverarbeitung erkennbar, dass Kernbereichsdaten betroffen sind und bestehen keine Anhaltspunkte dafür, dass diese Daten dazu dienen sollen, ein Verarbeitungsverbot herbeizuführen, ist die Datenverarbeitung unzulässig. Eine bereits laufende Datenverarbeitung ist unverzüglich oder zu einem Zeitpunkt, zu dem dies ohne Gefährdung einer eingesetzten verdeckt ermittelnden Person oder Vertrauensperson möglich ist, zu unterbrechen oder zu beenden. Dennoch erlangte Kernbereichsdaten dürfen nicht weiter verarbeitet werden. Vor der weiteren Verarbeitung der Daten erfolgt zur Aussonderung der Kernbereichsdaten eine Überprüfung durch das die Maßnahme anordnende Gericht, anderenfalls durch das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Eine unterbrochene Maßnahme darf in der Regel fortgeführt werden, wenn Kernbereichsdaten nicht mehr erfasst werden, begründete Zweifel bestehen, dass Kernbereichsdaten überhaupt betroffen sind, oder tatsächliche Anhaltspunkte vorliegen, dass die Kernbereichsdaten einen unmittelbaren Bezug zu einer dringenden konkreten Gefahr haben; andernfalls ist unverzüglich eine Entscheidung des zuständigen Gerichts herbeizuführen. Äußerungen in Betriebs- und Geschäftsräumen zählen in der Regel nicht zum Kernbereich privater Lebensgestaltung. In Wohnungen sind insbesondere die Art der zu überwachenden Räumlichkeiten und das Verhältnis der zu überwachenden Personen zueinander zu berücksichtigen.

(3) Daten nach den Absätzen 1 und 2, die nicht verarbeitet werden dürfen, sind unverzüglich zu löschen, es sei denn, dass diese zu Zwecken der Benachrichtigung der betroffenen Person oder zur gerichtlichen Überprüfung benötigt werden. Die Löschung ist in einer Weise zu protokollieren, die eine spätere Überprüfung ermöglicht. Die Protokolldaten dürfen nur verwendet werden,

um der betroffenen Person, einer dazu befugten öffentlichen Stelle oder einem Gericht die Prüfung zu ermöglichen, ob die Maßnahme rechtmäßig durchgeführt worden ist.

§ 35

Benachrichtigungspflichten

(1) Bei Maßnahmen der Verarbeitung personenbezogener Daten ohne Kenntnis der betroffenen Person ist diese durch die Polizei unverzüglich zu benachrichtigen, sobald dies ohne Gefährdung des Zwecks der Maßnahme, der eingesetzten Polizeivollzugsbediensteten, verdeckt ermittelnden Personen oder Vertrauenspersonen oder der in der jeweiligen Befugnisnorm genannten Rechtsgüter geschehen kann. Die Benachrichtigung einer betroffenen Person kann unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen wurde. Nachforschungen zur Feststellung der Identität oder des Aufenthaltsortes einer betroffenen Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist. Ist eine betroffene Person minderjährig, treten die Personensorgeberechtigten an ihre Stelle. Von ihrer Benachrichtigung kann abgesehen werden, solange zu besorgen ist, dass diese zu erheblichen Nachteilen für die minderjährige Person führt. An der Datenverarbeitung beteiligte Dritte können durch die Polizei benachrichtigt werden. Die Benachrichtigung Dritter unterbleibt, soweit überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen.

(2) Die Benachrichtigung enthält zumindest

1. die Zwecke der Verarbeitung personenbezogener Daten,
2. den Namen und die Kontaktdaten der erhebenden Stelle und der oder des behördlichen Datenschutzbeauftragten,
3. das Recht, sich an die oder den Landesbeauftragten zu wenden sowie deren oder dessen Kontaktdaten,
4. die Rechte auf Auskunft, Akteneinsicht, Berichtigung, Löschung und Sperrung,
5. die Rechtsgrundlagen der Datenverarbeitung,
6. Informationen über die mutmaßliche Dauer der Datenspeicherung oder, falls diese Angabe nicht möglich ist, Kriterien hierfür und
7. gegebenenfalls Informationen über die Kategorien der Empfängerinnen und Empfänger der Daten.

Bezieht sich die Benachrichtigung auf die Herkunft personenbezogener Daten von oder deren Übermittlung an Verfassungsschutzbehörden des Bundes oder der Länder, den Bundesnachrichtendienst oder den Militärischen Abschirmdienst, ist diese nur nach Zustimmung dieser Stellen zulässig.

(3) Ist wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen die betroffene Person eingeleitet worden, ist die Benachrichtigung im Sinne des Absatzes 1 in Abstimmung mit der Staatsanwaltschaft nachzuholen, sobald dies der Stand des Ermittlungsverfahrens zulässt. Die Unterrichtung kann unterbleiben, wenn die betroffene Person im Rahmen des Ermittlungsverfahrens von der Maßnahme Kenntnis erlangt.

(4) Die weitere Zurückstellung der Benachrichtigung im Sinne des Absatzes 1 bedarf der richterlichen Zustimmung, wenn sie nicht innerhalb von sechs Monaten nach Beendigung der Maßnahme erfolgt. Sind mehrere Maßnahmen in einem engen zeitlichen Zusammenhang durchgeführt worden, so beginnt die in Satz 1 genannte Frist mit der Beendigung der letzten Maßnahme. Zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Die richterliche Entscheidung ist vorbehaltlich einer anderen richterlichen Anordnung jeweils nach einem Jahr erneut einzuholen. Eine Benachrichtigung kann mit richterlicher Zustimmung frühestens nach dem Ablauf von fünf Jahren auf Dauer unterbleiben, wenn

1. überwiegende Interessen einer betroffenen Person entgegenstehen oder
2. die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden

und eine Verwendung der Daten gegen die betroffene Person ausgeschlossen ist. In diesem Fall sind die Daten zu löschen und die Löschung zu dokumentieren. Die Gründe für die Zurückstellung oder das Unterbleiben der Benachrichtigung sind zu dokumentieren.

§ 36

Auskunftsrecht, Akteneinsicht

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

1. die Rechtsgrundlage und die Zwecke der Verarbeitung,
2. verfügbare Informationen zur Herkunft der Daten oder, falls dies im Einzelfall nicht möglich ist, zu den Kategorien personenbezogener Daten, die verarbeitet werden,
3. die Empfängerinnen und Empfänger, gegenüber denen die personenbezogenen Daten offengelegt wurden, sowie die Teilnehmerinnen und Teilnehmer an automatisierten Abrufverfahren,
4. die für deren Speicherung vorgesehene Dauer oder, falls dies im Einzelfall nicht möglich ist, die Kriterien für deren Festlegung,
5. die bestehenden Rechte auf Berichtigung, Löschung und Sperrung und

6. die Kontaktdaten der oder des Landesbeauftragten und die Möglichkeit, bei ihr oder ihm Beschwerde einzulegen.

In dem Antrag soll die antragstellende Person die Art der personenbezogenen Daten, über die sie Auskunft verlangt, näher bezeichnen. Bestehen begründete Zweifel an der Identität der antragstellenden Person, kann die Erteilung der Auskunft von der Erbringung geeigneter Nachweise abhängig gemacht werden. Ein Auskunftsanspruch besteht nicht, wenn eine Auskunft bereits erteilt wurde und die gespeicherten personenbezogenen Daten sich nicht geändert haben oder die Auskunft offensichtlich missbräuchlich verlangt wird. Bei offensichtlich unbegründeten oder missbräuchlich gestellten Anträgen können angemessene Kosten erhoben werden, soweit nicht ausnahmsweise schon von der Bearbeitung abgesehen werden kann.

(2) Sind personenbezogene Daten in nichtelektronischen oder elektronischen Akten oder Dateien gespeichert, ist der antragstellenden Person Einsicht in die jeweiligen sie betreffenden Akten oder Dateien zu gewähren. Die Einsichtnahme darf nicht erfolgen, wenn die personenbezogenen Daten der antragstellenden Person mit personenbezogenen Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist der antragstellenden Person jedoch über die zu ihr gespeicherten Daten Auskunft zu erteilen. Rechtsvorschriften über die Akteneinsicht im Verwaltungsverfahren bleiben unberührt.

(3) Die Auskunftserteilung oder die Gewährung von Akteneinsicht kann verweigert werden, soweit und solange andernfalls

1. die Erfüllung polizeilicher Aufgaben gefährdet oder wesentlich erschwert würde,
2. die öffentliche Sicherheit oder Ordnung gefährdet würde,
3. überwiegende Rechte Dritter gefährdet würden,
4. die im Einzelfall erforderliche Geheimhaltung verarbeiteter Daten gefährdet würde oder
5. dem Wohl des Bundes oder eines Landes Nachteile entstehen würden und das Interesse der antragstellenden Person an der Auskunftserteilung nicht überwiegt.

Die Entscheidung über die Verweigerung der Auskunftserteilung oder der Gewährung von Akteneinsicht nach Satz 1 Nummer 5 trifft die Behördenleitung. § 35 bleibt unberührt.

(4) Die betroffene Person wird unverzüglich darüber in Kenntnis gesetzt, wie mit dem Antrag nach Absatz 1 oder 2 verfahren wird, falls über diesen keine unverzügliche Entscheidung erfolgt. Soweit ein Antrag abgelehnt wird, ist die betroffene Person hierüber schriftlich und unter Mitteilung der Gründe zu unterrichten. Die betroffene Person ist darauf hinzuweisen, dass sie Beschwerde bei der oder dem Landesbeauftragten einlegen, ihre Rechte auch über diesen ausüben oder gerichtlichen Rechtsschutz in Anspruch nehmen kann. Unterrichtungen können unterbleiben, soweit und solange hierdurch

1. die Erfüllung polizeilicher Aufgaben gefährdet oder wesentlich erschwert würde,
2. die öffentliche Sicherheit oder Ordnung gefährdet würde,
3. überwiegende Rechte Dritter gefährdet würden oder
4. dem Wohl des Bundes oder eines Landes Nachteile entstehen würden und das Interesse der antragstellenden Person an der Auskunftserteilung nicht überwiegt.

Absatz 3 Satz 2 gilt entsprechend.

(5) Die Gründe für die Ablehnung eines Antrags und das Unterbleiben einer Unterrichtung sind von der Polizei zu dokumentieren. Sie sind der oder dem Landesbeauftragten für deren oder dessen Kontrolle in auswertbarer Weise zur Verfügung zu stellen, soweit nicht das für Inneres zuständige Ministerium im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Eine Mitteilung der oder des Landesbeauftragten an die betroffene Person im Beschwerdeverfahren darf keine Rückschlüsse auf den Erkenntnisstand der Polizei zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(6) Bezieht sich die Auskunftserteilung oder die Akteneinsicht auf die Herkunft personenbezogener Daten von oder auf deren Übermittlung an

1. Verfassungsschutzbehörden des Bundes oder der Länder,
2. den Bundesnachrichtendienst,
3. den Militärischen Abschirmdienst und andere Behörden des Bundesministeriums der Verteidigung, soweit die Sicherheit des Bundes berührt wird,
4. Staatsanwaltschaften oder
5. Finanzbehörden, soweit diese personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern,

ist diese nur mit Zustimmung dieser Stellen zulässig. Hinsichtlich der von Verfassungsschutzbehörden, dem Bundesnachrichtendienst oder dem Militärischen Abschirmdienst stammenden oder für diese bestimmte Informationen gilt dies auch für die Auskunft über den Inhalt der Erkenntnisse.

§ 37

Verzeichnis von Verarbeitungstätigkeiten, Protokollierung, Kontrolle durch die oder den Landesbeauftragten

(1) Die Behördenleitung führt ein Verzeichnis über die Tätigkeiten der Polizei bei der Verarbeitung personenbezogener Daten. Dieses Verzeichnis enthält

1. den Namen und die Kontaktdaten der Behördenleitung als die verantwortliche Person und einer oder eines Datenschutzbeauftragten der Polizei,

2. die Zwecke der Verarbeitung,
3. die Kategorien von Empfängerinnen und Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfängerinnen und Empfängern in Drittländern oder bei über- oder zwischenstaatlichen Stellen,
4. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
5. die Verwendung von Profiling,
6. die Kategorien von Übermittlungen personenbezogener Daten an ein Drittland oder an eine über- oder zwischenstaatliche Stelle,
7. Angaben über die Rechtsgrundlage der Verarbeitung, einschließlich der Übermittlungen, für die die personenbezogenen Daten bestimmt sind,
8. wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Kategorien personenbezogener Daten, und
9. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherheit der Verarbeitung personenbezogener Daten.

(2) Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag der Polizei verarbeitet (auftragsverarbeitende Stelle), führt ein Verzeichnis über ihre Tätigkeiten bei der Verarbeitung personenbezogener Daten. Dieses Verzeichnis enthält

1. Name und Kontaktdaten der auftragsverarbeitenden Stelle, der Behördenleitung und eines Datenschutzbeauftragten der auftragsverarbeitenden Stelle,
2. die Kategorien von Verarbeitungen, die im Auftrag der Polizei durchgeführt werden,
3. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine über- oder zwischenstaatliche Stelle, wenn von der Polizei entsprechend angewiesen, einschließlich der Identifizierung des Drittlandes oder der über- oder zwischenstaatlichen Stelle, und
4. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherheit der Verarbeitung personenbezogener Daten.

(3) Die Verzeichnisse in den Absätzen 1 und 2 sind schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(4) Maßnahmen der Verarbeitung personenbezogener Daten sind zu protokollieren, soweit dies ohne Gefährdung der jeweiligen Maßnahme möglich ist. Aus den Protokollen müssen ersichtlich sein

1. die für die Maßnahmen verantwortliche Person,

2. Ort, Zeitpunkt und Dauer der Maßnahme,
3. Zweck und Art der Ausführung,
4. Angaben zu den nach § 35 Absatz 1 Satz 1 zu benachrichtigen Personen, wobei § 35 Absatz 1 Satz 3 entsprechend gilt, und
5. das wesentliche Ergebnis der Maßnahme.

Die Protokolldaten dürfen nur zur Erfüllung der Benachrichtigungspflichten nach § 35 Absatz 1 und der Unterrichtungspflichten nach § 41 sowie zu den in § 38 Absatz 3 Satz 1 genannten Zwecken verwendet werden; § 38 Absatz 3 Satz 4 gilt entsprechend.

(5) Die oder der Landesbeauftragte führt zu den Maßnahmen der Verarbeitung personenbezogener Daten im Abstand von längstens zwei Jahren Kontrollen durch. Zu diesem Zweck sind ihr oder ihm die Verzeichnisse nach den Absätzen 1 und 2, die Protokolle nach Absatz 4 sowie die Dokumentationen von Datenlöschungen und Vernichtungen von Unterlagen in auswertbarer Weise zur Verfügung zu stellen. Soweit die Protokolle für Zwecke des Absatzes 4 Satz 3 nicht mehr benötigt werden, sind sie zu löschen.

§ 38

Automatisierte Verfahren der Datenverarbeitung

(1) Die Einrichtung eines automatisierten Verfahrens, das die Verarbeitung, insbesondere die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der betroffenen Person und der Erfüllung polizeilicher Aufgaben angemessen ist. Der Abruf durch andere als Polizeibehörden ist nur auf Grund besonderer Rechtsvorschriften zulässig.

(2) Bei Datenverarbeitungsvorgängen nach Absatz 1 müssen

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

protokolliert werden. Die Protokolle müssen die dafür maßgeblichen Gründe samt Geschäftszeichen nennen sowie Datum und Uhrzeit dieser Vorgänge enthalten und, soweit möglich, die Feststellung der Identität der abrufenden oder offenlegenden Person sowie der Empfängerin oder des Empfängers ermöglichen.

(3) Die nach Absatz 2 erstellten Protokolle dürfen nur verwendet werden zur

1. Überprüfung der Rechtmäßigkeit der Datenverarbeitung, einschließlich der Eigenüberwachung,
2. Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten,
3. Verhütung, vorbeugenden Bekämpfung, Unterbindung oder Verfolgung von Straftaten, Ordnungswidrigkeiten und Kriminalitätsphänomenen oder
4. Kontrolle durch die oder den Landesbeauftragten.

Sie sind der oder dem Landesbeauftragten auf Anforderung in auswertbarer Weise zur Verfügung zu stellen. Soweit sie für Zwecke des Satzes 1 nicht mehr benötigt werden, sind sie zu löschen. Die Auswertung für Zwecke des Satzes 1 Nummer 3 bedarf der Anordnung durch die Behördenleitung.

(4) Die Polizei kann mit anderen Ländern und dem Bund einen Datenverbund vereinbaren, der eine automatisierte Datenübermittlung ermöglicht.

(5) Die Behördenleitung oder die auftragsverarbeitende Stelle ergreifen bei Einführung einer automatisierten Datenverarbeitung und danach in regelmäßigen Zeitabständen nach einer Risikobewertung Maßnahmen, um die Sicherheit der automatisierten Datenverarbeitung zu gewährleisten – unter Berücksichtigung des Stands der Technik, der Umsetzungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen. Umzusetzen sind Sicherheitsmaßnahmen

1. zur Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für unbefugte Personen (Zugangskontrolle),
2. zur Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (Datenträgerkontrolle),
3. zur Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),
4. zur Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch unbefugte Personen (Benutzerkontrolle),
5. zur Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems berechtigten Personen ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugangskontrolle),
6. zur Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),

7. zur Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
8. zur Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
9. zur Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können (Wiederherstellung),
10. zur Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit), und
11. zur Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).

(6) Eine Verletzung des Schutzes personenbezogener Daten wird dokumentiert. Die Behördenleitung meldet diese unverzüglich und möglichst innerhalb 72 Stunden nach dem Bekanntwerden der oder dem Landesbeauftragten, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Erfolgt die Meldung an die oder den Landesbeauftragten nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. Die auftragsverarbeitende Stelle meldet eine Verletzung des Schutzes personenbezogener Daten unverzüglich der Behördenleitung. Die Meldungen nach Satz 1 und 3 enthalten zumindest

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien personenbezogener Daten und der ungefähren Zahl der betroffenen personenbezogenen Datensätze,
2. Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und
4. eine Beschreibung der von der Behördenleitung oder der auftragsverarbeitenden Stelle ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls der Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann die Behördenleitung oder die auftragsverarbeitende Stelle diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(7) Die Behördenleitung benachrichtigt unverzüglich eine betroffene Person von der Verletzung des Schutzes personenbezogener Daten, wenn die Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Person zur Folge hat. Die Benachrichtigung beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Absatz 6 Satz 5 Nummer 2 bis 4 genannten Informationen und Maßnahmen. Die Behördenleitung kann schriftlich feststellen, dass die Benachrichtigung aufgeschoben, eingeschränkt oder unterlassen wird, wenn

1. geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung,
2. durch Maßnahmen sichergestellt wurde, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht,
3. diese mit einem unverhältnismäßigen Aufwand verbunden wäre und eine öffentliche Bekanntmachung oder ähnliche Maßnahme nicht in Betracht kommt,
4. dadurch behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren sichergestellt werden,
5. dies zur Verhütung, vorbeugenden Bekämpfung, Unterbindung oder Verfolgung von Straftaten, Ordnungswidrigkeiten von erheblicher Bedeutung oder Kriminalitätsphänomenen erforderlich ist,
6. dies dem Schutz der öffentlichen Sicherheit dient oder
7. dadurch der Schutz der Rechte und Freiheiten Dritter gewährleistet wird.

§ 39

Errichtungsanordnung für Dateien, Datenschutz-Folgenabschätzung

(1) Für den erstmaligen Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, ist in einer Errichtungsanordnung, die der Zustimmung des für Inneres zuständigen Ministeriums bedarf,

1. die speichernde Stelle,
2. die Bezeichnung der Datei,
3. der Zweck der Datei,
4. der betroffene Personenkreis,
5. die Art der zu speichernden Daten,

6. die Eingabeberechtigung,
7. die Zugangsberechtigung,
8. die regelmäßige Datenübermittlungen,
9. die Überprüfungsfristen,
10. die Speicherdauer,
11. die Protokollierung von Verarbeitungsvorgängen nach § 38 Absatz 2,
12. besondere Regelungen über die Verarbeitung von personenbezogenen Daten, insbesondere zum Verhältnis von Speicherinhalt und Abrufberechtigung, und
13. die Angaben nach Absatz 2 Satz 3

festzulegen. Nach der Zustimmung gemäß Satz 1 ist die Errichtungsanordnung der oder dem Landesbeauftragten mitzuteilen. Das gleiche gilt für wesentliche Änderungen des Verfahrens.

(2) Birgt eine Datenverarbeitung oder deren Änderung auf Grund ihrer Art, ihres Umfangs, ihres Zwecks, des Einsatzes neuer Technologien oder sonstiger Umstände voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen, führt die Behördenleitung vor ihrer erstmaligen Anwendung eine Abschätzung der Folgen für den Schutz personenbezogener Daten durch. Die oder der Landesbeauftragte kann zudem festlegen, welche Verarbeitungsvorgänge vor ihrer erstmaligen Anwendung einer Folgenabschätzung bedürfen. Die Folgenabschätzung muss den Rechten und schutzwürdigen Interessen betroffener Personen Rechnung tragen und eine allgemeine Beschreibung der vorgesehenen Verarbeitungsvorgänge und -zwecke, eine Bewertung der Risiken im Hinblick auf die Rechte der betroffenen Personen sowie eine Darstellung der vorgesehenen Abhilfe- und Schutzmaßnahmen enthalten. Ist zugleich eine Errichtungsanordnung nach Absatz 1 erforderlich, so ist vor deren Erstellung eine entsprechende Folgenabschätzung vorzunehmen; die Angaben nach Satz 3 sind in die Errichtungsanordnung aufzunehmen. Absatz 1 Satz 2 findet mit der Maßgabe Anwendung, dass der oder dem Landesbeauftragten vor der erstmaligen Anwendung vorgesehener Verarbeitungsvorgänge Gelegenheit zur Stellungnahme binnen sechs Wochen zu geben ist, wobei diese Frist auf dessen Ersuchen hin auf zehn Wochen verlängert werden kann. Bei Gefahr im Verzug findet Satz 5 keine Anwendung; die Mitteilung an die oder den Landesbeauftragten ist in diesen Fällen unverzüglich nachzuholen. Ihr oder ihm sind auf Anforderung alle für seine Kontrolle erforderlichen und für die Polizei verfügbaren Informationen zu übermitteln.

§ 40

Anwendung des Brandenburgischen Datenschutzgesetzes

Das Brandenburgische Datenschutzgesetz findet für den Bereich der Polizei ergänzend Anwendung, soweit in diesem Gesetz oder in anderen Rechtsvor-

schriften nichts Besonderes geregelt ist. § 28 des Brandenburgischen Datenschutzgesetzes gilt ausschließlich in Ausübung des Hausrechts.

§ 41

Parlamentarische Kontrolle

Das für Inneres zuständige Mitglied der Landesregierung unterrichtet den Landtag und dessen für Inneres zuständigen Ausschuss jährlich über die durchgeführten Maßnahmen nach Kapitel 2 Abschnitt 2 Unterabschnitt 2 und die mit diesen im Zusammenhang stehenden weiteren Maßnahmen. Der Bericht enthält unter anderem die folgenden Angaben über

1. den Maßnahmenanlass, soweit möglich, ihre Zuordnung zu bestimmten Gefahrenlagen und Deliktsbereichen,
2. den Umfang des Gebrauchmachens von den Befugnissen,
3. soweit möglich, die Zahl der hiervon betroffenen Personen, und wie sie informiert wurden,
4. im Falle einer vom Gericht anzuordnenden Maßnahme die Zahl der bei Gericht gestellten Anordnungsanträge und die jeweilige gerichtliche Entscheidung und
5. die Dauer der Maßnahme sowie die Dauer einer Verlängerung der Maßnahme.

Hierbei sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren.

Unterabschnitt 2

Datenerhebung

§ 42

Grundsätze der Datenerhebung

(1) Personenbezogene Daten sind grundsätzlich bei der betroffenen Person mit ihrer Kenntnis oder aus allgemein zugänglichen Quellen zu erheben. Personenbezogene Daten der betroffenen Person können auch bei Behörden, sonstigen öffentlichen Stellen oder bei Dritten erhoben werden, wenn die Datenerhebung nach Satz 1

1. bei der betroffenen Person nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist,
2. die schutzwürdigen Belange der betroffenen Person beeinträchtigt,
3. dem überwiegenden Interesse der betroffenen Person oder Dritter dient oder

4. die Erfüllung polizeilicher Aufgaben gefährden oder wesentlich erschweren würde.

(2) Die Polizei erhebt personenbezogene Daten grundsätzlich offen. Sie informiert dabei in geeigneter Weise über die Angaben in § 35 Absatz 2 Satz 1 Nummer 1 bis 7 sowie über eine im Einzelfall bestehende gesetzliche Auskunftspflicht oder die Freiwilligkeit der Auskunft. Das Informieren nach Satz 2 kann in den Fällen des Absatzes 3 Satz 1 Nummer 1 bis 3 zunächst unterbleiben. Sind die Voraussetzungen für das Unterbleiben nach Satz 3 entfallen, ist nach Satz 2 unverzüglich zu informieren.

(3) Eine verdeckte Datenerhebung, die nicht als polizeiliche Maßnahme erkennbar sein soll, ist zulässig, wenn

1. dies durch Gesetz bestimmt wird,
2. die Erfüllung polizeilicher Aufgaben auf andere Weise gefährdet oder wesentlich erschwert würde,
3. anzunehmen ist, dass dies überwiegenden Interessen oder schutzwürdigen Belangen der betroffenen Personen dient oder
4. dies dem Schutz der Rechte und Freiheiten Dritter dient.

Sind die Voraussetzungen für eine verdeckte Datenerhebung nach Satz 1 entfallen, erfolgt eine Benachrichtigung der betroffenen Person und Dritter nach § 35.

§ 43

Allgemeine Befugnis zur Datenerhebung

(1) Die Polizei kann personenbezogene Daten über die in den §§ 7, 8 und 10 genannten Personen und über andere Personen erheben, wenn dies erforderlich ist

1. zur Gefahrenabwehr (§ 1 Absatz 1), insbesondere
 - a. zur Verhütung oder vorbeugenden Bekämpfung von Straftaten oder Kriminalitätsphänomenen oder
 - b. zu Zwecken des Personenschutzes, soweit sich die diesbezügliche Gefahrenabwehr auf ein bedeutsames Rechtsgut bezieht,
2. zum Schutz privater Rechte (§ 1 Absatz 2),
3. zur Vollzugshilfe (§ 1 Absatz 3) oder
4. zur Erfüllung ihr durch andere Rechtsvorschriften übertragener Aufgaben (§ 1 Absatz 4).

(2) Die Polizei kann über

1. Personen, deren Kenntnisse oder Fähigkeiten zur Gefahrenabwehr benötigt werden,
2. verantwortliche Personen für Veranstaltungen in der Öffentlichkeit,
3. verantwortliche Personen für Anlagen oder Einrichtungen, von denen eine erhebliche konkrete Gefahr ausgehen kann, und
4. verantwortliche Personen für gefährdete Anlagen oder Einrichtungen

Namen, Vornamen, akademische Grade, Anschriften, Telefonnummern und andere Daten über die Erreichbarkeit sowie nähere Angaben über die Zugehörigkeit zu einer der genannten Personengruppen erheben, soweit dies zur Vorbereitung für die Hilfeleistung und das Handeln in Gefahrenfällen erforderlich ist. Wurden die Daten nicht bei der betroffenen Person erhoben, so sind ihr dies sowie der Zweck der beabsichtigten Nutzung unverzüglich mitzuteilen.

§ 44

Offene Bild- und Tonaufnahmen oder -aufzeichnungen

(1) Die Polizei kann bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, offen personenbezogene Daten von Teilnehmern und über die für eine konkrete Gefahr verantwortlichen Personen

1. auch durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen oder
2. wegen der Größe oder Unübersichtlichkeit der Örtlichkeit mittels Übersichtsaufnahmen oder -aufzeichnungen, einschließlich der gezielten Feststellung der Identität einer auf der Übersichtsaufzeichnung abgebildeten Person,

erheben, wenn Tatsachen die Annahme rechtfertigen, dass dabei Straftaten oder Ordnungswidrigkeiten begangen werden oder diese im Zusammenhang mit Kriminalitätsphänomenen stehen.

(2) Die Polizei kann

1. zur Abwehr einer konkreten Gefahr,
2. an öffentlich zugänglichen Orten, bei denen Tatsachen die Annahme rechtfertigen, dass dort vermehrt Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung drohen,
3. an den in § 15 Absatz 1 Nummer 2 genannten öffentlich zugänglichen Orten,
4. an oder in besonders gefährdeten öffentlich zugänglichen Objekten im Sinne von § 15 Absatz 1 Nummer 3 oder in deren unmittelbarer Nähe oder

5. zur Verhütung oder vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen, sofern diesbezüglich zumindest eine erhöhte abstrakte Gefahr besteht,

durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen offen Personen beobachten und personenbezogene Daten erheben.

(3) Die Polizei kann im Rahmen der Erfüllung ihrer Aufgaben zum Zwecke der Eigensicherung oder des Schutzes Dritter gegen eine konkrete Gefahr durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen in Fahrzeugen der Polizei offen personenbezogene Daten erheben.

(4) Die Polizei kann im Rahmen der Erfüllung ihrer Aufgaben an oder in öffentlich zugänglichen Orten oder Objekten zur Abwehr einer konkreten Gefahr durch den Einsatz körpernah getragener technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen offen personenbezogene Daten kurzfristig erheben. Die Speicherung der erlangten Daten für eine Dauer von mehr als 90 Sekunden ist zulässig, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz von Polizeivollzugsbediensteten oder Dritten gegen eine erhebliche konkrete Gefahr erforderlich ist. In Wohnungen dürfen Maßnahmen nach diesem Absatz nur zur Abwehr einer dringenden konkreten Gefahr für Leib, Leben oder Freiheit einer Person erfolgen, sofern damit nicht die Überwachung der Wohnung verbunden ist. In Wohnungen darf zudem keine kurzfristige technische Erhebung ohne unverzügliche Fertigung verarbeitungsfähiger Aufzeichnungen erfolgen. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34. Es ist sicherzustellen, dass im Falle einer kurzfristigen technischen Erhebung im Sinne von Satz 1, an die sich keine verlängerte Speicherung nach Satz 2 anschließt, die betroffenen personenbezogenen Daten unverzüglich gelöscht werden. Über die Anfertigung der technischen Aufnahmen oder Aufzeichnungen entscheidet der das Aufnahmegerät tragende Polizeivollzugsbedienstete anhand der konkreten Umstände des Einzelfalls.

(5) Die Polizei kann eine in Gewahrsam genommene Person durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen offen beobachten und personenbezogene Daten erheben, soweit dies zu ihrem oder zum Schutz des zur Durchführung des Gewahrsams eingesetzten Personals oder zur Verhütung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung in polizeilich genutzten Räumen erforderlich ist.

(6) Bei Maßnahmen nach den Absätzen 1 und 2 dürfen auf Anordnung der Behördenleitung und mit Zustimmung des für Inneres zuständigen Ministeriums Systeme zur automatischen Erkennung und Auswertung von Mustern bezogen auf Personen und Gegenstände einschließlich der automatischen Systemsteuerung zu diesem Zweck verwendet werden, soweit dies die Gefahrenlage auf Grund entsprechender Erkenntnisse erfordert. Der Verwendung dieser Systeme muss eine operative Präventionsplanung auf Grundlage eines kriminalpräventiven Handlungskonzepts zugrundeliegen; § 4 Absatz 2 bis 5 gilt entsprechend. Die längerfristige Verwendung dieser Systeme für mehr als einen Monat ist durch ein Monitoring zu begleiten und jährlich zu evaluieren. Die

Verwendung ist auf höchstens zwei Jahre zu befristen. Nach einem Bericht des für Inneres zuständigen Ministeriums an den Landtag und dessen für Inneres zuständigen Ausschuss sowie nach einer positiven auf Tatsachen beruhenden Einschätzung über die Verwendung solcher Systeme im konkreten Einzelfall kann die Maßnahme um jeweils längstens zwei Jahre verlängert werden.

(7) Die Polizei weist bei Maßnahmen nach den Absätzen 1 bis 5 in geeigneter Weise auf die Bild- und Tonaufnahmen und -aufzeichnungen hin, soweit nicht Gefahr im Verzug besteht. Auf die Verwendung von Systemen im Sinne des Absatzes 6 ist dabei gesondert hinzuweisen.

(8) Maßnahmen nach den Absätzen 1 bis 6 dürfen auch dann durchgeführt werden, wenn Dritte unvermeidlich betroffen werden.

(9) Bild- und Tonaufnahmen oder -aufzeichnungen und daraus gefertigte Unterlagen sind spätestens einen Monat nach der Datenerhebung zu löschen oder zu vernichten, soweit diese nicht benötigt werden

1. zur Verfolgung von Straftaten oder Ordnungswidrigkeiten,
2. zur Überprüfung der Rechtmäßigkeit der polizeilichen Maßnahme, wenn eine solche Überprüfung zu erwarten steht, oder
3. zum Zwecke der Benachrichtigung nach § 35 Absatz 1.

Die Löschung ist zu dokumentieren. § 58 Absatz 5 und 6 sowie § 67 Absatz 5 und 6 bleiben unberührt.

§ 45

Elektronische Aufenthaltsüberwachung, Strafvorschrift

(1) Auf Antrag der Behördenleitung und mit Zustimmung des für Inneres zuständigen Ministeriums kann

1. zur Abwehr einer erheblichen konkreten Gefahr oder
2. zur Verhütung oder vorbeugenden Bekämpfung von besonders schweren Straftaten oder von schwerwiegenden Kriminalitätsphänomenen

gegenüber einer dafür verantwortlichen Person angeordnet werden, die für eine elektronische Überwachung ihres Aufenthaltsorts erforderlichen technischen Mittel ständig in betriebsbereitem Zustand bei sich zu führen und deren Funktionsfähigkeit nicht zu beeinträchtigen. Eine Anordnung kann insbesondere mit Maßnahmen nach § 20 Absatz 2 verbunden werden.

(2) Die Polizei darf mit Hilfe der von der verantwortlichen Person mitgeführten technischen Mittel automatisiert Daten über deren Aufenthaltsort sowie über etwaige Beeinträchtigungen der Datenerhebung verarbeiten. Soweit es technisch möglich ist, ist sicherzustellen, dass innerhalb der Wohnung der verantwortlichen Person keine über den Umstand ihrer Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden. Die erhobenen Daten können zu ei-

nem Bewegungsbild verbunden werden, soweit dies zur Erfüllung des Überwachungszwecks erforderlich ist. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34.

(3) Maßnahmen nach Absatz 1 Satz 1 dürfen nur durch die Richterin oder den Richter angeordnet werden, bei Gefahr im Verzug auch durch die Behördenleitung; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen. Die Erstellung eines Bewegungsbildes ist nur zulässig, wenn dies richterlich besonders gestattet wird; Satz 1 gilt entsprechend. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Bestimmungen des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. In der schriftlichen Anordnung sind anzugeben

1. die betroffene Person, möglichst mit Namen und Anschrift,
2. die Art sowie einzelfallabhängig Umfang und Dauer der Maßnahme,
3. die tragenden Erkenntnisse für das Vorliegen der Gefahr, der Straftaten oder des Kriminalitätsphänomens nach Absatz 1 und
4. die Begründung der Verhältnismäßigkeit der Maßnahme.

Die Maßnahme ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Anordnungsvoraussetzungen fortbestehen. Sobald die Anordnungsvoraussetzungen weggefallen sind, ist die Maßnahme unverzüglich zu beenden und das anordnende Gericht davon zu unterrichten.

(4) Die nach Absatz 1 erhobenen Daten sind spätestens einen Monat nach Beendigung der Maßnahme zu löschen, soweit sie nicht für andere zulässige Zwecke verarbeitet werden. Die Löschung ist zu protokollieren.

(5) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer einer gerichtlichen Anordnung nach den Absätzen 1 und 3 absichtlich zuwiderhandelt und dadurch ständig oder wiederholt die Feststellung seines Aufenthaltsorts durch die Polizei verhindert. Die Tat wird nur auf Antrag der Behördenleitung verfolgt.

§ 46

Postsicherstellung

(1) Auf Antrag der Behördenleitung und mit Zustimmung des für Inneres zuständigen Ministeriums kann angeordnet werden, ohne Wissen der betroffenen Person Postsendungen sicherzustellen, wenn sich diese im Gewahrsam von postdiensteanbietenden Personen befinden, und von einer Person versandt wurden oder an eine Person gerichtet sind,

1. die für eine erhebliche konkrete Gefahr verantwortlich ist,
2. bei der hinreichend sichere Anhaltspunkte die Annahme rechtfertigen, dass diese besonders schwere Straftaten begehen, veranlassen oder un-

terstützen wird oder einem schwerwiegenden Kriminalitätsphänomen zugeordnet werden kann, oder

3. bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie für eine Person nach Nummer 1 oder 2 bestimmte oder von dieser herrührende Postsendungen entgegennimmt oder weitergibt und sie daher in Zusammenhang mit der Gefahrenlage, den angenommenen Straftaten oder einem schwerwiegenden Kriminalitätsphänomen steht, ohne diesbezüglich das Recht zur Verweigerung des Zeugnisses nach den §§ 53, 53a der Strafprozessordnung zu haben,

sofern andernfalls die Erfüllung der polizeilichen Aufgaben gefährdet oder wesentlich erschwert würde. Postdiensteanbietende Personen haben die Sicherstellung zu ermöglichen und unter den Voraussetzungen des Satzes 1 der Polizei auf Verlangen Auskünfte über derzeit oder ehemals in ihrem Gewahrsam befindliche oder angekündigte Postsendungen zu erteilen. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34.

(2) Maßnahmen nach Absatz 1 dürfen nur durch die Richterin oder den Richter angeordnet werden, bei Gefahr im Verzug auch durch die Behördenleitung; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Bestimmungen des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. In der schriftlichen Anordnung sind anzugeben

1. die betroffene Person, möglichst mit Namen und Anschrift,
2. die Art sowie einzelfallabhängig Umfang und Dauer der Maßnahme,
3. eine möglichst genaue Bezeichnung des Auskunftsverlangens und der der Sicherstellung unterliegenden Postsendungen,
4. die tragenden Erkenntnisse für das Vorliegen der Gefahr, der Straftaten oder des Kriminalitätsphänomens nach Absatz 1 und
5. die Begründung der Verhältnismäßigkeit der Maßnahme.

Die Maßnahme ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Anordnungsvoraussetzungen fortbestehen. Sobald die Anordnungsvoraussetzungen weggefallen sind, ist die Maßnahme unverzüglich zu beenden und das anordnende Gericht davon zu unterrichten.

(3) Die Öffnung der ausgelieferten Postsendungen erfolgt durch das zuständige Amtsgericht. Die Polizei legt die ihr ausgelieferten Postsendungen unverzüglich ohne vorherige inhaltliche Kenntnisnahme und ungeöffnet dem Gericht vor. Dieses entscheidet unverzüglich über die Öffnung. Es kann diese Befugnis bei Gefahr im Verzug widerruflich auf die Polizei übertragen. Bestehen Zweifel hinsichtlich der Verwertbarkeit der erlangten Erkenntnisse, hat die Entscheidung hierüber im Benehmen mit der oder dem Landesbeauftragten zu erfolgen.

(4) Postsendungen sind unverzüglich an die vorgesehene Empfängerin oder den vorgesehenen Empfänger weiterzuleiten, soweit

1. ihre Öffnung nicht angeordnet wurde oder
2. nach der Öffnung die Zurückbehaltung zur Gefahrenabwehr nicht mehr erforderlich ist.

§ 47

Einsatz besonderer Mittel der Datenerhebung

(1) Besondere Mittel der Datenerhebung sind

1. eine planmäßig angelegte Beobachtung
 - a. die durchgehend länger als zweiundsiebzig Stunden oder an mehr als an vier Tagen vorgesehen ist oder tatsächlich durchgeführt wird (längerfristige Observation) oder
 - b. die nicht die in Buchstabe a genannten Voraussetzungen erfüllt (kurzfristige Observation) oder
2. der verdeckte Einsatz technischer Mittel
 - a. zum Abhören oder Aufzeichnen des nichtöffentlich gesprochenen Wortes außerhalb von Wohnungen,
 - b. zur Anfertigung von Bildaufnahmen oder -aufzeichnungen außerhalb von Wohnungen, auch unter Verwendung von Systemen zur automatischen Erkennung und Auswertung von Mustern im Sinne des § 44 Absatz 6 und zum automatischen Datenabgleich, oder
 - c. zur Feststellung des Standortes oder der Bewegungen einer Person oder einer beweglichen Sache.

(2) Die Polizei kann personenbezogene Daten mit den besonderen Mitteln nach Absatz 1 Nummer 1 Buchstabe a und Nummer 2 erheben

1. zur Abwehr einer erheblichen konkreten Gefahr über die nach den §§ 7 oder 8 verantwortlichen oder nach § 10 notstandspflichtigen Personen,
2. zur Verhütung oder vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen über Personen, bei denen hinreichend sichere Anhaltspunkte die Annahme rechtfertigen, dass diese solche Straftaten begehen, veranlassen oder unterstützen werden oder einem solchen Kriminalitätsphänomen zugeordnet werden können, oder
3. über Kontakt- oder Begleitpersonen zu den in Nummer 1 oder 2 genannten Personen,

wenn andernfalls die Erfüllung der polizeilichen Aufgaben gefährdet oder wesentlich erschwert würde. Dabei dürfen auch personenbezogene Daten über

andere Personen erhoben werden, soweit dies erforderlich ist, um eine Datenerhebung nach Satz 1 durchführen zu können, es sei denn, es handelt sich um Berufsgeheimnisträger gemäß §§ 53, 53a der Strafprozessordnung, zu denen ein Vertrauensverhältnis besteht. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34. Die Benachrichtigung der betroffenen Person erfolgt nach § 35. Bei dem Einsatz von Mitteln nach Absatz 1 Nummer 2 Buchstabe c gilt, soweit dieser nicht ausschließlich zum Schutz der bei einem polizeilichen Einsatz tätigen Personen erfolgt, § 45 Absatz 2 Satz 2 und 3 sowie Absatz 3 Satz 2 entsprechend.

(3) Der Einsatz besonderer Mittel nach Absatz 2 in Verbindung mit Absatz 1

1. Nummer 1 Buchstabe a oder
2. Nummer 2
 - a. Buchstabe a oder
 - b. Buchstabe b oder c, bei dem durchgehend länger als zweiundsiebzig Stunden oder an mehr als vier Tagen die Anfertigung von Bild-, Standort- oder Bewegungsaufzeichnungen bestimmter Personen vorgesehen ist oder tatsächlich durchgeführt wird,

darf nur durch die Richterin oder den Richter angeordnet werden, bei Gefahr im Verzug auch durch die Behördenleitung; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen. Zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Der verdeckte Einsatz technischer Mittel nach Absatz 2 in Verbindung mit Absatz 1 Nummer 2 Buchstabe b oder c darf im Übrigen durch die Behördenleitung angeordnet werden, soweit dieser nicht von Satz 1 Nummer 2 Buchstabe b erfasst wird. In der schriftlichen Anordnung sind anzugeben

1. die betroffene Person, möglichst mit Namen und Anschrift,
2. die Art sowie einzelfallabhängig Umfang und Dauer der Maßnahme,
3. die tragenden Erkenntnisse für das Vorliegen der Gefahr, der Straftaten oder des Kriminalitätsphänomens nach Absatz 2 und
4. die Begründung der Verhältnismäßigkeit der Maßnahme.

Die Maßnahme ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Anordnungsvoraussetzungen fortbestehen. Sobald die Anordnungsvoraussetzungen weggefallen sind, ist die Maßnahme unverzüglich zu beenden und das anordnende Gericht davon zu unterrichten.

(4) Auf eine Observation nach Absatz 1 Nummer 1 Buchstabe b finden Absatz 2 Satz 1 und 5 und Absatz 3 keine Anwendung. Durch eine kurzfristige Observation kann die Polizei personenbezogene Daten über die in den §§ 7 und 8 genannten und über andere Personen nur erheben, wenn dies zum Zwecke

der Gefahrenabwehr (§ 1 Absatz 1) erforderlich ist und andernfalls die Erfüllung der polizeilichen Aufgaben gefährdet oder wesentlich erschwert würde.

§ 48

Einsatz technischer Mittel zur Überwachung von Wohnungen

(1) Die Polizei kann personenbezogene Daten durch den verdeckten Einsatz technischer Mittel zum Abhören und Aufzeichnen des gesprochenen Wortes oder zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen, auch unter Verwendung von Systemen zur automatischen Steuerung, in oder aus der Wohnung der betroffenen Person erheben, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass

1. dies zur Abwehr einer dringenden konkreten Gefahr unerlässlich ist oder
2. aufgrund tatsächlicher Anhaltspunkte, insbesondere aufgrund konkreter Informationen über Planungs- und Vorbereitungshandlungen, anzunehmen ist, dass besonders schwere Straftaten begangen, veranlasst oder unterstützt werden sollen und die Datenerhebung zur Abwehr der mit diesen Straftaten verbundenen dringenden konkreten Gefahr erforderlich ist.

(2) Die Polizei ist zur Datenerhebung nach Absatz 1 nur berechtigt über

1. die für die Gefahr nach den §§ 7 oder 8 verantwortlichen oder nach § 10 notstandspflichtigen Personen,
2. die für Straftaten nach Absatz 1 Nummer 2 potentiell verantwortlichen Personen oder
3. Kontakt- oder Begleitpersonen zu den in Nummer 1 oder 2 genannten Personen

und zu Eingriffen in das Recht auf Unverletzlichkeit der Wohnung dieser Personen. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden, es sei denn, es handelt sich um Berufsgeheimnisträger gemäß §§ 53, 53a der Strafprozessordnung, zu denen ein Vertrauensverhältnis besteht. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34. Die Benachrichtigung der betroffenen Person erfolgt nach § 35.

(3) Die Maßnahme darf nur durch die RichterIn oder den Richter angeordnet werden, bei Gefahr im Verzug auch durch die Behördenleitung; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen. Zuständig ist das Landgericht, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. In der schriftlichen Anordnung sind anzugeben

1. die betroffene Person, möglichst mit Namen und Anschrift,
2. die Art sowie einzelfallabhängig Umfang und Dauer der Maßnahme,

3. die zu überwachenden Wohnräume,
4. die tragenden Erkenntnisse für das Vorliegen der Gefahr oder der Straftaten nach Absatz 1 und
5. die Begründung der Verhältnismäßigkeit der Maßnahme.

Die Maßnahme ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Anordnungsvoraussetzungen fortbestehen. Sobald die Anordnungsvoraussetzungen weggefallen sind, ist die Maßnahme unverzüglich zu beenden und das anordnende Gericht davon zu unterrichten.

(4) Die durch die Überwachung erlangten personenbezogenen Daten sind stets als solche zu kennzeichnen. Sie dürfen für andere Zwecke verwendet werden, wenn dies zur Abwehr einer in Absatz 1 genannten dringenden Gefahr für die öffentliche Sicherheit oder für die Verfolgung der dort genannten Straftaten erforderlich ist. Eine solche Änderung der Zweckrichtung ist festzustellen und zu dokumentieren. Die Daten sind unverzüglich zu sperren, wenn sie nicht mehr erforderlich sind. Sie dürfen ausschließlich für eine gerichtliche Überprüfung verwendet werden und sind unverzüglich zu löschen, wenn sie hierfür nicht benötigt werden, spätestens zwei Wochen nach Benachrichtigung der betroffenen Person. Auf diese Frist ist in der Benachrichtigung hinzuweisen. Die Löschung ist zu dokumentieren.

(5) Dient die Überwachung ausschließlich dem Schutz der bei einem polizeilichen Einsatz in Wohnungen hoheitlich tätigen Personen, kann sie abweichend von Absatz 3 allein durch die Behördenleitung angeordnet werden. Die hierbei erlangten personenbezogenen Daten dürfen anderweitig nur zum Zwecke der Strafverfolgung oder der Gefahrenabwehr verwendet werden, wenn die Rechtmäßigkeit der Maßnahme zuvor richterlich festgestellt worden ist. Abweichend hiervon ist eine Verwendung der Daten bei Gefahr im Verzug zulässig, wenn die richterliche Entscheidung unverzüglich nachgeholt wird.

§ 49

Eingriffe in die Telekommunikation und in informationstechnische Systeme, Verkehrs- und Nutzungsdatenauskunft

(1) Die Polizei kann personenbezogene Daten durch den verdeckten Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation erheben

1. zur Abwehr einer erheblichen konkreten Gefahr über die nach den §§ 7 oder 8 verantwortlichen oder nach § 10 notstandspflichtigen Personen,
2. zur Verhütung oder vorbeugenden Bekämpfung von besonders schweren Straftaten oder von schwerwiegenden Kriminalitätsphänomenen über Personen, bei denen hinreichend sichere Anhaltspunkte die Annahme rechtfertigen, dass diese solche Straftaten begehen, veranlassen oder unterstützen werden oder einem solchen Kriminalitätsphänomen zugeordnet werden können, oder

3. über Kontakt- oder Begleitpersonen zu den in Nummer 1 oder 2 genannten Personen,

wenn andernfalls die Erfüllung der polizeilichen Aufgaben gefährdet oder wesentlich erschwert würde. Dabei dürfen, soweit zu Zwecken des Satzes 1 unerlässlich, auch visualisierte Darstellungen der Telekommunikation ausgeleitet und erhoben werden. Die Maßnahme darf auch auf Kommunikationssysteme erstreckt werden, die räumlich von den durch die betroffene Person genutzten Kommunikationssystemen getrennt sind, soweit sie im Rahmen des Telekommunikationsvorgangs verwendet werden. Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.

(2) Die Polizei kann durch den verdeckten Einsatz technischer Mittel auf informationstechnische Systeme zugreifen, um

1. die Durchführung von Maßnahmen nach Absatz 1 zu ermöglichen oder zu unterstützen,
2. Zugangsdaten und gespeicherte Daten zu erheben,
3. solche Daten zu löschen oder zu verändern oder
4. sonstige Eingriffe in informationstechnischen Systemen vorzunehmen,

wenn die Voraussetzungen des Absatzes 1 Satz 1 entsprechend vorliegen. Absatz 1 Satz 2 bis 4 gilt entsprechend. Vorgenommene Eingriffe nach Satz 1 sind, soweit technisch möglich, automatisiert rückgängig zu machen, wenn die Maßnahme beendet wird.

(3) Die Polizei kann unter den Voraussetzungen des Absatzes 1 oder 2 auch technische Mittel einsetzen, um

1. spezifische Kennungen, insbesondere Geräte- und Kartenummer von Mobilfunkendgeräten, zu ermitteln, wenn dies für die Durchführung einer Maßnahme nach Absatz 1 oder 2 unerlässlich ist,
2. den Standort eines Mobilfunkendgerätes oder eines sonstigen informationstechnischen Systems zu ermitteln oder
3. Telekommunikationsverbindungen zu unterbrechen, zu verhindern oder in anderer geeigneter Weise zu stören.

(4) Die Maßnahmen nach den Absätzen 1 bis 3 dürfen nur durch die Richterin oder den Richter angeordnet werden, bei Gefahr im Verzug auch durch die Behördenleitung; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen. Zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. In der schriftlichen Anordnung sind anzugeben

1. die betroffene Person, möglichst mit Namen und Anschrift,
2. die Art sowie einzelfallabhängig Umfang und Dauer der Maßnahme,

3. soweit bekannt, eine Kennung des betroffenen Telekommunikationsanschlusses oder Endgerätes und eine möglichst genaue Bezeichnung des betroffenen informationstechnischen Systems,
4. die tragenden Erkenntnisse für das Vorliegen der Gefahr, der Straftaten oder des Kriminalitätsphänomens nach Absatz 1 und
5. die Begründung der Verhältnismäßigkeit der Maßnahme.

Die Anordnung ist zeitlich zu befristen

1. im Falle des Absatzes 3 Nummer 2 auf höchstens zwei Wochen,
2. im Falle des Absatzes 2 Satz 1 Nummer 4 oder des Absatzes 3 Nummer 3 auf höchstens drei Tage und
3. in allen anderen Fällen auf höchstens einen Monat.

Eine Verlängerung um jeweils den gleichen Zeitraum ist zulässig, sofern die Anordnungsvoraussetzungen fortbestehen. Sobald die Anordnungsvoraussetzungen weggefallen sind, ist die Maßnahme unverzüglich zu beenden und das anordnende Gericht darüber zu unterrichten.

(5) Die Polizei kann unter den Voraussetzungen des Absatzes 1 Satz 1 telediensteanbietende Personen verpflichten, unverzüglich Auskunft über vorhandene Verkehrs- oder Nutzungsdaten der nach Absatz 1 oder 2 betroffenen Personen sowie über die für die Ermittlung des Standortes eines Mobilfunkendgerätes oder eines sonstigen informationstechnischen Systems dieser Personen erforderlichen spezifischen Kennungen, insbesondere die Geräte- und Kartenummer sowie die Zellinformation, zu erteilen. Eine Auskunftsanordnung über künftig anfallende Verkehrs-, Nutzungs- oder Standortdaten ist nach Maßgabe des Absatzes 4 Satz 5 Nummer 1 zu befristen. Im Übrigen gelten die Bestimmungen des Absatzes 4 entsprechend. Gefahr im Verzug ist insbesondere anzunehmen, wenn für die

1. Abwehr einer dringenden konkreten Gefahr,
2. Beseitigung einer Suizidgefahr,
3. Suche nach gefährdeten vermissten Personen,
4. Suche nach minderjährigen vermissten Personen oder
5. Befreiung aus einer hilflosen Lage

aufgrund einer Prüfung im Einzelfall die Zeit fehlt, vor dem Auskunftersuchen die Richterin oder den Richter zu erreichen.

(6) Eine Anordnung nach den Absätzen 4 und 5 verpflichtet telediensteanbietende Personen, nach Maßgabe der Regelungen des Telekommunikationsgesetzes, des Telemediengesetzes und der darauf beruhenden Rechtsverordnungen zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen der Polizei die Überwachung und Aufzeichnung zu ermöglichen. Die Entschädigung richtet sich nach § 23 des Justizvergütungs-

und -entschädigungsgesetzes, soweit nicht eine Entschädigung aufgrund des Telekommunikationsgesetzes oder des Telemediengesetzes zu gewähren ist.

(7) Die Maßnahmen nach den Absätzen 1, 2, 3 und 5 dürfen auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden, es sei denn, es handelt sich um Berufsgeheimnisträger gemäß §§ 53, 53a der Strafprozessordnung, zu denen ein Vertrauensverhältnis besteht. Die Daten Dritter sind nach Beendigung der Maßnahme unverzüglich zu löschen. Die Löschung ist zu dokumentieren. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34. Die Benachrichtigung der betroffenen Person erfolgt nach § 35.

(8) Die aufgrund einer Maßnahme nach den Absätzen 1, 2, 3 und 5 erlangten personenbezogenen Daten sind besonders zu kennzeichnen. Sie sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. Zum Zwecke der Datenschutzkontrolle sind

1. die Bezeichnung der technischen Erfassungsmittel, der Ort und der Zeitpunkt des Einsatzes,
2. die Angaben zur Identifizierung der Telekommunikation und des informationstechnischen Systems, die betroffen sind, und die daran vorgenommenen Eingriffe,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit und die Bediensteten, die die Maßnahme durchführt,

zu protokollieren. Die Protokolldaten dürfen nur verwendet werden, um einer betroffenen Person, einer dazu befugten öffentlichen Stelle oder einem Gericht die Prüfung zu ermöglichen, ob die Maßnahme rechtmäßig durchgeführt worden ist. Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 4 genannten Zweck erforderlich sind.

(9) Die aufgrund einer Maßnahme nach den Absätzen 1, 2, 3 und 5 erlangten personenbezogenen Daten dürfen für andere Zwecke verwendet werden, wenn dies zur Gefahrenabwehr nach Absatz 1 Nummer 1 bis 3 oder für die Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist. Eine solche Änderung der Zweckrichtung ist festzustellen und zu dokumentieren.

(10) Personenbezogene Daten, bei denen sich nach der Auswertung herausstellt, dass die Voraussetzungen für ihre Erhebung nicht vorlagen, dürfen nicht verwendet werden und sind unverzüglich zu löschen, es sei denn, ihre Verwendung ist zur Abwehr einer dringenden konkreten Gefahr erforderlich. In diesen Fällen ist eine richterliche Entscheidung über die Zulässigkeit der Verwendung unverzüglich einzuholen. Im Übrigen sind die aufgrund von Maßnahmen nach den Absätzen 1, 2, 3 und 5 erlangten personenbezogenen Daten unverzüglich zu sperren, wenn sie nicht mehr erforderlich sind. Sie dürfen ausschließlich für eine gerichtliche Überprüfung verwendet werden und sind unverzüglich zu löschen, wenn sie hierfür nicht benötigt werden, spätestens jedoch zwei Wochen nach Benachrichtigung der betroffenen Person. Auf die-

se Frist ist in der Benachrichtigung hinzuweisen. Die Löschung von Daten nach den Sätzen 1 und 4 ist zu dokumentieren.

§ 50

Bestandsdatenauskunft

(1) Die Polizei kann

1. zur Abwehr einer erheblichen konkreten Gefahr oder
2. zur Verhütung oder vorbeugenden Bekämpfung von besonders schweren Straftaten oder von schwerwiegenden Kriminalitätsphänomenen

telediensteanbietende Personen verpflichten, unverzüglich Auskunft über Bestandsdaten im Sinne der §§ 95 und 111 des Telekommunikationsgesetzes und § 14 des Telemediengesetzes zu erteilen. Bezieht sich das Auskunftsverlangen auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die konkret beabsichtigte Nutzung der Daten im Zeitpunkt des Ersuchens vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden.

(3) Die Maßnahme darf nur durch die Richterin oder den Richter angeordnet werden, bei Gefahr im Verzug auch durch die Behördenleitung; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen. Gefahr im Verzug ist insbesondere anzunehmen, wenn für die

1. Abwehr einer dringenden konkreten Gefahr,
2. Beseitigung einer Suizidgefahr,
3. Suche nach gefährdeten vermissten Personen,
4. Suche nach minderjährigen vermissten Personen oder
5. die Befreiung aus einer hilflosen Lage

aufgrund einer Prüfung im Einzelfall die Zeit fehlt, vor dem Auskunftersuchen ein Gericht zu erreichen. Zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. In der schriftlichen Anordnung sind anzugeben

1. die betroffene Person, möglichst mit Namen und Anschrift,
2. die Art sowie einzelfallabhängig Umfang und Dauer der Maßnahme,

3. soweit bekannt, eine Kennung des betroffenen Telekommunikationsanschlusses oder Endgerätes,
4. die tragenden Erkenntnisse für das Vorliegen der Gefahr, der Straftaten oder des Kriminalitätsphänomens nach Absatz 1 und
5. die Begründung der Verhältnismäßigkeit der Maßnahme.

(4) Die zur Auskunftserteilung erforderlichen Daten sind von der telediensteanbietenden Person unverzüglich zu übermitteln. Im Übrigen gilt für die Auskunftspflicht der telediensteanbietenden Personen und ihr Recht auf Entschädigung § 49 Absatz 6 entsprechend.

(5) Für das weitere Verfahren, insbesondere für die Benachrichtigung der betroffenen Person sowie für die Kennzeichnung, Verwendung, Sperrung und Löschung der Daten gilt § 49 Absatz 7 bis 9 entsprechend.

§ 51

Datenerhebung durch den Einsatz von Vertrauenspersonen

(1) Die Polizei kann personenbezogene Daten durch den Einsatz von Vertrauenspersonen erheben

1. zur Abwehr einer erheblichen konkreten Gefahr über die nach den §§ 7 oder 8 verantwortlichen oder nach § 10 notstandspflichtigen Personen,
2. zur Verhütung oder vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen über Personen, bei denen hinreichend sichere Anhaltspunkte die Annahme rechtfertigen, dass diese solche Straftaten begehen, veranlassen oder unterstützen werden oder einem solchen Kriminalitätsphänomen zugeordnet werden können, oder
3. über Kontakt- oder Begleitpersonen zu den in Nummer 1 oder 2 genannten Personen,

wenn andernfalls die Erfüllung der polizeilichen Aufgaben gefährdet oder wesentlich erschwert würde. Ein solcher Einsatz liegt nicht vor, soweit sich eine, auch wiederkehrende, polizeiliche Datenerhebung auf die Erlangung von bei dieser Person bereits vorhandenen und von dieser angebotenen Daten beschränkt. Es dürfen auch personenbezogene Daten über andere Personen erhoben werden, soweit dies erforderlich ist, um eine Datenerhebung nach Satz 1 durchführen zu können, es sei denn, es handelt sich um Berufsgeheimnisträger gemäß §§ 53, 53a der Strafprozessordnung, zu denen ein Vertrauensverhältnis besteht. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34. Die Benachrichtigung der betroffenen Person erfolgt nach § 35.

(2) Der Einsatz von Vertrauenspersonen darf nur durch die Richterin oder den Richter angeordnet werden, bei Gefahr im Verzug auch durch die Behördenleitung; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen. Zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizei-

behörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. In der schriftlichen Anordnung sind anzugeben

1. die betroffene Person, möglichst mit Namen und Anschrift,
2. die Art sowie einzelfallabhängig Umfang und Dauer der Maßnahme,
3. die tragenden Erkenntnisse für das Vorliegen der Gefahr, der Straftaten oder des Kriminalitätsphänomens nach Absatz 1 und
4. die Begründung der Verhältnismäßigkeit der Maßnahme.

Die Maßnahme ist auf höchstens sechs Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als sechs Monate ist zulässig, soweit die Anordnungsvoraussetzungen fortbestehen. Sobald die Anordnungsvoraussetzungen weggefallen sind, ist die Maßnahme unverzüglich zu beenden und das anordnende Gericht davon zu unterrichten. Sie kann insbesondere auch nähere Maßgaben zur Führung der Vertrauensperson enthalten.

(3) Vertrauenspersonen dürfen insbesondere nicht eingesetzt werden, um

1. in einer Person, die nicht zur Begehung von Straftaten bereit ist, den Entschluss zu wecken, solche zu begehen,
2. eine Person zur Begehung einer über ihre erkennbare Bereitschaft hinausgehenden Straftat zu bestimmen oder
3. Daten mit Mitteln oder Methoden zu erheben, die die Polizei nicht einsetzen dürfte.

(4) Als Vertrauensperson darf nicht eingesetzt werden, wer

1. nicht voll geschäftsfähig, insbesondere minderjährig ist,
2. an einem Aussteigerprogramm teilnimmt,
3. Mitglied des Europäischen Parlaments, des Deutschen Bundestages, eines Landesparlaments oder diesbezüglicher Mitarbeiter eines solchen Mitglieds ist oder
4. im Bundeszentralregister mit einer Verurteilung als Täter eines Totschlags (§§ 212, 213 des Strafgesetzbuchs) oder einer allein mit lebenslanger Haft bedrohten Straftat eingetragen ist.

(5) Eine Vertrauensperson ist fortlaufend auf ihre Zuverlässigkeit zu überprüfen. Die von der Vertrauensperson bei einem Einsatz gewonnenen Informationen sind unverzüglich auf ihren Wahrheitsgehalt zu prüfen. Ergeben sich begründete Zweifel an der Zuverlässigkeit, ist der Einsatz nicht durchzuführen oder zu beenden. Bei der Prüfung der Zuverlässigkeit ist insbesondere zu berücksichtigen, ob die einzusetzende Vertrauensperson

1. von den Geld- und Sachzuwendungen für die Tätigkeit auf Dauer als überwiegende Lebensgrundlage abhängen würde oder
2. im Bundeszentralregister mit einer Verurteilung wegen eines Verbrechens oder zu einer Freiheitsstrafe, deren Vollstreckung nicht zur Bewährung ausgesetzt wurde, eingetragen ist.

(6) § 52 Absatz 2 Satz 1 und 2 findet auf die polizeilichen Führungspersonen einer Vertrauensperson Anwendung, soweit dies zur Vorbereitung, Durchführung, Lenkung oder Absicherung ihres Einsatzes erforderlich ist.

§ 52

Datenerhebung durch den Einsatz verdeckt ermittelnder Personen

(1) Die Polizei kann personenbezogene Daten durch den Einsatz von verdeckt ermittelnden Personen erheben

1. zur Abwehr einer erheblichen konkreten Gefahr über die nach den §§ 7 oder 8 verantwortlichen oder die nach § 10 notstandspflichtigen Personen,
2. zur Verhütung oder vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen über Personen, bei denen hinreichend sichere Anhaltspunkte die Annahme rechtfertigen, dass diese solche Straftaten begehen, veranlassen oder unterstützen werden oder einem solchen Kriminalitätsphänomen zugeordnet werden können, oder
3. über Kontakt- oder Begleitpersonen zu den in Nummer 1 oder 2 genannten Personen,

wenn andernfalls die Erfüllung der polizeilichen Aufgaben gefährdet oder wesentlich erschwert würde. Es dürfen auch personenbezogene Daten über andere Personen erhoben werden, soweit dies erforderlich ist, um eine Datenerhebung nach Satz 1 durchführen zu können, es sei denn, es handelt sich um Berufsgeheimnisträger gemäß §§ 53, 53a der Strafprozessordnung, zu denen ein Vertrauensverhältnis besteht. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34. Die Benachrichtigung der betroffenen Person erfolgt nach § 35.

(2) Soweit es für den Aufbau und zur Aufrechterhaltung der Legende unerlässlich ist, dürfen entsprechende Urkunden hergestellt oder verändert werden. Eine verdeckt ermittelnde Person darf unter der Legende zur Erfüllung ihres Auftrages am Rechtsverkehr teilnehmen. Sie darf unter der Legende mit Einverständnis der berechtigten Person deren Wohnung betreten. Die Sätze 1 und 2 gelten entsprechend für

1. das Auftreten und Handlungen einer verdeckt ermittelnden Person in elektronischen Medien und Kommunikationseinrichtungen sowie
2. die polizeilichen Führungspersonen einer verdeckt ermittelnden Person, soweit dies zur Vorbereitung, Durchführung, Lenkung oder Absicherung von deren Einsatz erforderlich ist.

Im Übrigen richten sich die Befugnisse einer verdeckt ermittelnden Person nach diesem Gesetz und der Strafprozessordnung.

(3) Der Einsatz einer verdeckt ermittelnden Person, der sich gegen eine bestimmte Person richtet oder bei dem die Vertrauensperson oder die verdeckt ermittelnde Person eine Wohnung betritt, die nicht allgemein zugänglich ist, darf nur durch die RichterIn oder den Richter angeordnet werden, bei Gefahr im Verzug auch durch die Behördenleitung; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen. Zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Im Übrigen darf der Einsatz einer verdeckt ermittelnden Person nur durch die Behördenleitung angeordnet werden. In der schriftlichen Anordnung sind anzugeben

1. die betroffene Person, möglichst mit Namen und Anschrift,
2. die Art sowie einzelfallabhängig Umfang und Dauer der Maßnahme,
3. die tragenden Erkenntnisse für das Vorliegen der Gefahr, der Straftaten oder des Kriminalitätsphänomens nach Absatz 1 und
4. die Begründung der Verhältnismäßigkeit der Maßnahme.

Die Maßnahme ist auf höchstens sechs Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als sechs Monate ist zulässig, soweit die Anordnungsvoraussetzungen fortbestehen. Sobald die Anordnungsvoraussetzungen weggefallen sind, ist die Maßnahme unverzüglich zu beenden und das anordnende Gericht davon zu unterrichten.

§ 53

Polizeiliche Ausschreibung

(1) Die Polizei kann personenbezogene Daten, insbesondere die Personalien einer Person sowie Kennzeichen des von ihr benutzten oder eingesetzten Fahrzeuges, zur polizeilichen Beobachtung, verdeckten Registrierung und gezielten Kontrolle (Artikel 99 des Schengener Durchführungsübereinkommens) in einer Datei speichernd ausschreiben

1. zur Abwehr einer erheblichen konkreten Gefahr über die nach den §§ 7 oder 8 verantwortlichen Personen,
2. zur Verhütung oder vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen über Personen, bei denen
 - a. Tatsachen die Annahme rechtfertigen, dass diese solche Straftaten begehen, veranlassen oder unterstützen werden,

- b. die Gesamtbeurteilung, insbesondere auf Grund der bisher von ihnen begangenen Straftaten, erwarten lässt, dass sie auch künftig solche Straftaten begehen, veranlassen oder unterstützen werden, oder
 - c. hinreichende Anhaltspunkte vorliegen, dass diese einem solchen Kriminalitätsphänomen zugeordnet werden können, oder
3. über Kontakt- oder Begleitpersonen zu den in Nummer 1 oder 2 genannten Personen.

Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34. Die Benachrichtigung der betroffenen Person erfolgt nach § 35.

(2) Im Falle eines Antreffens der ausgeschriebenen Person oder des ausgeschriebenen Fahrzeugs können die nachstehenden Informationen verdeckt erhoben und der ausschreibenden Stelle übermittelt werden:

- 1. das Antreffen,
- 2. Ort, Zeit und Anlass der Überprüfung,
- 3. Reiseweg und Reiseziel,
- 4. Begleitpersonen und Insassen,
- 5. benutztes Fahrzeug,
- 6. mitgeführte Sachen sowie
- 7. Umstände des Antreffens der Person und des Fahrzeugs.

(3) Die polizeiliche Ausschreibung darf nur durch die Behördenleitung angeordnet werden. Die Anordnung ist auf höchstens ein Jahr zu befristen. Eine Verlängerung um nicht mehr als jeweils ein Jahr ist zulässig, soweit die Voraussetzungen des Absatzes 1 weiterhin vorliegen. Spätestens nach Ablauf von jeweils sechs Monaten ist von der ausschreibenden Polizeibehörde zu prüfen, ob die Voraussetzungen für die Anordnung noch bestehen. Das Ergebnis dieser Prüfung ist aktenkundig zu machen.

§ 54

Anlassbezogene automatische Kennzeichenfahndung

(1) Die Polizei kann durch den verdeckten Einsatz technischer Mittel automatisiert Kennzeichen von Fahrzeugen sowie Ort, Datum, Uhrzeit und Fahrtrichtung erfassen,

- 1. wenn dies zur Abwehr einer erheblichen konkreten Gefahr erforderlich ist,
- 2. bei Vorliegen entsprechender Lageerkenntnisse einer konkreten Gefahr in den Fällen des § 15 Absatz 1 Nummer 1 bis 6 oder

3. bei einer polizeilichen Ausschreibung der Person oder des Fahrzeuges nach § 53 Absatz 1 Satz 1.

In den Fällen des Satzes 1 Nummer 3 dürfen Einzelerfassungen zu einem Bewegungsbild verbunden werden. Die Kennzeichenerfassung darf nicht flächendeckend eingesetzt werden. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34. Die Benachrichtigung der betroffenen Person erfolgt nach § 35. Die anlassbezogene automatische Kennzeichenfahndung darf nur durch die Behördenleitung angeordnet werden.

(2) Die erhobenen Daten können mit zur Abwehr der Gefahr nach Absatz 1 gespeicherten polizeilichen Daten und mit den Daten der polizeilichen Fahndungsbestände automatisch abgeglichen werden. Im Trefferfall ist unverzüglich die Datenübereinstimmung zu überprüfen. Bei Datenübereinstimmung können die Daten polizeilich verarbeitet und im Falle des Absatzes 1 Satz 1 Nummer 3 zusammen mit den gewonnenen Erkenntnissen an die ausschreibende Stelle übermittelt werden. Andernfalls sind sie sofort zu löschen.

§ 55

Einsatz und Abwehr unbemannter Luftfahrtsysteme

(1) Die Polizei kann personenbezogene Daten durch den Einsatz unbemannter Luftfahrtsysteme erheben, unter den Voraussetzungen

1. für offene Bild- und Tonaufnahmen oder -aufzeichnungen nach § 44 Absatz 1 oder 2, wenn die Offenheit der Maßnahme gewahrt bleibt und die Polizei auf den Einsatz von unbemannten Luftfahrtsystemen gesondert hinweist,
2. des Einsatzes besonderer Mittel der Datenerhebung nach § 47 Absatz 2,
3. des Einsatzes technischer Mittel in Wohnungen nach § 48 Absatz 1,
4. der Eingriffe in die Telekommunikation und in informationstechnische Systeme nach § 49 Absatz 1 bis 3 und
5. der anlassbezogenen automatischen Kennzeichenfahndung nach § 54 Absatz 1.

Die unbemannten Luftfahrtsysteme dürfen mit technischen Mitteln der Bild-, Ton- und Sensoraufklärung ausgestattet, nicht aber bewaffnet werden. Soweit in den Fällen des Satzes 1 eine richterliche Anordnung erforderlich ist, muss diese auch den Einsatz von unbemannten Luftfahrtsystemen umfassen.

(2) Die Polizei kann zur Abwehr einer konkreten Gefahr unbemannte Luftfahrtsysteme einschließlich ihrer Kontrollstation oder unbemannte Fluggeräte zu Zwecken des Sports oder der Freizeitgestaltung durch den Einsatz technischer oder anderer Mittel stören, herunterholen oder in sonstiger Weise beeinflussen, wenn

1. nicht zu erwarten ist, dass durch die Maßnahme das Leben von Menschen gefährdet wird, und
2. die Gefahr für die betroffenen Schutzgüter im Rahmen der Abwägung mit den Eingriffen in sonstige betroffene Rechtsgüter überwiegt.

Unterabschnitt 3

Datenspeicherung, Datenveränderung und Datennutzung

§ 56

Allgemeine Regeln über die Dauer der Datenspeicherung

Die Dauer der Speicherung ist auf das erforderliche Maß zu beschränken. Für automatisierte Dateien sind Termine festzulegen, zu denen spätestens überprüft werden muss, ob die suchfähige Speicherung von Daten weiterhin erforderlich ist (Prüfungstermine). Für nicht-automatisierte Dateien und Akten sind Prüfungstermine oder Aufbewahrungsfristen festzulegen. Dabei sind der Speicherungszweck sowie Art und Bedeutung des Anlasses der Speicherung zu berücksichtigen. Prüfungstermine oder Aufbewahrungsfristen für die in Dateien oder Akten suchfähig gespeicherten personenbezogenen Daten von Kindern dürfen zwei Jahre nicht überschreiten; die Frist beginnt mit dem Tag der ersten Speicherung. Es ist ein Verfahren festzulegen, welches die Einhaltung der Termine und Fristen sicherstellt.

§ 57

Zweckbindung bei der Datenspeicherung, Datenveränderung und Datennutzung

(1) Die Speicherung, Veränderung und Nutzung darf nur zu dem Zweck erfolgen, zu dem die Daten erlangt worden sind. Die Nutzung sowie die weitere Speicherung und Veränderung zu einem anderen Zweck sind jedoch zulässig, soweit die Polizei die Daten auch zu diesem Zweck erheben darf. Satz 2 gilt nicht für die nach § 43 Absatz 2 erhobenen Daten.

(2) Werden wertende Angaben über eine Person in Dateien gespeichert, muss feststellbar sein, bei welcher Stelle die den Angaben zugrunde liegenden Informationen vorhanden sind. Wertende Angaben dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen wurden.

§ 58

Speicherung, Veränderung und Nutzung von Daten

(1) Die Polizei kann rechtmäßig erlangte personenbezogene Daten in Akten oder Dateien speichern, verändern und nutzen, soweit dies zur Erfüllung ihrer Aufgaben, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsver-

waltung erforderlich ist. Die Benachrichtigung der betroffenen Person erfolgt nach § 35.

(2) Dabei kann die Polizei auch die im Rahmen der Verfolgung von Straftaten gewonnenen personenbezogenen Daten zum Zwecke der Gefahrenabwehr (§ 1 Absatz 1) speichern, verändern und nutzen. Eine suchfähige Speicherung dieser Daten in Dateien und Akten ist nur über Personen zulässig, gegen die ein strafrechtliches Ermittlungsverfahren eingeleitet worden ist. Die nach § 56 festzulegenden Prüfungstermine dürfen für Daten nach Satz 1 bei Erwachsenen zehn Jahre und bei Jugendlichen fünf Jahre nicht überschreiten. Die Frist beginnt mit dem Tag, an dem das letzte Ereignis eingetreten ist, das zur Speicherung der Daten geführt hat, jedoch nicht vor Entlassung der betroffenen Person aus einer Justizvollzugsanstalt oder Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung. Ist der Verdacht der Straftat gegen die Person entfallen, sind ihre in diesem Zusammenhang in Dateien suchfähig gespeicherten personenbezogenen Daten zu löschen sowie die zu ihrer Person suchfähig angelegten Akten zu vernichten. Wird gegen die Person erneut ein Ermittlungsverfahren wegen des Verdachts einer Straftat eingeleitet, können die nach § 56 festzulegenden Prüfungstermine entsprechend Satz 3 und 4 neu festgelegt werden.

(3) Über Kontakt- oder Begleitpersonen sowie über Auskunftspersonen kann die Polizei personenbezogene Daten suchfähig in Dateien speichern, verändern und nutzen, soweit dies

1. zur Abwehr einer erheblichen konkreten Gefahr oder
2. zur Verhütung oder vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen

erforderlich ist. Die Daten dürfen nur für die Dauer eines Jahres gespeichert werden. Die Speicherung für jeweils ein weiteres Jahr ist zulässig, soweit die Voraussetzungen des Satzes 1 weiterhin vorliegen, jedoch darf die Speicherdauer insgesamt drei Jahre nicht überschreiten. Die Entscheidung über die jeweilige Verlängerung trifft die Behördenleitung.

(4) Die Polizei kann Anrufe über Notrufeinrichtungen auf Tonträger aufzeichnen. Eine Aufzeichnung von Anrufen im Übrigen ist nur zulässig, soweit die Aufzeichnung zur polizeilichen Aufgabenerfüllung erforderlich ist. Die Aufzeichnungen sind spätestens nach einem Monat zu löschen, es sei denn, dass

1. sie zur Verfolgung von Straftaten benötigt werden,
2. Tatsachen die Annahme rechtfertigen, dass die anrufende Person Straftaten begehen, veranlassen oder unterstützen wird, oder
3. die Aufbewahrung zur Verhütung oder vorbeugenden Bekämpfung von Straftaten oder Kriminalitätsphänomenen erforderlich ist.

(5) Die Polizei kann gespeicherte personenbezogene Daten zu statistischen Zwecken nutzen; die Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren oder zu pseudonymisieren.

(6) Die Polizei kann personenbezogene Daten zur polizeilichen Aus- und Fortbildung nutzen. Die personenbezogenen Daten sind vorher zu anonymisieren oder zu pseudonymisieren. Personenbezogene Daten, die auf der Grundlage der §§ 48 und 49 Absatz 2 erhoben worden sind, dürfen nicht für polizeiliche Aus- und Fortbildungszwecke genutzt werden.

§ 59

Datenabgleich

(1) Die Polizei kann personenbezogene Daten der in den §§ 7 und 8 genannten Personen mit dem Inhalt polizeilicher Dateien abgleichen. Personenbezogene Daten anderer Personen kann die Polizei nur abgleichen, wenn Tatsachen die Annahme rechtfertigen, dass dies zur Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich ist. Die Polizei kann ferner rechtmäßig erlangte personenbezogene Daten mit dem Fahndungsbestand abgleichen. Die betroffene Person kann für die Dauer des Datenabgleichs angehalten werden. Rechtsvorschriften über den Datenabgleich in anderen Fällen bleiben unberührt.

(2) Ein Datenabgleich nach Absatz 1 kann auch unter Verwendung bildverarbeitender Systeme und durch Auswertung biometrischer Daten erfolgen, wenn andernfalls die Erfüllung polizeilicher Aufgaben gefährdet oder wesentlich erschwert würde.

Unterabschnitt 4

Datenübermittlung

§ 60

Allgemeine Regeln der Datenübermittlung

(1) Personenbezogene Daten dürfen nur zu dem Zweck übermittelt werden, zu dem sie erlangt oder gespeichert worden sind. Abweichend hiervon kann die Polizei personenbezogene Daten übermitteln, soweit dies

1. durch Gesetz zugelassen ist oder
2. zur Abwehr einer konkreten Gefahr erforderlich ist und die Empfängerin oder der Empfänger die Daten auf andere Weise nicht oder nicht rechtzeitig oder nur mit unverhältnismäßig hohem Aufwand erlangen kann.

Die auf der Grundlage der §§ 48 und 49 Absatz 2 erhobenen Daten und die nach § 58 Absatz 3 gespeicherten Daten dürfen nur an Polizeibehörden übermittelt werden.

(2) Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der Polizei von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, ist die Datenübermittlung durch die Polizei nur zulässig, wenn die Emp-

fängerin oder der Empfänger die Daten zur Erfüllung des gleichen Zwecks benötigt, zu dem sie die Polizei erlangt hat.

(3) Die Verantwortung für die Übermittlung trägt die übermittelnde Polizeibehörde. Sie prüft die Zulässigkeit der Datenübermittlung. Erfolgt die Datenübermittlung aufgrund eines Ersuchens der Empfängerin oder des Empfängers, hat diese oder dieser der übermittelnden Polizeibehörde die zur Prüfung erforderlichen Angaben zu machen. Erfolgt die Datenübermittlung durch automatisierten Abruf, trägt die Verantwortung für die Rechtmäßigkeit des Abrufs die Empfängerin oder der Empfänger. Personenbezogene Daten, die auf der Grundlage der §§ 48 und 49 Absatz 2 erhoben worden sind, dürfen nicht im automatisierten Abrufverfahren übermittelt werden.

(4) Die Empfängerin oder der Empfänger darf die übermittelten personenbezogenen Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck nutzen, zu dem sie ihr oder ihm übermittelt worden sind. Ausländische öffentliche Stellen, über- und zwischenstaatliche Stellen sowie Personen und Stellen außerhalb des öffentlichen Bereichs sind bei der Datenübermittlung darauf hinzuweisen.

(5) Eine Datenübermittlung im Sinne dieses Gesetzes ist nicht die Weitergabe personenbezogener Daten zwischen Stellen innerhalb der Behörde.

§ 61

Datenübermittlung zwischen Polizeibehörden

(1) Zwischen Polizeibehörden können personenbezogene Daten übermittelt werden, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Eine Übermittlung zu einem anderen Zweck als dem, zu dem die Daten erlangt oder gespeichert worden sind, ist zulässig, soweit die Daten auch zu diesem Zweck erhoben werden dürfen. Satz 2 gilt nicht für die nach § 43 Absatz 2 erhobenen Daten.

(2) § 62 Absatz 5 und 6 gilt entsprechend. Das für Inneres zuständige Mitglied der Landesregierung wird ermächtigt, durch Rechtsverordnung zu bestimmen, dass die Datenübermittlung gemäß Satz 1 an Polizeibehörden bestimmter ausländischer Staaten zulässig ist, wenn dies wegen der internationalen polizeilichen Zusammenarbeit oder der polizeilichen Zusammenarbeit im Grenzgebiet erforderlich ist.

§ 62

Datenübermittlung an öffentliche Stellen, an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen

(1) Die Polizei kann von sich aus personenbezogene Daten an öffentliche Stellen sowie an ausländische öffentliche und an über- und zwischenstaatliche Stellen übermitteln, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist.

(2) Die Polizei kann von sich aus anderen für die Gefahrenabwehr zuständigen öffentlichen Stellen bei ihr vorhandene personenbezogene Daten übermit-

teln, soweit die Kenntnis dieser Daten zur Aufgabenerfüllung der Empfängerin oder des Empfängers für den Bereich der Gefahrenabwehr erforderlich erscheint.

(3) Die Polizei kann auf Ersuchen personenbezogene Daten an öffentliche Stellen übermitteln, soweit dies

1. zur Abwehr einer konkreten Gefahr durch die Empfängerin oder den Empfänger,
2. in besonders gelagerten Einzelfällen zur Wahrnehmung einer sonstigen Gefahrenabwehraufgabe durch die Empfängerin oder den Empfänger,
3. zur Abwehr erheblicher Nachteile für das Gemeinwohl oder
4. zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer Person

erforderlich ist.

(4) Die Polizei kann personenbezogene Daten von sich aus oder auf Ersuchen an Verfassungsschutzbehörden des Bundes oder der Länder, den Bundesnachrichtendienst und den Militärischen Abschirmdienst übermitteln, wenn die Daten zugleich konkrete Erkenntnisse zu einer Gefährdung der jeweiligen Rechtsgüter erkennen lassen, die für die Lagebeurteilung nach Maßgabe der Aufgaben der genannten Behörden bedeutsam sind.

(5) Die Polizei kann personenbezogene Daten unter den gleichen Voraussetzungen wie im Inland übermitteln an öffentliche Stellen

1. eines Mitgliedstaats der Europäischen Union,
2. der Europäischen Union oder
3. eines Staats, der die Bestimmungen des Schengen-Besitzstandes auf Grund eines Assoziierungsübereinkommens mit der Europäischen Union über die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes anwendet (Schengenassoziiertes Land).

(6) Die Polizei kann personenbezogene Daten an andere als die in Absatz 5 genannten öffentlichen Stellen ausländischer Staaten (Drittstaat) sowie über- und zwischenstaatlichen Stellen übermitteln, wenn dies auf Grund eines konkreten Ermittlungsansatzes zur Verhütung, vorbeugenden Bekämpfung, Unterbindung oder Verfolgung von Straftaten oder Kriminalitätsphänomenen oder zur Abwehr von konkreten Gefahren erforderlich ist, die empfangende Stelle für diese Zwecke zuständig ist und

1. die Europäische Kommission einen Beschluss gefasst hat, wonach der Drittstaat oder die über- oder zwischenstaatliche Stelle ein angemessenes Datenschutzniveau bietet,
2. auf Grund völkerrechtlicher Vereinbarungen oder anderer geeigneter Garantien der Schutz personenbezogener Daten sichergestellt ist oder

3. soweit die Voraussetzungen der Nummer 1 oder 2 nicht vorliegen, die Übermittlung erforderlich ist
 - a. zur Abwehr von erheblichen oder gegenwärtigen konkreten Gefahren oder
 - b. zur Wahrung schutzwürdiger Interessen oder Belange einer betroffenen Person, sofern Rechte oder Interessen Dritter nicht überwiegen.

Die Polizei kann personenbezogene Daten im Einzelfall bei Gefahr im Verzug unmittelbar an andere als in Satz 1 genannte öffentliche Stellen in Drittstaaten übermitteln. Die Datenübermittlung unterbleibt, soweit Grund zu der Annahme besteht, dass dadurch gegen den Zweck eines deutschen Gesetzes oder einer Regelung der Europäischen Union oder der Konvention zum Schutz der Menschenrechte und Grundfreiheiten – insbesondere gegen Menschen- und Grundrechte, Datenschutzregelungen oder die Vorschriften zur Speicherungs-, Nutzungs- oder Übermittlungsbeschränkung oder zur Lösungsverpflichtung – verstoßen wird oder schutzwürdige Belange einer betroffenen Person, die das öffentliche Interesse an der Übermittlung überwiegen, beeinträchtigt werden.

§ 63

Datenübermittlung an Personen oder an Stellen außerhalb des öffentlichen Bereichs, Bekanntgabe an die Öffentlichkeit

(1) Die Polizei kann von sich aus personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit dies

1. zur Erfüllung ihrer Aufgaben oder
2. zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer Person erforderlich ist.

(2) Die Polizei kann auf Antrag von Personen oder Stellen außerhalb des öffentlichen Bereichs personenbezogene Daten übermitteln, soweit die auskunftsbegehrende Person

1. ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, dass das Geheimhaltungsinteresse der betroffenen Person überwiegt, oder
2. ein berechtigtes Interesse geltend macht und offensichtlich ist, dass die Datenübermittlung im Interesse der betroffenen Person liegt und diese in Kenntnis der Sachlage ihre Einwilligung hierzu erteilen würde.

§ 36 Absatz 5 gilt entsprechend.

(3) Die Polizei kann personenbezogene Daten und Abbildungen einer Person zum Zweck der Ermittlung ihrer Identität oder ihres Aufenthaltsortes oder zur Warnung öffentlich bekannt geben, wenn

1. dies zur Abwehr einer dringenden konkreten Gefahr unerlässlich ist oder
2. Tatsachen die Annahme rechtfertigen, dass diese Person Straftaten von erheblicher Bedeutung begehen, veranlassen oder unterstützen wird, und die Verhütung oder vorbeugende Bekämpfung dieser Straftaten auf andere Weise nicht möglich erscheint oder wesentlich erschwert wird.

Die Bekanntgabe kann mit auf tatsächlichen Anhaltspunkten beruhenden wertenden Angaben über die Person verbunden werden, wenn dies zur Abwehr der in Satz 1 genannten Gefahren oder Straftaten erforderlich ist. Die Maßnahme darf nur durch die Behördenleitung angeordnet werden.

§ 64

Datenübermittlung an die Polizei

(1) Öffentliche Stellen können, soweit gesetzlich nichts anderes bestimmt ist, von sich aus personenbezogene Daten an die Polizei übermitteln, wenn dies zur Erfüllung polizeilicher Aufgaben erforderlich erscheint.

(2) Die Polizei kann an öffentliche Stellen Ersuchen auf Übermittlung von personenbezogenen Daten stellen, soweit die Voraussetzungen für eine Datenerhebung vorliegen. Die ersuchte öffentliche Stelle prüft die Zulässigkeit der Datenübermittlung. Wenn gesetzlich nichts anderes bestimmt ist, prüft sie nur, ob das Ersuchen im Rahmen der Aufgaben der Polizei liegt, es sei denn, im Einzelfall besteht Anlass zur Prüfung der Rechtmäßigkeit des Ersuchens. Die Polizei hat die zur Prüfung erforderlichen Angaben zu machen. Die ersuchte öffentliche Stelle hat die Daten an die Polizei zu übermitteln, soweit gesetzlich nichts anderes bestimmt ist.

(3) Die Polizei kann die Verfassungsschutzbehörden des Bundes oder der Länder, den Bundesnachrichtendienst und den Militärischen Abschirmdienst um Übermittlung mit nachrichtendienstlichen Mitteln erhobener personenbezogener Daten nur ersuchen, wenn

1. dies Abwehr einer erheblichen konkreten Gefahr erforderlich ist oder
2. die Informationen auch mit eigenen Befugnissen in gleicher Weise hätten erhoben werden können.

(4) Die Polizei kann an ausländische öffentliche Stellen sowie über- und zwischenstaatliche Stellen Ersuchen auf Übermittlung von personenbezogenen Daten stellen, soweit die Voraussetzungen für eine Datenerhebung vorliegen und gesetzlich nichts anderes bestimmt ist. Das Ersuchen an Drittstaaten oder an andere über- oder zwischenstaatliche Stellen als die Europäischen Union unterbleibt, soweit Grund zu der Annahme besteht, dass dadurch oder durch die Datenverarbeitung des Drittstaates oder der über- oder zwischenstaatlichen Stelle gegen den Zweck eines deutschen Gesetzes oder einer Regelung der Europäischen Union oder der Konvention zum Schutz der Menschenrechte und Grundfreiheiten – insbesondere gegen Menschen- und Grundrechte, Datenschutzregelungen oder die Vorschriften zur Speicherungs-, Nutzungs- oder Übermittlungsbeschränkung oder zur Löschungsverpflichtung – versto-

ßen wird oder schutzwürdige Belange einer betroffenen Person, die das öffentliche Interesse an dem Ersuchen überwiegen, beeinträchtigt werden.

§ 65

Rasterfahndung, Profiling

(1) Die Polizei kann von öffentlichen Stellen und Stellen außerhalb des öffentlichen Bereichs die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateien zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen (Rasterfahndung) verlangen, soweit dies

1. zur Abwehr einer erheblichen konkreten Gefahr oder
2. zur Verhütung oder vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen erforderlich ist.

Die Polizei kann unter den Voraussetzungen des Satzes 1 die Übermittlung personenbezogener Daten von öffentlichen Stellen und Stellen außerhalb des öffentlichen Bereichs verlangen und diese mit anderen Datenbeständen automatisiert verarbeiten, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu analysieren, zu bewerten oder vorherzusagen (Profiling). Eine Maßnahme, die zur Folge hat, dass natürliche Personen auf Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist verboten. Für den Einsatz von Systemen der automatischen Datenverarbeitung zur automatisierten Entscheidungsfindung gilt § 33 Absatz 7. Die Benachrichtigung der betroffenen Person erfolgt nach § 35.

(2) Das Übermittlungsersuchen ist auf Namen, Anschrift, Tag und Ort der Geburt sowie andere für den Einzelfall benötigte Daten zu beschränken; es darf sich nicht auf personenbezogene Daten erstrecken, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34. Von Übermittlungsersuchen nicht erfasste personenbezogene Daten dürfen übermittelt werden, wenn wegen erheblicher technischer Schwierigkeiten oder wegen eines unangemessenen Zeit- oder Kostenaufwandes eine Beschränkung auf die angeforderten Daten nicht möglich ist; diese Daten dürfen von der Polizei nicht genutzt werden.

(3) Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten auf den Datenträgern zu löschen und die Akten, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind, zu vernichten. Über die getroffene Maßnahme ist eine Niederschrift anzufertigen. Diese Niederschrift ist gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Löschung der Daten oder der Vernichtung der Akten nach Satz 1 folgt, zu vernichten.

(4) Die Maßnahme darf auf Antrag der Behördenleitung nur durch die Richterin oder den Richter angeordnet werden, bei Gefahr im Verzug auch durch die Behördenleitung; in diesem Fall ist unverzüglich eine richterliche Bestätigung

einzuholen. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Die Anordnung ist schriftlich zu erlassen und zu begründen. Sie muss die zur Übermittlung verpflichtete Person bezeichnen und ist auf die Daten und Prüfungsmerkmale zu beschränken, die für den Einzelfall benötigt werden. Von der Maßnahme ist die oder der Landesbeauftragte unverzüglich zu unterrichten.

§ 66

Projektbezogene gemeinsame Dateien mit dem Verfassungsschutz Brandenburg

(1) Die Polizei kann auf Grundlage einer gemeinsamen Anordnung der Polizeipräsidentin oder des Polizeipräsidenten und der Leiterin oder des Leiters des Verfassungsschutzes Brandenburg mit Zustimmung des für Inneres zuständigen Ministeriums für die Dauer einer befristeten projektbezogenen Zusammenarbeit mit dem Verfassungsschutz eine gemeinsame Datei errichten. Die projektbezogene Zusammenarbeit bezweckt nach Maßgabe der Aufgaben und Befugnisse der in Satz 1 genannten Stellen den Austausch und die gemeinsame Auswertung von polizeilichen oder nachrichtendienstlichen Erkenntnissen zu

1. Straftaten nach § 99 des Strafgesetzbuchs oder
2. Straftaten nach § 129a, auch in Verbindung mit § 129b Absatz 1 des Strafgesetzbuchs und
3. Straftaten, die mit Straftaten nach den Nummern 1 und 2 in einem unmittelbaren Zusammenhang stehen.

Der projektbezogenen Zusammenarbeit muss ein bestimmter Projektauftrag mit konkret vereinbarten Projektzielen und Verfahrensweisen zugrunde liegen.

(2) Die Daten der gemeinsamen Datei beziehen sich auf

1. Personen, die
 - a. eine geheimdienstliche Agententätigkeit nach § 99 des Strafgesetzbuchs ausüben,
 - b. einer terroristischen Vereinigung nach § 129a des Strafgesetzbuchs, auch in Verbindung mit § 129b Absatz 1 des Strafgesetzbuchs angehören oder
 - c. Personen oder Vereinigungen nach Buchstabe a oder b willentlich unterstützen oder
2. Kontakt- oder Begleitpersonen, Vereinigungen, Gruppierungen, Stiftungen, Unternehmen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüsse, Telekommunikationsendgeräte, Internetseiten oder Adressen für elektronische Post, bei denen tatsächliche Anhaltspunkte die

Annahme begründen, dass sie im Zusammenhang mit einer Person nach Nummer 1 stehen und durch sie Hinweise für die Verhütung, vorbeugende Bekämpfung oder Unterbindung von Straftaten nach Absatz 1 Satz 2 Nummer 1 bis 3 gewonnen werden können.

(3) Für die Speicherung personenbezogener Daten in der gemeinsamen Datei gelten die jeweiligen Übermittlungsvorschriften zugunsten der an der Zusammenarbeit beteiligten öffentlichen Stellen entsprechend mit der Maßgabe, dass die Speicherung nur zulässig ist, wenn die Daten allen an der projektbezogenen Zusammenarbeit teilnehmenden Stellen übermittelt werden dürfen. Eine Speicherung ist ferner nur zulässig, wenn die speichernde Stelle die Daten auch in eigenen Dateien speichern darf. Die personenbezogenen Daten müssen besonders gekennzeichnet werden. Zu den Personen nach Absatz 2 Nummer 1 können

1. der Familienname, die Vornamen, frühere Namen, andere Namen, Aliaspersonalien, abweichende Namensschreibweisen, das Geschlecht, das Geburtsdatum, der Geburtsort, der Geburtsstaat, aktuelle und frühere Staatsangehörigkeiten, gegenwärtige und frühere Anschriften, besondere körperliche Merkmale, Sprachen, Dialekte, Lichtbilder und Angaben zu Identitätspapieren (Grunddaten) und
2. soweit erforderlich eigene oder von ihnen genutzte Telekommunikationsanschlüsse und Telekommunikationsendgeräte, Adressen für elektronische Post, Bankverbindungen, Schließfächer, auf die Person zugelassene oder von ihr genutzte Fahrzeuge, Familienstand, Volkszugehörigkeit, Angaben zur Religionszugehörigkeit, besondere Kenntnisse und Fertigkeiten, Bildungsabschlüsse, Berufstätigkeit, Angaben zur Gefährlichkeit, Fahr- und Flugerlaubnisse, besuchte Orte oder Gebiete, Kontaktpersonen, Bezeichnung der konkreten Vereinigung oder fremden Macht, der Tag der die Speicherung verursachenden Erkenntnisse, auf tatsächlichen Anhaltspunkten beruhende zusammenfassende besondere Bemerkungen, ergänzende Hinweise und Bewertungen zu Grunddaten und erweiterten Grunddaten und von dieser Person betriebene oder maßgeblich zum Zweck ihrer Aktivitäten genutzte Internetseiten (erweiterte Grunddaten)

gespeichert werden. Darüber hinaus können Angaben zur Identifizierung der in Absatz 2 Nummer 2 genannten Kontakt- und Begleitpersonen, Vereinigungen, Gruppierungen, Stiftungen, Unternehmen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüsse, Telekommunikationsendgeräte, Internetseiten und Adressen für elektronische Post gespeichert werden.

(4) Im Rahmen der gemeinsamen Datei obliegt die datenschutzrechtliche Verantwortung für die in der gemeinsamen Datei gespeicherten Daten den Stellen, die die Daten speichern. Die verantwortliche Stelle muss feststellbar sein. Die Verantwortung für die Zulässigkeit des Abrufs trägt die abrufende Stelle. Nur die Stelle, die Daten zu einer Person eingegeben hat, ist befugt, diese zu ändern, zu berichtigen, zu sperren oder zu löschen. Für die Änderung, Berichtigung, Sperrung und Löschung personenbezogener Daten durch die speichernde Stelle gelten die jeweiligen, für diese Stelle anwendbaren Vorschriften entsprechend. Hat eine beteiligte Stelle Anhaltspunkte dafür, dass die Daten unrichtig sind, teilt sie dies umgehend der speichernden Stelle mit, die verpflichtet ist, diese Mitteilung unverzüglich zu prüfen und erforderlichenfalls die

Daten unverzüglich zu ändern, zu berichtigen, zu sperren oder zu löschen. Sind Daten zu einer Person gespeichert, kann jede beteiligte Stelle weitere Daten ergänzend speichern.

(5) Die Behördenleitung hat für eine gemeinsame Datei ein Verzeichnis von Verarbeitungstätigkeiten nach § 37 Absatz 1 zu führen sowie im Einvernehmen mit dem Verfassungsschutz die jeweiligen Organisationseinheiten zu bestimmen, die zur Speicherung und zum Abruf befugt sind. Das Verzeichnis von Verarbeitungstätigkeiten bedarf der Zustimmung des für Inneres zuständigen Ministeriums.

(6) Das für Inneres zuständige Ministerium und die oder der Landesbeauftragte haben die Einhaltung der Regelungen zur Zusammenarbeit, zur Führung und zum Datenschutz der gemeinsamen Datei zu überwachen. Sie überprüfen in regelmäßigen Abständen das Verzeichnis von Verarbeitungstätigkeiten nach § 37 Absatz 1 einschließlich der Angaben, die die Feststellung der abgerufenen Datensätze sowie der verantwortlichen Stelle ermöglicht.

(7) Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34. Die Benachrichtigung der betroffenen Person erfolgt nach § 35.

(8) Eine gemeinsame Datei nach Absatz 1 ist auf höchstens zwei Jahre zu befristen. Die Frist kann um bis zu jeweils einem Jahr verlängert werden, höchstens jedoch für insgesamt 10 Jahre, wenn das Ziel der projektbezogenen Zusammenarbeit bei Projektende noch nicht erreicht worden und die Datei weiterhin für die Erreichung des Ziels erforderlich ist. Die Gründe für die Verlängerung sind zu dokumentieren.

Unterabschnitt 5

Datenberichtigung, Datenlöschung und Datensperrung

§ 67

Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie falsch oder fehlerhaft sind. Sind personenbezogene Daten in Akten zu berichtigen, ist in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt und aus welchem Grund diese Daten falsch oder fehlerhaft waren oder geworden sind.

(2) In Dateien suchfähig gespeicherte personenbezogene Daten und die dazugehörigen zu den Personen suchfähig angelegten Akten sind zu löschen oder zu vernichten, wenn

1. dies durch dieses Gesetz bestimmt ist,
2. die Speicherung nicht zulässig ist oder
3. bei der zu bestimmten Terminen vorzunehmenden Prüfung oder aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass die Daten für die Erfüllung der Aufgaben der speichernden Stelle nicht mehr erforderlich sind.

In Dateien nicht suchfähig gespeicherte Daten sind unter den Voraussetzungen des Satzes 1 zu löschen, soweit die Speicherung festgestellt wird. Die nach Satz 1 Nummer 3 vorzunehmende Aktenvernichtung ist nur durchzuführen, wenn die gesamte Akte für die Aufgabenerfüllung nicht mehr erforderlich ist, es sei denn, dass die betroffene Person die Vernichtung von Teilen der Akte verlangt und die weitere Speicherung diese in unangemessener Weise beeinträchtigt. Soweit hiernach eine Vernichtung nicht in Betracht kommt, sind die Daten zu sperren und mit einem Sperrvermerk zu versehen.

(3) Andere als die in Absatz 2 genannten Akten sind nach Ablauf der jeweiligen Aufbewahrungsfrist zu vernichten.

(4) Stellt die Polizei fest, dass unrichtige oder nach Absatz 2 Satz 1 Nummer 2 zu löschende personenbezogene Daten übermittelt worden sind, ist der Empfängerin oder dem Empfänger die Berichtigung oder Löschung mitzuteilen, es sei denn, die Mitteilung ist für die Beurteilung der Person oder des Sachverhalts nicht oder nicht mehr von Bedeutung.

(5) Löschung und Vernichtung unterbleiben, wenn

1. Grund zu der Annahme besteht, dass schutzwürdige Belange der betroffenen Person beeinträchtigt werden,
2. die Daten zur Behebung einer bestehenden Beweisnot unerlässlich sind oder
3. die Nutzung der Daten zu wissenschaftlichen Zwecken erforderlich ist.

In diesen Fällen sind die Daten zu sperren und mit einem Sperrvermerk zu versehen. Sie dürfen nur zu den in Satz 1 genannten Zwecken oder sonst mit Einwilligung der betroffenen Person genutzt werden. Im Falle des Satzes 1 Nummer 3 gilt § 25 des Brandenburgischen Datenschutzgesetzes.

(6) Anstelle der Löschung oder Vernichtung sind die Datenträger oder die Akten an ein öffentliches Archiv abzugeben, soweit archivrechtliche Regelungen dies vorsehen.“

33. Der bisherige § 50 wird § 68 und wie folgt geändert:

a) Nach Absatz 1 wird folgender Absatz 2 eingefügt:

„(2) Soweit Dienstkräfte der Justizverwaltung nicht oder nicht ausreichend zur Verfügung stehen, führt die Polizei Personen dem Gericht oder der Staatsanwaltschaft vor und unterstützt die Gerichtsvorsitzenden erforderlichenfalls bei der Aufrechterhaltung der Ordnung in der Sitzung.“

b) Der bisherige Absatz 2 wird Absatz 3 und in Satz 2 das Wort „übrigen“ durch das Wort „Übrigen“ ersetzt.

c) Der bisherige Absatz 3 wird Absatz 4.

34. Der bisherige § 51 wird § 69 und in Absatz 3 werden nach den Wörtern „ersuchende Behörde“ die Wörter „oder das ersuchende Gericht“ eingefügt.

35. Der bisherige § 52 wird § 70 und in Absatz 3 wird die Angabe „§§ 19 und 20“ durch die Angabe „§§ 23 und 24“ ersetzt.
36. Der bisherige § 53 wird § 71 und in Absatz 2 dem Wort „Gefahr“ das Wort „konkreten“ vorangestellt.
37. Der bisherige § 54 wird § 72 und Absatz 1 wie folgt geändert:
- a) Satz 1 wird wie folgt geändert:
 - aa) In Nummer 1 wird die Angabe „§ 55“ durch die Angabe „§ 73“ ersetzt.
 - bb) In Nummer 2 wird die Angabe „§ 56“ durch die Angabe „§ 74“ ersetzt.
 - cc) In Nummer 3 wird die Angabe „§ 58“ durch die Angabe „§ 76“ ersetzt.
 - b) In Satz 2 wird die Angabe „§§ 59 und 64“ durch die Angabe „§§ 77 und 82“ ersetzt.
38. Der bisherige § 55 wird § 73 und wie folgt geändert:
- a) In Absatz 1 Satz 1 werden die Wörter „des Betroffenen“ durch die Wörter „der betroffenen Person“ ersetzt.
 - b) In Absatz 2 Satz 1 bis 3 wird das Wort „daß“ durch das Wort „dass“ und jeweils die Wörter „der Betroffene“ durch die Wörter „die betroffene Person“ ersetzt.
39. Der bisherige § 56 wird § 74 und wie folgt geändert:
- a) In Absatz 2 werden die Wörter „dem Betroffenen“ durch die Wörter „der betroffenen Person“ ersetzt.
 - b) In Absatz 3 werden jeweils die Wörter „der Betroffene“ durch die Wörter „die betroffene Person“ ersetzt.
40. Der bisherige § 57 wird § 75 und in Absatz 2 wird die Angabe „der §§ 901, 904 bis 910“ durch die Wörter „des § 802g Absatz 2 und § 802h“ ersetzt.
41. Der bisherige § 58 wird § 76 und in Absatz 1 Satz 2 wird die Angabe „§§ 60 bis 69“ durch die Angabe „§§ 78 bis 87“ ersetzt.
42. Der bisherige § 59 wird § 77 und wie folgt geändert:
- a) Absatz 1 wird wie folgt geändert:
 - aa) In Satz 2 werden die Wörter „Dem Betroffenen“ durch die Wörter „Der betroffenen Person“ ersetzt.
 - bb) In Satz 3 wird dem Wort „Gefahr“ das Wort „konkreten“ vorangestellt.
 - b) In Absatz 3 Satz 1 wird das Wort „muß“ durch das Wort „muss“ ersetzt.
43. Der bisherige § 60 wird § 78 und in Absatz 1 die Angabe „§§ 61 bis 69“ durch die Angabe „§§ 79 bis 87“ ersetzt.

44. Der bisherige § 61 wird § 79 und wie folgt geändert:

- a) In Absatz 2 wird nach dem Wort „Dienstfahrzeuge,“ das Wort „Luftfahrzeuge,“ eingefügt.
- b) Absatz 3 wird wie folgt gefasst:

„(3) Als Waffen sind Schlagstock, Pistole, Revolver, Gewehr, Maschinenpistole, Distanz-Elektroimpulsgerät sowie Sprengmittel, die vor Umsetzung von einem festen Mantel umgeben sind, zugelassen. Waffen können auf Anordnung des für Inneres zuständigen Ministeriums zeitlich befristet als Einsatzmittel erprobt werden.“

45. Der bisherige § 62 wird § 80 und wie folgt geändert:

- a) In Absatz 1 Satz 1 werden die Wörter „einem Weisungsberechtigten“ durch die Wörter „einer weisungsberechtigten Person“ ersetzt.
- b) Absatz 2 Satz 2 wird wie folgt gefasst:

„Befolgt die oder der Polizeivollzugsbedienstete die Anordnung trotzdem, so trifft sie oder ihn eine Schuld nur, wenn sie oder er erkennt oder wenn es nach den ihr oder ihm bekannten Umständen offensichtlich ist, dass dadurch eine Straftat begangen wird.“

- c) In Absatz 3 Satz 1 werden die Wörter „der Polizeivollzugsbedienstete dem Anordnenden“ durch die Wörter „die oder der Polizeivollzugsbedienstete der anordnenden Person“ ersetzt.

46. Der bisherige § 63 wird § 81 und das Wort „zuläßt“ durch das Wort „zulässt“ ersetzt.

47. Der bisherige § 64 wird § 82 und wie folgt geändert:

- a) Absatz 1 wird wie folgt geändert:
 - aa) In Satz 2 wird dem Wort „Gefahr“ das Wort „konkreten“ vorangestellt.
 - bb) In Satz 3 wird das Wort „Schußwaffengebrauchs“ durch das Wort „Schusswaffengebrauchs“ ersetzt.
- b) In Absatz 2 wird das Wort „Schußwaffen“ durch das Wort „Schusswaffen“ ersetzt und dem Wort „Gefahr“ das Wort „konkreten“ vorangestellt.
- c) Absatz 3 wird wie folgt geändert:
 - aa) In Satz 1 werden die Wörter „daß sich Unbeteiligte“ durch die Wörter „dass sich unbeteiligte Personen“ ersetzt.
 - bb) In Satz 2 wird das Wort „Schußwaffen“ durch das Wort „Schusswaffen“ ersetzt.

48. Der bisherige § 65 wird § 83 und in dem Satzteil des Satzes 1 vor Nummer 1 das Wort „daß“ durch das Wort „dass“ ersetzt.

49. Der bisherige § 66 wird § 84 und wie folgt geändert:

- a) In der Überschrift wird das Wort „Schußwaffengebrauch“ durch das Wort „Schusswaffengebrauch“ ersetzt.
- b) Absatz 1 wird wie folgt geändert:
 - aa) In Satz 1 wird das Wort „Schußwaffen“ durch das Wort „Schusswaffen“ ersetzt.
 - bb) In Satz 2 wird das Wort „Schußwaffengebrauch“ durch das Wort „Schusswaffengebrauch“ ersetzt.
- c) Absatz 2 wird wie folgt geändert:
 - aa) In Satz 1 wird das Wort „Schußwaffen“ durch das Wort „Schusswaffen“ ersetzt.
 - bb) In Satz 2 werden die Wörter „Lebensgefahr oder der gegenwärtigen Gefahr einer schwerwiegenden Verletzung der körperlichen Unversehrtheit“ durch die Worte „konkreten Gefahr für Leib oder Leben“ ersetzt.
- d) Absatz 3 wird wie folgt geändert:
 - aa) In Satz 1 wird das Wort „Schußwaffen“ durch das Wort „Schusswaffen“ ersetzt.
 - bb) In Satz 2 wird das Wort „Schußwaffengebrauch“ durch das Wort „Schusswaffengebrauch“ ersetzt und dem Wort „Gefahr“ das Wort „konkreten“ vorangestellt.
- e) Absatz 4 wird wie folgt geändert:
 - aa) In Satz 1 wird das Wort „Schußwaffengebrauch“ durch das Wort „Schusswaffengebrauch“ und das Wort „Unbeteiligte“ durch die Wörter „unbeteiligte Personen“ ersetzt.
 - bb) In Satz 2 wird das Wort „Schußwaffengebrauch“ durch das Wort „Schusswaffengebrauch“ und das Wort „Lebensgefahr“ durch die Wörter „konkreten Gefahr für das Leben einer Person“ ersetzt.

50. Der bisherige § 67 wird § 85 und wie folgt geändert:

- a) In der Überschrift wird das Wort „Schußwaffengebrauch“ durch das Wort „Schusswaffengebrauch“ ersetzt.
- b) Absatz 1 wird wie folgt geändert:
 - aa) Jeweils das Wort „Schußwaffen“ wird durch das Wort „Schusswaffen“ ersetzt.
 - bb) In Nummer 1 wird dem Wort „Gefahr“ das Wort „konkrete“ vorangestellt.

- cc) In den Nummern 3 Buchstabe b und 4 Buchstabe b wird jeweils das Wort „daß“ durch das Wort „dass“ ersetzt.
 - c) In Absatz 2 wird das Wort „Schußwaffen“ durch das Wort „Schusswaffen“ und die Angabe „Nr.“ durch das Wort „Nummer“ ersetzt.
51. Der bisherige § 68 wird § 86 und wie folgt geändert:
- a) In der Überschrift wird das Wort „Schußwaffengebrauch“ durch das Wort „Schusswaffengebrauch“ ersetzt.
 - b) Absatz 1 wird wie folgt geändert:
 - aa) In Satz 1 wird das Wort „Schußwaffengebrauch“ durch das Wort „Schusswaffengebrauch“ und das Wort „Unbeteiligte“ durch die Wörter „unbeteiligte Personen“ ersetzt.
 - bb) In Satz 2 wird das Wort „Schußwaffengebrauch“ durch das Wort „Schusswaffengebrauch“ und das Wort „Lebensgefahr“ durch die Wörter „konkreten Gefahr für das Leben einer Person“ ersetzt.
 - c) In Absatz 2 werden das Wort „Unbeteiligte“ durch die Wörter „Unbeteiligte Personen“ und die Angabe „§ 64 Abs. 3“ durch die Angabe „§ 82 Absatz 3“ ersetzt.
52. Der bisherige § 69 wird § 87 und wie folgt gefasst:

„§ 87

Sprengmittel

(1) Sprengmittel dürfen durch Spezialeinheiten gegen Personen zielgerichtet angewendet werden, wenn

1. diese Personen Schusswaffen oder Sprengmittel mit sich führen,
2. andere Waffen erfolglos angewendet wurden oder deren Gebrauch offensichtlich keinen Erfolg verspricht,
3. eine Gefährdung unbeteiligter Personen mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden kann und
4. der Einsatz von Sprengmitteln unerlässlich ist, um eine von den Personen ausgehende gegenwärtige konkrete Gefahr für das Leben der eingesetzten Polizeivollzugsbediensteten oder unbeteiligter Dritter abzuwehren.

Im Übrigen gilt § 84 mit Ausnahme von Absatz 4 entsprechend. Die Anwendung von Sprengmitteln ist spätestens unmittelbar nach dem Einsatz umfassend zu dokumentieren.

(2) Die Anwendung von Sprengmitteln gegen Personen auf der Flucht oder in einer Menschenmenge ist unzulässig. Andere Sprengmittel als nach § 79 Absatz 3 dürfen nicht gegen Personen angewendet werden.

(3) Die Anwendung von Sprengmitteln gegen Personen bedarf der Anordnung der Behördenleitung und der Zustimmung des für Inneres zuständigen Ministeriums.“

53. Der bisherige § 70 wird § 88.

54. Kapitel 6 wird aufgehoben.

55. Das bisherige Kapitel 7 wird Kapitel 6.

56. Der bisherige § 72 wird § 89.

57. Der bisherige § 76 wird § 90 und wie folgt geändert:

- a) In der Überschrift wird das Wort „Polizeivollzugsbeamten“ durch das Wort „Polizeivollzugsbediensteten“ ersetzt.
- b) Absatz 1 wird wie folgt geändert:
 - aa) In Satz 1 wird das Wort „Polizeivollzugsbeamten“ durch das Wort „Polizeivollzugsbediensteten“, die Angabe „Abs. 2“ durch die Angabe „Absatz 2“ und die Angabe „§ 77 Abs. 1“ durch die Angabe „§ 91 Absatz 1“ ersetzt.
 - bb) In Satz 2 wird das Wort „Polizeivollzugsbeamte“ durch das Wort „Polizeivollzugsbedienstete“ ersetzt.
- c) In Absatz 2 Satz 1 wird das Wort „Polizeivollzugsbeamten“ durch das Wort „Polizeivollzugsbediensteten“ ersetzt.

58. Der bisherige § 77 wird § 91 und wie folgt geändert:

- a) In der Überschrift wird das Wort „Polizeivollzugsbeamten“ durch das Wort „Polizeivollzugsbediensteten“ ersetzt.
- b) Absatz 1 Satz 1 wird wie folgt geändert:
 - aa) In dem Satzteil vor der Nummer 1 wird das Wort „Polizeivollzugsbeamte“ durch das Wort „Polizeivollzugsbedienstete“ ersetzt.
 - bb) In Nummer 2 wird jeweils die Angabe „Abs.“ durch das Wort „Absatz“ ersetzt.
 - cc) In Nummer 3 wird dem Wort „Gefahr“ das Wort „konkreten“ vorangestellt.

59. Der bisherige § 78 wird § 92 und wie folgt geändert:

- a) Die Überschrift wird wie folgt gefasst:

„§ 92 Zuständigkeit des Polizeipräsidiums, des Zentraldienstes der Polizei mit seiner Zentralen Bußgeldstelle und der Polizeivollzugsbediensteten“.
- b) Absatz 2 wird wie folgt gefasst:

„(2) Das Polizeipräsidium und der Zentraldienst der Polizei mit seiner Zentralen Bußgeldstelle sind zuständig für die Überwachung des Straßenverkehrs. Das Polizeipräsidium ist zudem zuständig für die Überwachung des Verkehrs auf schiffbaren Wasserstraßen.“

c) In Absatz 3 wird dem Wort „Gefahr“ das Wort „konkreten“ vorangestellt.

60. Die bisherigen §§ 82 bis 85 werden die §§ 93 bis 95.

61. Das bisherige Kapitel 8 wird Kapitel 7.

62. Die bisherigen §§ 87 und 88 werden die §§ 96 und 97.

63. Der bisherige § 89 wird § 98 und wie folgt gefasst:

„§ 98

Opferschutz, Zeugenschutz

(1) Die Polizei kann zur Abwehr einer erheblichen konkreten Gefahr für eine Person,

1. die Opfer einer Straftat wurde oder bei der davon auszugehen ist, dass sie in absehbarer Zeit Opfer einer Straftat werden kann, oder
2. bei der Maßnahmen nach dem Zeugenschutz-Harmonisierungsgesetz beendet wurden oder bei der erst nach rechtskräftigem Verfahrensabschluss Schutzmaßnahmen erforderlich werden,

auf Anordnung der Behördenleitung Urkunden und sonstige Dokumente zum Aufbau und zur Aufrechterhaltung einer vorübergehend geänderten Identität herstellen, vorübergehend verändern und die entsprechend geänderten Daten verarbeiten, wenn die Person für diese Schutzmaßnahme geeignet ist.

(2) Die zu schützende Person nach Absatz 1 darf unter der vorübergehend geänderten Identität am Rechtsverkehr teilnehmen. Soweit erforderlich, können Maßnahmen nach Absatz 1 auch auf Angehörige dieser Person oder ihr sonst nahestehende Personen erstreckt werden.

(3) § 52 Absatz 2 findet auf die mit dem Schutz betrauten Polizeivollzugsbediensteten entsprechende Anwendung, soweit dies zur Vorbereitung, Durchführung, Lenkung oder Absicherung der Schutzmaßnahmen erforderlich ist.“

Artikel 2

Änderung des Ordnungsbehördengesetzes

Das Ordnungsbehördengesetz in der Fassung der Bekanntmachung vom 21. August 1996 (GVBl. I Nr. 21 S. 266), das zuletzt durch Artikel 5 des Gesetzes vom 15. Oktober 2018 (GVBl. I Nr. 22 S. 26) geändert worden ist, wird wie folgt geändert:

1. Im Inhaltsverzeichnis wird die Angabe zu § 2 durch die Abgabe „§ 2 Verhältnis zu anderen Behörden“ ersetzt.
2. § 2 wird wie folgt geändert:
 - a) In der Überschrift werden die Wörter „Vollzugshilfe der Polizei“ durch die Wörter „Verhältnis zu anderen Behörden“ ersetzt.
 - b) In Satz 1 wird die Angabe „§§ 50 bis 52“ durch die Angabe „§§ 68 bis 70“ ersetzt.
 - c) Dem Satz 1 wird der folgende Satz angefügt:
 „Die Ordnungsbehörden sind zur vernetzten Zusammenarbeit mit anderen Sicherheitsbehörden (Polizei, Verfassungsschutz, Staatsanwaltschaften und Ordnungsbehörden) verpflichtet, soweit dies rechtlich möglich ist.“
3. § 23 wird wie folgt gefasst:

„§ 23

Geltung des Brandenburgischen Polizeigesetzes

Folgende Vorschriften des Brandenburgischen Polizeigesetzes gelten entsprechend für die Ordnungsbehörden, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist:

1. Von den Vorschriften über die Befugnisse der Polizei
 - a. § 14 (Befragung und Auskunftspflicht),
 - b. § 15 (Identitätsfeststellung) mit Ausnahme des Absatzes 1 Nummer 4, 5, 6, 7, 8 und 9,
 - c. § 17 (Prüfung von Berechtigungsscheinen und sonstigen Urkunden),
 - d. § 18 (Vorladung) mit Ausnahme des Absatzes 1 Nummer 2 und des Absatzes 3 Satz 1 Nummer 2,
 - e. § 20 (Platzverweisung und Aufenthaltsverbot) mit Ausnahme des Absatzes 2 Nummer 1 und 3 und des Absatzes 3,
 - f. §§ 21 bis 24 (Gewahrsam) mit den Einschränkungen
 - aa. in § 21 Absatz 1 Nummer 3 auf die Platzverweisung und das Aufenthaltsverbot nach § 20 Absatz 1 und Absatz 2 Nummer 2 sowie
 - bb. in § 24 Absatz 1 Nummer 3 unter der Maßgabe, dass die Dauer der Freiheitsentziehung vier Tage nicht überschreiten darf,
 - g. §§ 25 bis 28 (Durchsuchung von Personen, Sachen und Wohnungen) mit Ausnahme des § 27 Absatz 1 Satz 1 Nummer 5,

- h. §§ 29 bis 32 (Sicherstellung).
2. Von den Vorschriften über die Datenverarbeitung
- a. entsprechende Anwendung der Vorschriften des Kapitel 2 Abschnitt 2 Unterabschnitt 1 (Allgemeine Vorschriften zur Datenverarbeitung und zum Datenschutz), soweit die Ordnungsbehörden Gefahrenabwehr betreiben,
 - b. § 43 (Allgemeine Befugnis zur Datenerhebung) und § 44 (Offene Bild- und Tonaufnahmen oder -aufzeichnungen) mit Ausnahme des § 44 Absatz 1 Nummer 2 und Absatz 2, 3 und 6 sowie mit der Einschränkung des Absatzes 4 durch die Erfordernisse der Zustimmung des für Inneres zuständigen Ministeriums und einer zwei jährigen Pilotphase mit einer Erforderlichkeitsanalyse unter dessen Aufsicht,
 - c. § 56 (Allgemeine Regeln über die Dauer der Datenspeicherung),
 - d. § 57 (Zweckbindung bei der Datenspeicherung, Datenveränderung und Datennutzung),
 - e. § 58 (Speicherung, Veränderung und Nutzung von Daten) mit Ausnahme der Absätze 2, 3 und 4,
 - f. §§ 60 bis 63 (Datenübermittlung) mit Ausnahme des § 63 Absatz 3,
 - g. § 67 (Berichtigung, Löschung und Sperrung von Daten).“
4. § 43 wird wie folgt gefasst:

„§ 43

Einschränkung von Grundrechten

Durch dieses Gesetz werden die Grundrechte auf

- 1. körperliche Unversehrtheit (Artikel 2 Absatz 2 Satz 1 des Grundgesetzes, Artikel 8 Absatz 1 Satz 1 der Verfassung des Landes Brandenburg),
- 2. Freiheit der Person (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes, Artikel 9 Absatz 1 Satz 1 der Verfassung des Landes Brandenburg),
- 3. Freizügigkeit (Artikel 11 des Grundgesetzes, Artikel 17 der Verfassung des Landes Brandenburg),
- 4. Unverletzlichkeit der Wohnung (Artikel 13 Abs. 1 des Grundgesetzes, Artikel 15 Abs. 1 der Verfassung des Landes Brandenburg),
- 5. Datenschutz (Artikel 11 der Verfassung des Landes Brandenburg) und
- 6. Eigentum (Artikel 14 des Grundgesetzes, Artikel 41 Absatz 1 Satz 1 der Verfassung des Landes Brandenburg)

eingeschränkt.“

Artikel 3

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Potsdam, den [Datum der Ausfertigung]

Die Präsidentin des Landtages Brandenburg

Britta Stark

Begründung

A. Allgemeiner Teil

Der mit der Polizeireform des Jahres 2011 prognostizierte erhebliche Rückgang der Kriminalität im Land Brandenburg hat sich bisher nicht so bestätigt. Zwar sind die registrierten Straftaten von 2016 (185.831) auf 2017 (175.003) zurückgegangen. Es ist allein im Kriminalitätshellfeld aber immer noch ein Schaden von 316.686.993 Euro zu verzeichnen und die Anzahl der Tatverdächtigen mit rund 67.000 Personen bleibt auf einem hohen Niveau. Während die Fallzahlen beim Diebstahl zurückgegangen sind, bleiben die Schäden weiterhin hoch.

Diebstahl	2008	2009	2012	2013	2016	2017
Schäden in Mio. Euro	86,5	84,5	97,9	114,6	115,0	100,9

Bei den Vermögensdelikten nahm die Schadenshöhe von rund 87 Millionen Euro in 2016 auf rund 146 Millionen Euro in 2017 erheblich zu. Beim Geldkreditbetrug beispielsweise hatte sich der Schaden auf über 18 Millionen Euro fast verdreifacht und auch im Bereich der Untreue erhöhte sich die Schadenssumme erheblich.

Im Jahr 2017 wurden durch das Landeskriminalamt 12 Verfahrenskomplexe der Organisierten Kriminalität bearbeitet. Im Rahmen dieser Verfahren wurden 131 Straftaten verfolgt, von denen fünf Verfahren dem Kriminalitätsbereich der Eigentumskriminalität, vier Verfahren dem Rauschgifthandel und -schmuggel, ein Verfahren der Gewaltkriminalität, ein Verfahren der Kriminalität im Zusammenhang mit dem Nachleben und ein Verfahren der sonstigen Kriminalität zuzurechnen sind. Es wurden 131 Tatverdächtige ermittelt, von denen 47 deutsche Staatsangehörige sind. Der Organisierten Kriminalität zuzuordnende Straftaten verursachten 2017 einen Schaden in Höhe von 6,02 Millionen Euro (2016: 1,3 Millionen Euro). Kriminelle Erträge wurden in Höhe von 3,2 Millionen Euro durch die Täter erlangt (2016: 0,84 Millionen Euro). Von diesen Erträgen wurden 125.000 Euro (2016: 171.000 Euro) vorläufig gesichert.

Bei der Grenzüberschreitenden Kriminalität spielen in Brandenburg folgende Straftaten eine erhebliche Rolle: Im Landeskriminalamt werden mehrere Verfahren gegen unterschiedliche Tätergruppierungen geführt, denen Diebstähle von Fahrzeugen der Marken Audi, Skoda, VW sowie Mazda angelastet werden. Die Verfahren richten sich hauptsächlich gegen polnische Tätergruppierungen. Weiterhin wurden LKW, Baumaschinen und landwirtschaftliche Nutzfahrzeuge entwendet. Aufgrund des hohen Zeitwertes der Kraftfahrzeuge und Maschinen entsteht trotz geringerer Fallzahlen ein hoher wirtschaftlicher Schaden. Die diesbezüglich im Landeskriminalamt geführten Verfahren richten sich sowohl gegen polnische als auch gegen litauische Tatverdächtige. Im Jahr 2017 wurden zudem insgesamt 26 Angriffe auf Geldausgabeautomaten verübt. Die Tatorte sind auf das Land Brandenburg gleichmäßig verteilt. Das Landeskriminalamt ist darüber hinaus landesweit für die Bearbeitung von Straftaten mit dem Modus Operandi „Planenschlitzen“ zuständig. Der örtliche Schwerpunkt liegt auf Parkplätzen und Raststätten entlang der Bundesautobahnen im Westen, Süden und Osten Brandenburgs. In unregelmäßigen Abständen sind auch Angriffe auf Lastkraftwagen und deren Ladungen festzustellen, die abseits von Bundesautobahnen auf Autohöfen oder in Gewerbegebieten geparkt wurden. Größtenteils richten sich die Ermittlungen gegen polnische Täter-

gruppierungen. Die Schäden des Planenschlitzens haben sich auf rund 1,3 Millionen Euro fast verdoppelt.

Die Politisch motivierte Kriminalität hat in den vergangenen Jahren in Brandenburg erheblich zugenommen. Von 2011 bis 2017 war ein Anstieg der Straftaten um rund 60 Prozent zu verzeichnen.

Politisch-motivierte Kriminalität	2011	2012	2013	2014	2015	2016	2017
PMK-rechts	1.140	1.354	1.379	1.281	1.581	1.664	1.488
PMK-links	138	166	211	360	223	244	361
PMK-sonstige	131	102	192	252	156	217	349
Politisch motivierte Ausländerkriminalität	1	5	4	10	12	38	51
PMK-gesamt	1.410	1.627	1.786	1.903	1.972	2.163	2.249

Auch die Politisch-motivierte Gewaltkriminalität hat ein hohes Niveau. Diese hat sich mehr als verdoppelt.

Politisch-motivierte Gewaltkriminalität	2011	2012	2013	2014	2015	2016	2017
PMK-rechts	36	58	45	73	129	167	124
PMK-links	25	27	15	30	48	53	24
PMK-gesamt	61	88	62	108	186	260	176

Im Jahr 2017 sind 44 Straftaten gemeldet worden, bei denen Bezüge zur Politisch motivierten Kriminalität – religiöse Ideologie – gesehen werden. Dabei handelt es sich um 18 terroristische Straftaten (§§ 89a, 89b und 129a i. V. m. § 129b StGB), 10 Gewaltdelikte (§§ 177, 212, 223, 224 StGB) und 16 sonstige Straftaten (§§ 126, 130, 167, 241, 303 StGB). Sieben weitere Straftaten weisen Bezüge zur Politisch motivierten Kriminalität – ausländische Ideologie – auf. Dabei handelt es sich um zwei terroristische Straftaten (§§ 129a i. V. m. § 129b StGB), zwei Gewaltdelikte (§§ 223, 224 StGB) und drei sonstige Straftaten (§§ 185, 241 StGB und Vereinsgesetz).

Während die Linksextremisten ein leicht steigendes Personenpotenzial zu verzeichnen haben, ist das rechtsextremistische Personenpotenzial erheblich angestiegen. Besonders dynamisch ist das islamistische Personenpotential. Gegenwärtig gibt es bereits 130 Islamisten in Brandenburg. 51 Islamisten kommen aus der Russischen Föderation zumeist Tschetschenen, 40 aus Syrien sowie 16 aus Afghanistan und Pakistan. Die Personengruppe der bekannten „Gefährder“ und „relevanten Personen“ verteilt sich auf insgesamt sechs Landkreise bzw. kreisfreie Städte und liegt im einstelligen Bereich. Die Tendenz beim islamistischen Personenpotential ist weiter steigend. Die islamistische Szene in Brandenburg ist eng mit der Szene in Berlin verbunden. Bis Ende 2017 ist die Zahl der Salafisten in Berlin auf 900 gestiegen.

Personenpotential	2013	2014	2015	2016	2017
--------------------------	-------------	-------------	-------------	-------------	-------------

in Brandenburg					
rechts	1.125	1.160	1.230	1.390	1.540
links	485	490	490	500	520
islamistisches	30	40	70	100	130

Der rapide Anstieg beim extremistischen und islamistischen Personenpotential lässt befürchten, dass Politisch motivierte Kriminalität, verfassungsfeindliche Handlungen und auch Terrorismus im Kriminalitätsraum Brandenburg-Berlin zunehmen werden. Nicht nur Rechtsextremisten sondern auch Linksextremisten und Islamisten sind verfassungsfeindlich eingestellt und streben danach, ihre verfassungsfeindlichen Ideologien zu verbreiten. Unter diesen Bedingungen ist ein sich gegenseitiges Hochschaukeln der Extremisten und Islamisten möglich.

Das Personenpotenzial des islamistischen Extremismus setzt sich in Brandenburg aus Einzelpersonen zusammen, die teilweise Kennverhältnisse pflegen und informationell vernetzt sind. Es liegen Erkenntnisse vor, wonach einzelne Personen im Namen des Islamischen Staates (IS) bzw. diesem angeschlossenen Gruppen Radikalisierungs- und Rekrutierungshandlungen vornahmen und für die Ausreise in das Einflussgebiet des IS warben. Zudem wurden bereits unterschiedliche Arten von Geldtransfers in Richtung der Krisen- und Kriegsregionen Syriens und des Iraks festgestellt, bei denen die Möglichkeit besteht, dass diese islamistischen Terrororganisationen zugutekommen könnten.

In Brandenburg geht vom Islamismus aus dem Kaukasus die größte abstrakte Gefahr aus. Dessen Personenkreis reist über die Ukraine, Weißrussland und Polen in Deutschland ein. Einige von diesen Personen haben Kriegserfahrung in Syrien und im Irak gesammelt. In der Ukraine haben Tschetschenen auf beiden Seiten der Front als Söldner gedient. Die Brandenburger Sicherheitsbehörden sind zu der Einschätzung gekommen, dass bereits im Land befindliche Angehörige der Russischen Föderation mit tschetschenischer Volkszugehörigkeit sowohl in den Kommunen als auch in der Aufnahmeeinrichtung erhebliche Probleme verursachen. Dies schließt gewaltbereites Verhalten gegenüber Bewohnern anderer Herkunftsländer, Gewalttätigkeiten in der Partnerschaft, mangelnde Integrationswilligkeit und die Nichtmitwirkung bei bestehender Ausreisepflicht ein. Es besteht die Gefahr der Abschottung, existiert eine sehr gute überregionale Vernetzung, erfolgt eine zum Teil massive Beeinflussung gemäßigter Tschetschenen und die Anwerbung durch Islamisten. So ist Brandenburg inzwischen zu einem ländlichen Rückzugsraum für eine erhebliche Zahl von Islamisten und Salafisten tschetschenischer Herkunft geworden.

Darüber hinaus versucht der Verein „Sächsische Begegnungsstätte e. V.“, der der Muslimbruderschaft nahesteht und dem legalistischen Islamismus zugerechnet wird, auch in Brandenburg Moscheegemeinden aufzubauen. In Brandenburg an der Havel, Luckenwalde, Senftenberg und zukünftig wohl auch in Cottbus werden Anlaufstellen eingerichtet. Es besteht die Gefahr, dass in Brandenburg Islamisten aus dem Osten und dem Süden gemeinsame Ziele verfolgen und Strukturen aufbauen, um den wahhabitisch-salafistischen Islam insbesondere unter muslimischen Flüchtlingen zu verbreiten, deren Integration zu verhindern, Konflikte herbeizuführen und die Gesellschaft in Brandenburg zu destabilisieren.

Eine besondere Gefahr für die öffentliche Sicherheit stellt der Terrorismus dar. Terroristen verüben Gewalttaten, die sich zumindest mittelbar gegen Leib und Leben richten, um politische Ziele zu erreichen. Der islamistische Terrorismus ist gegenwärtig die größte Gefahr wegen seines enormen Schadenspotentials. Die Anschläge in Paris, Nizza, der Normandie, Brüssel, Hannover, Essen, Würzburg, Ansbach und Berlin zeigen, wie verwundbar die freie Gesellschaft ist. Die Opfer von Terroranschlägen sind für die islamistischen Terroristen vor allem Mittel zum Zweck. Sie wollen die Autorität ihrer Organisation in der islamistischen Szene durch Anschläge gegen den westlichen Feind erhöhen und dadurch ihr Rekrutierungspotential erweitern. Die Bevölkerung soll eingeschüchtert werden. Hoheitliche Stellen sollen zu überzogenen Abwehrmaßnahmen provoziert und ihre Legitimität geschwächt werden. Dies zielt auf die Destabilisierung der staatlichen und gesellschaftlichen Infrastruktur ab.

In einer Europol-Veröffentlichung („Changes in modus operandi of Islamic State terrorist attacks“) vom Januar 2016 und überarbeitet im November des gleichen Jahres heißt es, dass die Pariser Angriffe und die anschließenden Nachforschungen auf eine Verlagerung hin zu einer breiteren Strategie des Islamischen Staates auf globaler Ebene deuten. Dieser greife insbesondere Frankreich an, aber auch Angriffe auf andere Mitgliedstaaten der EU wie Belgien, Deutschland, die Niederlande und das Vereinigte Königreich seien in naher Zukunft zu erwarten. Viele Personen waren zunächst an schwerer und organisierter Kriminalität beteiligt, bevor sie durch terroristische Vergehen in Erscheinung traten. Der Islamische Staat habe laut nachrichtendienstlichen Informationen ein externes Aktionskommando aufgebaut, das für Angriffe in der Weise von Spezialeinheiten im internationalen Umfeld ausgebildet wurde. Die Terrorzellen operierten größtenteils lokal. Außerdem bestehe weiterhin eine Bedrohung durch Einzeltäter. Neben Ausbildungseinrichtungen in Syrien gebe es auch kleinere Ausbildungslager in der EU und in den Balkanländern. Die Ausbildung der Rekruten bestehe aus eingeführten Techniken der Kriegsführung in der Handhabung von Waffen, Sprengstoff und spezifischen Tötungsmethoden, die Enthauptungen einschließen. Operatives Personal werde auch in verdeckten Handlungsweisen und in Gegenaufklärung geschult. Überlebenstraining ermögliche den Ausbildern, die Fitness und die Entschlossenheit der aufstrebenden Mitglieder des Islamischen Staates zu überprüfen. Sportaktivitäten werden für Kampf- und Verhörwiderstandstraining genutzt. Die Rückkehr von islamistischen Kämpfern und ihren Familien aus den Kriegsgebieten in Syrien und dem Irak wird im Hinblick auf künftige Bedrohungen als kritisch angesehen. Außerdem sei immer noch mit anderen Terrororganisationen wie al-Qaida zu rechnen.

Weiterhin sind Deutschland und auch Brandenburg von Aktivitäten fremder Nachrichtendienste im Bereich der Wirtschafts- und politischen Spionage betroffen. Die Bundeshauptstadt Berlin liegt im Zentrum Brandenburgs, so dass ein zusätzlicher großer Anziehungspunkt für ausländische Dienste besteht. Neben Aktivitäten russischer, iranischer und chinesischer Geheimdienste ist eine Zunahme von Ausspähversuchen durch die Türkei zu registrieren. Weitere Staaten stehen im Verdacht, Wirtschaft und Politik in Deutschland auszuspionieren. Deutschen Unternehmen soll jährlich ein Schaden in zweistelliger Milliardenhöhe durch Wirtschaftsspionage entstehen.

Außerdem werden durch Wirtschaftskriminalität jedes Jahr in Brandenburg erhebliche Schäden verursacht.

Wirtschaftskriminalität	2011	2012	2013	2014	2015	2016
Schäden in Mio. Euro	183,2	185,7	125,0	332,5	91,0	195,0

Beteiligungs- und Kapitalanlagebetrug, Untreue sowie Straftaten nach dem AktG, GenG, GmbHG, HGB, RechnungslegungsG stellen hierbei einen besonderen Schwerpunkt dar. Der Schutz der deutschen und brandenburgischen Wirtschaft vor Angriffen ausländischer Mächte und vor Wirtschaftskriminalität ist ein überragend wichtiges Ziel, denn wirtschaftlicher Wohlstand bildet eine wichtige Grundlage für den sozialen Zusammenhalt des Landes.

Der zunehmende Einsatz von Informations- und Kommunikationstechnologien in der modernen Informationsgesellschaft bedeutet neben vielen positiven Fortschritten auch, dass die Internet- und Cyberkriminalität weiter zunehmen wird. Die Integrität informationstechnischer Systeme, traditionelle Rechtsgüter wie das Vermögen, Persönlichkeits- und Urheberrechte sowie der Datenschutz sind erheblich gefährdet. Außerdem gibt es heute eine Vielzahl von illegalen Inhalten im Internet wie den Erwerb von Drogen, Waffen, Sprengstoff, gestohlene Kreditkartendaten, gefälschte Ausweise und Kinderpornografie sowie Auftragsmorde und weitere kriminelle Dienstleistungen der Online-Schwarzmärkte. Kriminelle brauchen keine speziellen Kenntnisse mehr und können vom „Rundumsorglos-Paket des Darknets“ profitieren. Über das „Internet der Dinge“ können sie die Bürger, Unternehmen, Behörden und die Politik viel unmittelbarer schädigen. Die Verbreitung und der Einsatz von Schadprogrammen auf Opfersystemen bilden eine wichtige Grundlage für die Begehung von Internet- und Cyberkriminalität. Die häufigsten Verbreitungswege von Schadprogrammen sind Anhänge in Spam-Mails sowie die vom Anwender unbemerkte Infektion beim Besuch von präparierten Webseiten. Das Ausspähen und Abfangen von Daten, der Diebstahl digitaler Identitäten, das sogenannte „Phishing“ und „Skimming“, die digitale Erpressung unter Einsatz sogenannter Ransomware, die massenhafte Fernsteuerung von Computern durch Botnetze sowie Angriffe auf die Verfügbarkeit von Webseiten, Internetdiensten und Netzwerken (DDoS-Angriffe) sind Taten von erheblicher wirtschaftlicher und sozialer Schädlichkeit.

In diesem Kriminalitätsbereich ist mit einer hohen Dunkelfeldziffer zu rechnen. In der Studie „Tatort Internet: Kriminalität verursacht Bürgern Schäden in Milliardenhöhe“ („DIW WOCHENBERICHT“ Nr. 12/ 2015 vom 23. März 2015) wurde auf Grundlage von Befragungen berechnet, dass es in den vier wichtigen Bereichen der Internetkriminalität – Phishing, Identitätsbetrug, Waren- und Dienstleistungs-betrug und Schadsoftware – jährlich bundesweit etwa 14,7 Millionen Fälle gebe und sich der Schaden auf insgesamt 3,4 Milliarden Euro belaufe. In Brandenburg wären dies pro Jahr 16.763 Fälle je 100.000 Einwohner (insgesamt rund 418.000 Fälle) und ein Schaden von 36 Euro je Einwohner (insgesamt rund 90 Mio. Euro). Durch Cyberspionage und Sabotage entstehen deutschen Unternehmen jedes Jahr gewaltige Schäden. Laut einer Studie des Digitalverbandes Bitkom und des Bundesamtes für Verfassungsschutz wird mehr als jedes zweite Unternehmen in Deutschland angegriffen, ausspioniert, sabotiert oder bestohlen. Der Schaden betrage 55 Milliarden Euro. Auch im Bereich der Organisierten, Grenzüberschreitenden und Politisch-motivierten Kriminalität spielen Cyberfähigkeiten im Rahmen internationaler, arbeitsteiliger Strukturen eine immer wichtigere Rolle. Cyberterrorismus und staatlich unterstützte Cyberangriffe sind besonders schwerwiegende Straftaten in diesem Kriminalitätsbereich.

Diese Entwicklungen bei den genannten Kriminalitätsphänomenen machen es notwendig die oben aufgeführten Gesetzesänderungen im Polizeigesetz und Ordnungsbehördengesetz vorzunehmen. Die Vorgaben der Europäischen Union und des Bundesverfassungsgerichtes sind umzusetzen. Außerdem dienen die Änderungen dazu, ein Auseinanderfallen des Normenbestandes im Polizeirecht zu den Regelungen des Bundes (BKAG) und der anderen Bundesländer zu verhindern. In Bayern, Baden-Württemberg, Rheinland-Pfalz und Sachsen-Anhalt wurden die Polizeigesetze an neuere Entwicklungen angepasst. In Nordrhein-Westfalen und Niedersachsen befinden sich Gesetzentwürfe zum Polizeigesetz in der parlamentarischen Beratung. Das BKAG und das Bayerische Polizeiaufgabengesetz zeigen im Rechtsvergleich die meisten Fortentwicklungsmöglichkeiten auf. Diese werden für das Brandenburgische Polizeigesetz größtenteils aufgegriffen. Der Begriff „drohende Gefahr“ wird jedoch nicht übernommen.

In diesem Kontext hat sich die Polizeiarbeit in den vergangenen Jahrzehnten erheblich verändert. Insbesondere die oben aufgeführten Kriminalitätsphänomene haben dazu geführt, dass die Polizei im Bereich der selektiven Kriminalprävention verstärkt strategisch auf Grundlage kriminalpräventiver Handlungskonzepte und operativ durch Präventionsplanungen handelt. Um diese Entwicklung im Polizeigesetz nachzuvollziehen, werden

- das Merkmal „Kriminalitätsphänomen“ in das Polizeigesetz eingeführt und definiert,
- die schwerwiegenden Kriminalitätsphänomene des Terrorismus und der Politisch motivierten Kriminalität, der Organisierten und schwerwiegenden Grenzüberschreitenden Kriminalität sowie der schwerwiegenden Wirtschafts- und Cyberkriminalität definiert und in den Befugnisnormen verankert,
- polizeiliche Maßnahmen zur „Verhütung oder vorbeugenden Bekämpfung von Straftaten oder Kriminalitätsphänomenen“ an kriminalpräventive Handlungskonzepte und operative Präventionsplanungen gebunden und
- die Gefahrenabwehr im digitalen Raum ausdrücklich als polizeiliche Aufgabe geregelt.

Wichtige Begriffe werden zusammengefasst vorne im Gesetz definiert. So wird der polizeiliche Gefahrenbegriff konkretisiert. In der Entscheidung des Bundesverfassungsgerichtes zum Bundeskriminalamtgesetz wurden die Kriterien des Begriffs der „konkreten Gefahr“ hinsichtlich der Online-Durchsuchung fortentwickelt, der die maßgebliche Eingriffsvoraussetzung in den Polizeigesetzen bildet. Weiterhin werden im Gesetz die abstrakte und die erhöhte abstrakte Gefahr definiert. Darüber hinaus werden auch Definitionen der EU-Datenschutzrichtlinie für den Bereich der Polizei übernommen.

Die EU-Datenschutzrichtlinie für den Bereich der Polizei und die Rechtsprechung des Bundesverfassungsgerichtes werden im Polizeigesetz in Kapitel 2 Abschnitt 2 zur Datenverarbeitung als neuer Unterabschnitt 1 „Allgemeine Vorschriften zur Datenverarbeitung und zum Datenschutz“ geregelt und durch einen Verweis im Ordnungsbehördengesetz entsprechend auf die gefahrenabwehrrechtlichen Maßnahmen der Ordnungsbehörden angewendet. Der Unterabschnitt 1 hat die folgenden Regelungsinhalte:

- Grundsätze der Verarbeitung personenbezogener Daten und besonders geschützte Datenkategorien,
- Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung,
- Benachrichtigungspflichten,
- Auskunftsrecht und Akteneinsicht,
- Verzeichnis von Verarbeitungstätigkeiten, Protokollierung und Kontrolle durch die oder den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht,
- automatisierte Verfahren der Datenverarbeitung,
- Errichtungsanordnung für Dateien und Datenschutz-Folgenabschätzung,
- Anwendung des Brandenburgischen Datenschutzgesetzes und
- parlamentarische Kontrolle.

Weiterhin werden die polizeilichen Befugnisnormen im Sinne der Nummern 1 bis 3 angepasst und insbesondere der folgende Katalog an Maßnahmen umgesetzt, die zum Teil je nach Schwere des Eingriffs an einen Richtervorbehalt gebunden sowie ministeriellen und parlamentarischen Kontrollsystemen unterworfen werden:

- Anpassung der Regelung zur Videoüberwachung: Übersichtsaufzeichnungen bei Veranstaltungen und Ansammlungen, Ausweitung der Videoüberwachung im öffentlichen Raum, Einbeziehung intelligenter Videoüberwachungssysteme einschließlich des Abgleichs mit biometrischen Daten von Straftätern und Gefährdern sowie Verlängerung der Datenspeicherfrist;
- Regelung des Einsatzes von Bodycams mit Pre-Recording-Funktion einschließlich der Verwendung in Wohnungen;
- Ermöglichung sogenannter verdachts- und anlassunabhängiger Kontrollen („Schleierfahndung“) im gesamten öffentlichen Verkehrsraum des Landes Brandenburg;
- Ausweitung der Frist des Polizeigewahrsams auf einen Monat mit der Möglichkeit, bei einem weiteren Vorliegen der Tatbestandsvoraussetzungen Verlängerungen herbeizuführen;
- Einführung von Rechtsgrundlagen zur elektronischen Aufenthaltsüberwachung einschließlich einer Strafvorschrift für Maßnahmenverstöße sowie zur Verhängung eines Aufenthaltsgebotes und Kontaktverbotes insbesondere für als Gefährder eingestufte Personen;
- Kodifizierung der Meldeauflage mit einem hinreichend weiten zeitlichen Aufwandsraum;
- Regelung der Identitätsfeststellung durch die Erhebung genetischer Daten;

- Ermöglichung der Durchsuchung räumlich getrennter elektronischer Speichermedien;
- Kodifizierung der Sicherstellung von Forderungen und anderen Vermögensrechten durch Pfändung sowie der Postsicherstellung;
- Schaffung einer klaren Rechtsgrundlage für die Quellen-Telekommunikationsüberwachung und Online-Durchsuchung;
- Regelungen zur präventiven Öffentlichkeitsfahndung, zum Einsatz und zur Abwehr unbemannter Luftfahrtsysteme und zur Möglichkeit des zielgerichteten Einwirkens auf Straftäter mit Sprengmitteln in Fällen des Terrorismus oder sonstiger Schwerstkriminalität;
- Konkretisierung des Einsatzes von Vertrauenspersonen als Folge verfassungsrechtlicher Rechtsprechung und der NSU-Erkenntnisse;
- Ermöglichung projektbezogener gemeinsamer Dateien mit dem Verfassungsschutz Brandenburg im Bereich Terrorismus und geheimdienstlicher Tätigkeit;
- Regelung der in der EU-Datenschutzrichtlinie für den Bereich der Polizei niedergelegten Voraussetzungen für das sogenannte „Profiling“;
- Opfer- und Zeugenschutzregelung zur Herstellung und Veränderung von Urkunden und sonstigen Dokumenten für den Aufbau und die Aufrechterhaltung einer vorübergehend geänderten Identität.

Im Ordnungsbehördengesetz werden die Verweise auf das Polizeigesetz angepasst. Bestimmte Maßnahmenenerweiterungen bei der Polizei (z. B. Frist des Polizeigewahrsams und Videoüberwachung) werden für die Ordnungsbehörden nicht übernommen. Der Einsatz von Bodycams wird nach der Zustimmung des für Inneres zuständigen Ministeriums und einer Pilotphase in den betroffenen Kommunen auch den Ordnungsbehörden ermöglicht, wenn dieser erforderlich ist.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Brandenburgischen Polizeigesetzes)

Zu Nummer 1 (Inhaltsübersicht)

Die amtliche Inhaltsübersicht wird an die vorgenommenen Ergänzungen und Umstellungen sowie die sich daraus ergebende neue Paragrafenreihung angepasst.

Zu Nummer 2 (§ 1 Aufgaben der Polizei)

§ 1 Absatz 1 BbgPolG wird angepasst. So werden in Satz 1 klarstellend die Wörter „allgemeine oder im Einzelfall bestehende“ Gefahren für die öffentliche Sicherheit und Ordnung eingefügt. Auf der Ebene der Aufgabeneröffnung ist also das Vorliegen einer abstrakten Gefahr ausreichend.

Satz 2 wird nun klarer durch die Nummern 1 bis 5 strukturiert. In der Nummer 1 wird der Schutz wichtiger Verfassungsgüter wie im Polizeigesetz des Freistaates Sachsen eingefügt. Geschützt wird die freiheitliche demokratische Grundordnung

sowie die ungehinderte Ausübung der Grundrechte und der staatsbürgerlichen Rechte gewährleistet.

Freiheitliche demokratische Grundordnung ist eine Ordnung, die unter Ausschluss jeglicher Gewalt- und Willkürherrschaft eine rechtsstaatliche Herrschaftsordnung auf der Grundlage der Selbstbestimmung des Volkes nach dem Willen der jeweiligen Mehrheit und der Freiheit und Gleichheit darstellt. Zu den grundlegenden Prinzipien dieser Ordnung sind mindestens zu rechnen:

- die Achtung vor den im Grundgesetz konkretisierten Menschenrechten, vor allem vor dem Recht der Persönlichkeit auf Leben und freie Entfaltung,
- die Volkssouveränität,
- die Gewaltenteilung,
- die Verantwortlichkeit der Regierung,
- die Gesetzmäßigkeit der Verwaltung,
- die Unabhängigkeit der Gerichte,
- das Mehrparteienprinzip und
- die Chancengleichheit für alle politischen Parteien mit dem Recht auf verfassungsmäßige Bildung und Ausübung einer Opposition.

Grundrechte sind wesentliche Rechte, die Mitgliedern der Gesellschaft gegenüber dem Staat als beständig, dauerhaft und einklagbar garantiert werden. In erster Linie sind sie Abwehrrechte des Bürgers gegen den Staat, sie können sich jedoch auch auf das Verhältnis der Bürger untereinander auswirken. Die Grundrechte werden im Grundgesetz und in der Verfassung des Landes Brandenburg gewährleistet.

Artikel 33 Absatz 1 des Grundgesetzes erwähnt die staatsbürgerlichen Rechte, die jeder Deutsche hat. Bei den staatsbürgerlichen Rechten handelt es sich um die dem Staatsbürger vom Staat garantierte Rechtsstellung, auch gegenüber den Trägern der öffentlichen Gewalt. Davon erfasst ist unter anderem das Recht auf Mitgestaltung des Staates durch Teilnahme an Wahlen, auf Gründung politischer Vereine und auf Zugang zu den öffentlichen Ämtern.

Nummer 2 erfasst die Vorbereitungshandlungen für die Hilfeleistungen und das Handeln in Gefahrenfällen.

In Nummer 3 wird die selektive Kriminalprävention als „Straftaten und Kriminalitätsphänomene zu verhüten und vorbeugend zu bekämpfen“ definiert. Im Rahmen der selektiven Kriminalprävention durch die Polizei spielt nicht nur die Straftatenverhütung, sondern auch die Ausleuchtung und Zerschlagung oder zumindest Schwächung der Strukturen von Kriminalitätsphänomenen eine wichtige Rolle. Durch die Einführung des Begriffs „Kriminalitätsphänomen“ können bereits sehr frühzeitig erst in der Entstehung befindliche Kriminalitätsstrukturen ausgeleuchtet und bekämpft werden, die noch nicht mit der Planung und Vorbereitung von Straftaten begonnen haben müssen. Die Anknüpfung erfolgt über Anhaltspunkte, die eine Zuordnung zu einem Kriminalitätsphänomen ermöglichen oder als möglich

erscheinen lassen. Auf diesem Feld der Polizeiarbeit gibt es bereits polizeiinterne Vorschriften und Anweisungen. Die Bekämpfung solcher Kriminalitätsphänomene erfolgt auf Grundlage strategisch ausgerichteter Handlungskonzepte und operativer Präventionsplanungen. Durch den Begriff „Kriminalitätsphänomen“ im Polizeigesetz wird für das Gefahrenabwehrrecht des Landes Brandenburg der gesetzliche Anknüpfungspunkt hierfür geschaffen.

Während es bei der Nummer 3 um selektive Kriminalprävention geht, wird in Nummer 4 („Vermeidung strafbarer Verhaltensweisen beizutragen“) insbesondere die universelle Kriminalprävention erfasst. Die Polizei trägt durch Förder- und Beratungsmaßnahmen, die sich an die Allgemeinheit oder bestimmte Bevölkerungsgruppen richten, dazu bei, dass strafbare Verhaltensweisen vermieden und Kriminalität reduziert wird.

Durch die Nummer 5 wird klargestellt, dass die Polizei auch Gefahrenabwehr im digitalen Raum zu betreiben hat, soweit ein Bezug zum Land Brandenburg besteht, also irgendein Anknüpfungspunkt. Der Begriff „digitaler Raum“ wird im neuen § 3 BbgPolG definiert. Im Zusammenspiel mit dem ebenfalls dort definierten Kriminalitätsphänomen der Cyberkriminalität im weiteren Sinne und dessen Verankerung in den polizeilichen Befugnisnormen werden Gesetzesnormen geschaffen, die der Polizei nunmehr auch die effektive Gefahrenabwehr im Internet ermöglichen. Beispielsweise hat die Internetstreife nun eine klare Rechtsgrundlage, aber auch andere Standardbefugnisse können bei technischer Umsetzbarkeit entsprechend im digitalen Raum angewendet werden. So kommen beispielsweise die Identitätsfeststellung im digitalen Raum, die Überwachung eines gefährlichen digitalen Ortes z.B. im „Darknet“ oder ein virtueller Platzverweis in Betracht.

In Absatz 3 wird klargestellt, dass die Vollzugshilfe der Polizei nicht nur anderen Behörden, sondern auch den Gerichten gewährt wird.

In Absatz 5 erfolgt eine Anpassung der Paragraphenbezeichnungen.

Zu Nummer 3 (§ 2 Verhältnis zu anderen Behörden)

In § 2 Satz 1 BbgPolG erfolgt eine grammatikalische Anpassung.

Durch den neuen Satz 2 wird die Polizei zur vernetzten Zusammenarbeit mit anderen Sicherheitsbehörden (Polizei, Verfassungsschutz, Staatsanwaltschaften und Ordnungsbehörden) verpflichtet, soweit dies rechtlich möglich ist. Vernetzte Zusammenarbeit im Bereich der inneren Sicherheit bedeutet insbesondere eine kommunikative Vernetzung in dem Sinne, dass verschiedene Informationen und Daten aus unterschiedlichen Quellen zusammengeführt werden, um damit ein einheitliches Lageverständnis gemeinsam agierender Sicherheitsbehörden zu erzeugen. Die Informationen und Daten werden in einem ganzheitlichen Sicherheitsprozess den vereint agierenden Sicherheitsbehörden zur Verfügung gestellt, um die Arbeitseffizienz in einer vernetzten Umgebung zu steigern. Die Informationen und Daten der einzelnen Behörden werden in das gemeinsame Lagebild zurückgeführt, um das integrierte Lagebild zu erweitern und damit seine Qualität zu erhöhen. Letztlich bedeutet dies, dass alle Akteure in derselben Lage leben und an einem Strang ziehen. Die Selbstverstärkung ist damit der Schlüssel zum Erfolg, der aus einem erweiterten Fähigkeitenpotential eine signifikante strategische und operative Verbesserung erzeugt. Jedoch sind gerade auch die rechtlichen Grenzen insbesondere zwischen der Polizei und dem Verfassungsschutz zu wahren.

In Satz 3 wird klargestellt, dass neben der Unterrichtung über die Vorgänge auch die relevanten Daten übermittelt werden sollen.

Zu Nummer 4 (§§ 3 und 4)

Zu § 3 (Begriffsbestimmungen)

Im neuen § 3 BbgPolG werden die für das Polizeigesetz relevanten Begriffe definiert. Einige Bundesländer wie beispielsweise Bremen und Sachsen-Anhalt haben in ihren Polizei- und Sicherheitsgesetzen Begriffsbestimmungen eingeführt. Dadurch wird dem Bestimmtheitsgrundsatz und der Rechtsklarheit besser Rechnung getragen. Insbesondere Begrifflichkeiten aus der Rechtsprechung und der EU-Datenschutzrichtlinie für den Bereich der Polizei werden übernommen. Begriffsdefinitionen im Polizeigesetz werden nach vorne gezogen. Dies erhöht die Übersichtlichkeit und die Verständlichkeit nicht nur für die Polizeibediensteten, sondern auch für die Bürgerinnen und Bürger.

In den Nummern 1 bis 3 werden die Rechtsgüter öffentliche Sicherheit, öffentliche Ordnung und bedeutsame Rechtsgüter bestimmt.

In den Nummern 4 bis 11 werden die unterschiedlichen Gefahrenbegriffe definiert. Die Nummern 4 bis 8 erfassen den Begriff der konkreten Gefahr in seinen verschiedenen Ausprägungen. Die Nummern 9 und 10 enthalten die Begriffe der abstrakten und erhöhten abstrakten Gefahr. In Nummer 11 wird die Gefahr im Verzug bestimmt.

Nach dem herkömmlichen Gefahrenprinzip soll die Polizei erst bei einer konkreten Gefahr polizeiliche Maßnahmen ergreifen dürfen. Die Entwicklungen verschiedener Kriminalitätsphänomene in einer globalen Welt haben aber dazu geführt, dass die Polizei bei bedeutsamen Rechtsgütern, bei Straftaten von erheblicher Bedeutung und bei schwerwiegenden Kriminalitätsphänomenen selektive Kriminalprävention betreiben soll. Deshalb stehen in diesem Änderungsgesetz im Bereich der polizeilichen Aufklärungsmaßnahmen die abstrakte und die konkrete Gefahr in einem Stufenverhältnis. So ist es rein logisch, dass im Rahmen der Gefahrenvorsorge die frühen Ansatzpunkte einer konkreten Gefahr bereits im Stadium einer abstrakten oder erhöhten abstrakten Gefahr durch die Polizei erhellte werden müssen, wenn sie eine vorsorgende und nicht eine abwartende Polizei ist. Die abstrakte und erhöhte abstrakte Gefahr wird auf Aufklärungsmaßnahmen beschränkt, die keinen schwerwiegenden Grundrechtseingriff befürchten lassen und mit denen sich relevante polizeiliche Sachverhalte aus dem Sachverhaltsmeer herausfiltern lassen. Dies umfasst insbesondere die Identitätsfeststellung mittels Schleierfahndung oder Kontrollstellen sowie die offene Videoüberwachung. Insbesondere die Regelung zur Identitätsfeststellung mittels Schleierfahndung ermöglicht der Polizei nach der Rechtsprechung des Bayerischen Verwaltungsgerichtshofs (BayVerfGH vom 28.3.2003 Az. Vf. 7-VII-00 und vom 7.2.2006 Az. Vf. 69-VI-04) unterhalb der Schwelle der konkreten Gefahr zu handeln. Die Auslegung dieser Rechtsprechung zeigt, dass bereits im Bereich einer abstrakten oder erhöhten abstrakten Gefahr grundrechtsrelevante polizeiliche Aufklärungsmaßnahmen ergriffen werden können.

Aber auch die konkrete Gefahr ist sehr flexibel, so dass sie eine Vielzahl polizeilicher Sachverhalte erfasst und die polizeilichen Maßnahmen anzuleiten vermag. Das Gefahrenurteil eröffnet diese Flexibilität. Der erforderliche Wahrscheinlich-

keitsgrad hängt vom Gewicht des Schadensereignisses und der betroffenen Schutzgüter ab. Je schwerer das Schadensereignis und je wichtiger die betroffenen Schutzgüter, umso geringere Anforderungen sind an die Eintrittswahrscheinlichkeit zu stellen. Auch die Art der polizeilichen Maßnahme wirkt sich auf die Anforderungen an das Gefahrenurteil aus. An Aufklärungs- und Erforschungsmaßnahmen werden regelmäßig geringere Anforderungen als an imperative Maßnahmen gestellt, weil ansonsten mit einem Erkenntnisverlust zu rechnen ist. Dies gilt insbesondere bei Ermittlungsmaßnahmen, um Straftaten zu verhindern. Wird die vorbeugende Bekämpfung von Kriminalitätsphänomenen zum Bezugspunkt der konkreten Gefahr, so wird deren Flexibilität ausgeweitet, weil sich diese nicht auf Straftaten oder ein bestimmtes Schutzgut, sondern auf eine kriminelle Struktur bezieht. Bei Straftaten und Kriminalitätsphänomenen wird insbesondere auf die kriminalistische Erfahrung abgestellt. Diese allgemein anerkannte Auslegung des Gefahrenbegriffs wird in Nummer 4 Buchstabe a verankert.

Nummer 4 Buchstabe b enthält eine zusätzliche Ausweitung des Begriffs der konkreten Gefahr. Im Jahr 2007 urteilte das Bundesverfassungsgericht zur Online-Durchsuchung im Hinblick auf Vorschriften des Verfassungsschutzgesetzes Nordrhein-Westfalen (BVerfGE 120, 274): „Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen. Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann.“

Das Bundesverfassungsgericht hat in seinem Urteil zum Bundeskriminalamtgesetz vom 20. April 2016 (Az. 1 BvR 966/09 und 1 BvR 1140/09, Rdnr. 111 ff., 163 f.) diese Rechtsprechung zur Online-Durchsuchung für das Polizeirecht weiterentwickelt. Die Ermächtigungen des Bundeskriminalamts zum Einsatz von heimlichen Überwachungsmaßnahmen (Wohnraumüberwachungen, Online-Durchsuchungen, Telekommunikationsüberwachungen, Telekommunikationsverkehrsdatenerhebungen und Überwachungen außerhalb von Wohnungen mit besonderen Mitteln der Datenerhebung) müssen auf den Schutz oder die Bewehrung hinreichend gewichtiger Rechtsgüter begrenzt sein und setzen voraus, dass eine Gefährdung dieser Rechtsgüter hinreichend konkret absehbar ist. § 20g Abs. 1 Nr. 2 BKAG a. F. ergänzt die auf die Gefahrenabwehr begrenzte Eingriffsgrundlage des § 20g Abs. 1 Nr. 1 BKAG a. F. und soll nach der Vorstellung des Gesetzgebers schon früher ansetzen und der Straftatenverhütung dienen. Nach den oben dargelegten Maßstäben ist der Gesetzgeber hieran nicht grundsätzlich gehindert und zwingt ihn die Verfassung nicht, Sicherheitsmaßnahmen auf die Abwehr von – nach tradiertem Verständnis – konkreten Gefahren zu beschränken. Allerdings bedarf es aber auch bei solchen Maßnahmen zur Straftatenverhütung zumindest einer auf bestimmte Tatsachen und nicht allein auf allgemeine Erfahrungssätze gestützten Prognose, die auf eine konkrete Gefahr bezogen ist. Grundsätzlich gehört hierzu, dass insoweit ein wenigstens seiner Art nach konkretisiertes und zeitlich absehba-

res Geschehen erkennbar ist (vgl. BVerfGE 110, 33, 56 f.; 113, 348, 377 f.; 120, 274, 328 f.; 125, 260, 330). Stattdessen kann aber auch darauf abgestellt werden, ob das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft beispielsweise terroristische Straftaten begeht. Der Gesetzgeber kann mithin die konkrete Gefahr weiter ziehen, indem er die Anforderungen an den Kausalverlauf reduziert.

Die weite Auslegung der konkreten Gefahr wird in diesem Änderungsgesetz nicht auf die Abwehr terroristischer Gefahren beschränkt, denn auch in anderen Kriminalitätsbereichen drohen schwerwiegende Rechtsgutverletzungen und Straftaten von erheblicher Bedeutung. Eine Beschränkung auf den Bereich des Terrorismus würde die Gefahrenabwehr an die Motive von Straftätern binden. Deshalb ist der Bezugspunkt in diesem Gesetz eine schwere Schädigungshandlung gegen bedeutsame Rechtsgüter und nicht speziell terroristische Straftaten.

Außerdem ist bisher durch die höchstrichterliche Rechtsprechung noch nicht geklärt, ob die weite Auslegung der konkreten Gefahr auch abseits von polizeilichen Aufklärungsmaßnahmen auf imperative Maßnahmen wie beispielsweise den Platzverweis, das Aufenthaltsverbot oder den Präventivgewahrsam angewendet werden kann. Zumindest für den Schutz der besonders schützenswerten Rechtsgüter Leib, Leben und Freiheit der Person vor erheblichen Beeinträchtigungen dürfte dies jedoch verhältnismäßig sein.

In den Nummern 12 und 13 erfolgt eine Definition des Begriffs „Kriminalitätsphänomen“ sowie die Bestimmung bestimmter schwerwiegender Kriminalitätsphänomene wie der Organisierten, schwerwiegenden Grenzüberschreitenden, Politisch motivierten Kriminalität einschließlich des Terrorismus, schwerwiegenden Wirtschaftskriminalität einschließlich der Wirtschafts- und Konkurrenzspionage sowie der schwerwiegenden Cyberkriminalität im weiteren Sinne. Dies dient dazu, das Handeln der Polizei auf die Zerschlagung und Schwächung bestimmter Kriminalitätsphänomene besser auszurichten und gesetzgeberisch zu unterfüttern.

In den Nummern 14 bis 19 werden die Begriffe der verfassungsfeindlichen Handlung, Ordnungswidrigkeit, Ordnungswidrigkeit von erheblicher Bedeutung, Straftat, Straftaten von erheblicher Bedeutung und der besonders schweren Straftaten definiert. Die Straftatenkataloge der §§ 100a, b der Strafprozessordnung werden in den Definitionen der Straftaten von erheblicher Bedeutung und der besonders schweren Straftaten übernommen. Dadurch werden Kettenverweise vermieden.

In Nummer 20 wird der Begriff „öffentlicher Verkehrsraum“, in Nummer 21 der „digitale Raum“ und in Nummer 22 die „Wohnung“ bestimmt.

In den Nummern 23 bis 32 werden die Begriffe der personenbezogenen Daten, Kernbereichsdaten, besonderen Kategorien personenbezogener Daten, genetischen Daten, biometrischen Daten, Gesundheitsdaten, Datenverarbeitung, Pseudonymisierung, des informationstechnischen Systems und der Datei definiert. Die Definitionen werden hauptsächlich aus der EU-Datenschutzrichtlinie für den Bereich der Polizei übernommen. Aufgrund des einheitlichen und umfassenden Begriffs der Datenverarbeitung wird in Kapitel 2 Abschnitt 2 der neue Unterabschnitt 1 „Allgemeine Vorschriften zur Datenverarbeitung und zum Datenschutz“ eingeführt.

Die Nummern 33 bis 39 enthalten die Begriffe von besonderen Personen nämlich die Behördenleitung, die oder der Landesbeauftragte, die Kontakt- oder Begleitperson, die postdiensteanbietende Person, die telediensteanbietende Person, die Vertrauensperson und die verdeckt ermittelnde Person.

Zu § 4 (Allgemeine Voraussetzungen selektiver Kriminalprävention)

Der neue § 4 BbgPolG ist so in keinem der Bundes- oder anderen Länderpolizeigesetze enthalten. Die selektive Kriminalprävention mittels abstrakter, erhöhter abstrakter und ausgeweiteter konkreter Gefahrentatbestände in diesem Polizeigesetz soll planvoll durch strategisch ausgerichtete kriminalpräventive Handlungskonzepte und operative Präventionsplanungen angeleitet werden, damit die polizeilichen Maßnahmen gezielt eingesetzt und im Rahmen eines wirksamen Grundrechtsschutzes eingegrenzt werden. Diese polizeiliche Praxis wird in den Grundzügen gesetzgeberisch abgebildet.

Das hergebrachte reaktive und einzelfallbezogene Handlungskonzept setzt einen bereits sichtbar gewordenen sozialen Konflikt, oft in der Gestalt von möglichen Straftaten voraus, den die Polizei durch ihr reaktives Verhalten beenden will. Dieses hergebrachte Handlungskonzept muss die Polizei verlassen, wenn sie aktiv und gezielt nach sozialen Konflikten einer bestimmten Art sucht oder wenn sie konfliktträchtige soziale Verhältnisse über den Einzelfall hinaus gestalten will.

Deshalb bedarf es kriminalpräventiver Handlungskonzepte wie der strategischen Überwachung von komplexen Strukturen bestimmter Kriminalitätsphänomene, die über den Einzelfall hinaus ausgeleuchtet werden. Gefahren von Kriminalitätsphänomenen mit verdeckten Strukturen einschließlich der oben aufgeführten schwerwiegenden Kriminalitätsphänomene lassen sich oft nur durch eine aktive Vorfeldaufklärung abwehren oder verhüten. Diese Strukturen zeichnen sich zudem dadurch aus, dass von ihnen immer wieder erhebliche Gefahren ausgehen. Mit hergebrachten Handlungskonzepten der Polizei können diese kriminellen Strukturen nicht zerschlagen oder zumindest nachhaltig geschwächt werden. Vielmehr ist es notwendig, Überwachungsmaßnahmen und imperative Zugriffe der Polizei in einem strategischen Konzept gezielt auf die Bekämpfung der Kriminalitätsphänomene auszurichten.

Ein weiteres kriminalpräventives Handlungskonzept ist die gelegenheitsorientierte Kriminalprävention, durch die die Gelegenheit zu Straftaten eingeschränkt wird. Durch sie soll verhindert werden, dass in Zukunft weitere soziale Konflikte entstehen. Dies kann die Polizei durch Überwachung oder imperative Zugriffe erreichen. Das Ziel von den Überwachungsmaßnahmen ist es nicht nur polizeiliche Zugriffe zu ermöglichen, sondern durch ihre offene Weise auch kriminelles Verhalten aufgrund von fehlenden Tatgelegenheiten vorbeugend zu unterbinden. Proaktive Maßnahmen in diesem Bereich beruhen auf Risikoanalysen.

Kriminalpräventive Handlungskonzepte haben in der Regel einen operativen Unterbau, der durch die operative Präventionsplanung ausgestaltet wird. Dadurch werden polizeitaktische Maßnahmen auf die operativen Ziele ausgerichtet.

§ 4 BbgPolG legt in Absatz 1 fest, dass die Polizei Maßnahmen zur Verhütung oder vorbeugenden Bekämpfung von Straftaten oder Kriminalitätsphänomenen ergreifen und hierdurch erlangte personenbezogene Daten verarbeiten kann, soweit dies durch die Vorschriften des Kapitels 2 erlaubt ist. Die Reichweite selekti-

ver Kriminalprävention richtet sich nach den Gefahrenbegriffen, die den jeweiligen Vorschriften zugrunde liegen.

In Absatz 2 werden diese Maßnahmen nach Absatz 1 einer schriftlichen operativen Präventionsplanung unterworfen, in der Anlass, Ziele, Mittel und Ort der jeweiligen Maßnahme vor dem Hintergrund polizeilicher Erfahrung und den Lageerkennnissen beschrieben werden. Die operative Präventionsplanung umfasst zudem eine Gefahrenprognose sowie eine Abwägung der Verhältnismäßigkeit der Maßnahmen und die Gründe für die Ermessensausübung.

Der operativen Präventionsplanung muss ein schriftliches kriminalpräventives Handlungskonzept der Polizei nach Absatz 3 zugrunde liegen, das unter der Federführung der Behördenleitung und in Abstimmung mit dem für Inneres zuständigen Mitglied der Landesregierung erstellt wurde. Kriminalpräventiven Handlungskonzepten kommt in Bezug auf die operative Präventionsplanung und die zu ergreifenden Maßnahmen eine strategische Ausrichtungs-, Eingrenzungs- und Leitfunktion zu.

Die polizeitaktischen Maßnahmen, operativen Präventionsplanungen und die kriminalpräventiven Handlungskonzepte sind nach Absatz 4 im verwaltungsgerichtlichen Verfahren überprüfbar.

Darüber hinaus besteht nach Absatz 5 eine jährliche Berichtspflicht des für Inneres zuständigen Mitglieds der Landesregierung gegenüber dem Landtag und dessen für Inneres zuständigen Ausschuss.

Zu Nummern 5 bis 8 (§§ 5 bis 8)

In den Nummern 5 bis 8 erfolgen Anpassungen der Paragrafennummerierung sowie grammatikalische Anpassungen.

Zu Nummer 9 (§ 9 Unmittelbare Ausführung einer Maßnahme)

Im neuen § 9 BbgPolG wird in Absatz 1 nun ausdrücklich wie in anderen Bundesländern beispielsweise in Bayern und Baden-Württemberg geregelt, dass die Polizei eine Maßnahme selbst oder durch Beauftragte ausführen kann, wenn der Zweck der Maßnahme durch Inanspruchnahme der Störer nach den §§ 7 oder 8 BbgPolG nicht oder nicht rechtzeitig erreicht werden kann. Die von der Maßnahme betroffene Person ist unverzüglich zu unterrichten. Entstehen der Polizei durch die unmittelbare Ausführung einer Maßnahme Kosten, so werden diese nach Absatz 2 von den nach §§ 7 oder 8 BbgPolG verantwortlichen Personen erhoben.

Diese Vorschrift steht nach der Störer- und vor der Nichtstörer-Haftung. Sie dient daher auch dem Schutz des Nichtstörers vor ungebührlicher Inanspruchnahme. Erfasst wird polizeiliches Handeln durch gerichtlich überprüfbare Realakte mit Eingriffscharakter. Der behördliche Wille wird also ohne Zwischenschaltung einer Polizeiverfügung unmittelbar vollzogen. Hierbei handelt es sich nicht um eine eigenständige Eingriffsermächtigung, so dass die formellen und materiellen Voraussetzungen polizeilichen Handelns vorliegen müssen.

Zu Nummer 10 (§ 10)

In der Nummer 10 erfolgen eine Anpassung der Paragrafennummerierung sowie grammatikalische Anpassungen.

Zu Nummer 11 (§ 11 Einschränkung von Grundrechten)

Im neuen § 11 BbgPolG werden die Grundrechte aufgeführt, in die durch dieses Gesetz eingegriffen wird. Die Unverletzlichkeit des Fernmeldegeheimnisses wird um das Brief- und Postgeheimnis erweitert (Artikel 10 Absatz 1 des Grundgesetzes, Artikel 16 Absatz 1 der Verfassung des Landes Brandenburg). Der Eingriff in das Eigentum (Artikel 14 des Grundgesetzes, Artikel 41 Absatz 1 Satz 1 der Verfassung des Landes Brandenburg) wird nun ausdrücklich genannt.

Zu Nummer 12 (§ 12)

In der Nummer 12 erfolgen eine Anpassung der Paragrafennummerierung sowie grammatikalische Anpassungen.

Zu Nummer 13 (§ 13 Allgemeine Befugnisse)

Der neue § 13 BbgPolG enthält in Absatz 1 die Regelungen zur allgemeinen polizeilichen Eingriffsermächtigung, die Generalklausel. Es wird ein klarstellender Satz angefügt. Danach kann die Polizei Maßnahmen im Sinne des Satzes 1 insbesondere treffen, um Straftaten, Kriminalitätsphänomene, Ordnungswidrigkeiten oder verfassungsfeindliche Handlungen zu verhüten, vorbeugend zu bekämpfen oder zu unterbinden.

Absatz 3 wird aufgehoben, weil dieser in den Begriffsbestimmungen des neuen § 3 BbgPolG aufgegangen ist. Dies erfordert zudem die Streichung des Kommas und des Wortes „Begriffsbestimmung“ in der Überschrift.

Zu Nummer 14 (§ 14 Befragung, Auskunftspflicht)

Im Absatz 2 des neuen § 14 BbgPolG wird die Möglichkeit der Zwangsgeldfestsetzung eröffnet, wenn die Auskunft nach Satz 1 oder 2 unberechtigtweise verweigert wird. Dieses ist zuvor in bestimmter Höhe anzudrohen. Absatz 3 wird aufgehoben, weil dieser in der Regelung des neuen § 15 Absatz 1 Nummer 6 BbgPolG im Rahmen einer Identitätsfeststellung mittels Schleifahndung erfasst wird.

Zu Nummer 15 (§ 15 Identitätsfeststellung)

Der neue § 15 Absatz 1 Nummer 2 BbgPolG wird erweitert auf Straftaten insgesamt, Ordnungswidrigkeiten von erheblicher Bedeutung sowie um Orte, an denen Personen der Prostitution nachgehen. Hierbei handelt es sich um Orte, an denen es vermehrt zu sozialen Konflikten kommt, bei denen ein polizeiliches Eingreifen erforderlich ist. Orte der Prostitution werden bisher von den Polizeigesetzen der Bundesländer Baden-Württemberg, Bayern, Hessen, Mecklenburg-Vorpommern, Rheinland-Pfalz, Saarland und Thüringen erfasst. Dies dient dem Schutz insbesondere von Frauen und Kindern vor Zwangsprostitution.

In der Nummer 4 wird die Möglichkeit der Identitätsfeststellung an Kontrollstellen auf die Verhütung und vorbeugende Bekämpfung von Straftaten von erheblicher Bedeutung und von schwerwiegenden Kriminalitätsphänomenen erweitert, sofern diesbezüglich zumindest eine erhöhte abstrakte Gefahr besteht.

Die Nummer 5 erfasst nunmehr klarstellend neben Flugplatzbereichen auch die Grenzbereiche.

Die sogenannte Schleierfahndung in Nummer 6 wird auf den gesamten öffentlichen Verkehrsraum des Landes Brandenburg zur Verhütung oder vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen erweitert, sofern diesbezüglich zumindest eine abstrakte Gefahr besteht.

Der Nummer 7 werden die Nummern 8 und 9 angefügt. Dadurch wird wie im hessischen Polizeigesetz die Identitätsfeststellung auf die Vollzugshilfe (§ 1 Absatz 3) und auf das Umfeld besonders gefährdeter Personen ausgedehnt.

In Absatz 2 Satz 2 wird der Zusatz „Kleidungsstücke sowie Gegenstände, die eine Identitätsfeststellung verhindern oder erschweren, abnimmt“ angefügt. Die Änderung dient der ergänzenden Konkretisierung und Klarstellung der dort bereits enthaltenen Befugnis. Zu einer Identitätsfeststellung gehört notwendigerweise auch, dass die zu identifizierende Person durch Abnehmen solcher Kleidungsstücke oder Gegenstände, die eine Identitätsfeststellung verhindern oder erschweren, eine Identifizierung ermöglicht. Darunter fallen sämtliche Kleidungsstücke und Gegenstände, die objektiv geeignet sind, die Identitätsfeststellung zu verhindern oder zu erschweren.

Der alte § 12 Absatz 2 Satz 3 und 4 BbgPolG wird durch den neuen Satz 3 ersetzt. Im neuen Satz 3 wird auch das Verbringen auf die Dienststelle als Sonderfall des Festhaltens ausdrücklich aufgeführt. Die betroffene Person kann also festgehalten, seine Person sowie die von ihm mitgeführten Sachen können durchsucht oder er kann zur Dienststelle gebracht werden. Die Identität darf auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden können. Die Durchsuchung muss auf das Auffinden von Gegenständen zielen, die zur Feststellung der Identität geeignet sind (z.B. Ausweise, Quittungen, Scheck- und Kreditkarten, Karten der Sozialversicherungsträger und Briefe). Eine Durchsuchung zur Eigensicherung kann sich folglich nicht auf diese Vorschrift stützen. Die betroffene Person muss zudem nicht in die nächstgelegene Dienststelle gebracht werden. Entscheidend ist vielmehr, dass dort eine schnelle Identifizierung durchgeführt werden kann.

Wenn die betroffene Person keine oder nur unzureichende Angaben zu seiner Identität macht, begründete Bedenken an der Richtigkeit genannter Personalien bestehen oder sich Zweifel an dem ausgehändigten Ausweispapier ergeben, ist die Polizei gegebenenfalls wegen § 111 OWiG, § 273 StGB auf Grund von § 46 OWiG, § 163b Absatz 1 Satz 2 und 3 StPO zum Festhalten, zur Durchsuchung und zur Durchführung erkennungsdienstlicher Maßnahmen befugt. Diese Befugnisse setzen den Anfangsverdacht einer Ordnungswidrigkeit oder Straftat voraus. Sie gehen den verdachts- und ereignisunabhängigen Befugnissen vor. § 111 OWiG soll dem amtlichen Auskunftsverlangen Nachdruck verleihen und damit anderweitig geregelte Auskunftspflichten absichern. Die Androhung des Bußgelds soll die Bereitschaft der aufgeforderten Person erhöhen, wahrheitsgemäß und lückenlos Auskunft zu erteilen, damit ihm aufwändigere und umständlichere Maßnahmen erspart bleiben.

Es folgen Ausführungen zur Schleierfahndung:

Der bisherige räumliche Anwendungsbereich für verdachts- und ereignisunabhängige Kontrollen nach dem alten § 12 Absatz 1 Nummer 6 BbgPolG ist auf das Gebiet der Bundesgrenze bis zu einer Tiefe von dreißig Kilometern begrenzt. Die Po-

lizeigesetze anderer Bundesländer erfassen auch Durchgangsstraßen (Bundesautobahnen, Europastraßen und andere Straßen von erheblicher Bedeutung für den grenzüberschreitenden Verkehr) und öffentliche Einrichtungen des internationalen Verkehrs. Damit ist der Tatbestand auf die Grenzüberschreitende Kriminalität zugeschnitten. Der neue § 15 Absatz 1 Nummer 6 BbgPolG ist darüber hinaus auch auf andere Kriminalitätsphänomene zugeschnitten, wie beispielsweise der Politisch motivierten Kriminalität, die sich vielmehr im städtischen und ländlichen Bereich als an den Hauptverkehrswegen abspielt. Weiterhin kann die Schleierfahndung auch bei der Bekämpfung der Organisierten Kriminalität und des Terrorismus eine wichtige Rolle spielen.

Darüber hinaus entsteht ein Stufenverhältnis zwischen den in Nummer 1 und 4 geregelten polizeilichen Maßnahmen mit unterschiedlichen Gefahrenschwellen. Dies ist so vom Gesetzgeber gewollt, um die Identitätsfeststellung als eine der wichtigsten polizeilichen Maßnahmen noch effektiver auszugestalten und unterschiedlichen Schweregraden des Grundrechtseingriffs gerecht zu werden. Während beispielsweise an Kontrollstellen allgemein sichtbar ist, wer kontrolliert wird, kann die Schleierfahndung auch so eingesetzt werden, dass eine Person nicht vor aller Augen einer Kontrolle unterzogen wird.

Verdachts- und ereignisunabhängige Kontrollen ermöglichen jedoch kein vollkommen willkürliches Kontrollieren und bedürfen einer gewissen Eingriffsschwelle (vgl. BayVerfGH, Entscheidung vom 28. März 2003, Vf. 7-VII-00, Vf. 8-VIII-00). Die Eingriffsschwelle nach dieser Gesetzesänderung wird bereits genommen, wenn ein Kontrollanlass vor dem Hintergrund wenigstens allgemeiner Lageerkenntnisse und polizeilicher Erfahrung aufgrund eines abstrakten Gefahrenpotenzials besteht und sich dieser auf die Kontrollziele, -orte und -maßnahmen bezieht. Mit einem abstrakten Gefahrenpotenzial wird generell eine Sachlage umschrieben, aus der nach allgemeiner Lebenserfahrung konkrete Gefahren im Einzelfall erst entstehen können. Durch die Identitätskontrolle soll gerade erforscht werden, ob eine auch personell konkretisierbare und damit zurechenbare Gefahr vorliegt. Kriminalpräventive Handlungskonzepte und Präventionsplanungen nach dem neuen § 4 BbgPolG dienen in diesem Zusammenhang der strategischen und operativen Ausrichtung der verdachts- und ereignisunabhängigen Kontrollen und der schriftlichen Dokumentation der Eingriffsschwellen, denn im Streitfall unterliegt die polizeiliche Einschätzung in vollem Umfang der verwaltungsgerichtlichen Nachprüfung (§§ 40, 86 Absatz 1, 113 Absatz 1 VwGO). Sie haben also einen anleitenden Charakter im Rahmen der vom Gesetzgeber eröffneten Möglichkeit der Polizei, selektive Kriminalprävention zu betreiben.

Im Grenzgebiet bis zu einer Tiefe von 30 Kilometern liegt ein Kontrollanlass regelmäßig schon vor, weil es sich um einen Raum mit gesteigerter Kriminalität handelt. Im sonstigen öffentlichen Verkehrsraum wird dies auf Durchgangsstraßen (Bundesautobahnen, Europastraßen und anderen Straßen von erheblicher Bedeutung für den grenzüberschreitenden Verkehr) und in öffentlichen Einrichtungen des internationalen Verkehrs auch der Fall sein, weil diese regelmäßig kriminellen Personen als Transitstrecken dienen. Im Übrigen sind durch die Präventionsplanung der Kontrollanlass eindeutig zu bestimmen und der Kontrollort genauer einzugrenzen.

§ 15 Absatz 1 Nummer 6 und Absatz 2 BbgPolG ist auch verfassungsgemäß. Der Gesetzgeber des Landes Brandenburg wird im Rahmen seiner Kompetenzen tätig. Die von der Gesetzesänderung betroffene Vorschrift regelt nicht die strafver-

folgende, repressive Tätigkeit der Polizei (Artikel 74 Absatz 1 Nummer 1 des Grundgesetzes), sondern ihre präventive Tätigkeit (Gefahrenabwehr), insbesondere die vorbeugende Bekämpfung von schwerwiegenden Kriminalitätsphänomenen sowie die Verhütung von Straftaten von erheblicher Bedeutung. Dieser hat also eine präventiv-polizeiliche Zweckbestimmung.

Die Befugnisse zum Anhalten, Befragen und die Aufforderung zu Angaben der Identitätsfeststellung und zur Aushändigung der mitgeführten Ausweispapiere nach § 15 Absatz 1 Nummer 6, Absatz 2 Satz 2 BbgPolG greifen in die Schutzbereiche der Grundrechte auf allgemeine Handlungsfreiheit (Artikel 2 Absatz 1 des Grundgesetzes, Artikel 10 der Verfassung des Landes Brandenburg), informationelle Selbstbestimmung (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes, Artikel 11 Absatz 1 der Verfassung des Landes Brandenburg) und Freiheit der Person in der Form der Freiheitsbeschränkung (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes, Artikel 9 Absatz 1 der Verfassung des Landes Brandenburg) ein. Dieser wahrt jedoch bei der Einschränkung der Grundrechte den Grundsatz der Verhältnismäßigkeit, an den das Rechtsstaatsprinzip und die genannten Grundrechte den Gesetzgeber binden. Der Grundsatz der Verhältnismäßigkeit fordert, dass das Gesetz einem legitimen Zweck dient, hierzu geeignet und erforderlich ist, und dass es zwischen der Schwere der grundrechtlichen Beeinträchtigung und der Bedeutung des legitimen Zwecks einen angemessenen Ausgleich schafft.

Die Befugnis zur Identitätsfeststellung dient einem legitimen Zweck, der durch deren Kontrollziele beschrieben wird. Die vorbeugende Bekämpfung von schwerwiegenden Kriminalitätsphänomenen sowie die Verhütung von Straftaten von erheblicher Bedeutung beziehen ihre Legitimität aus der Verpflichtung des Staates zum Schutz seiner Bürger vor Gefahren und Straftaten. Die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit der Bevölkerung vor Gefahren sind Verfassungswerte. Die Schutzpflicht des Staates findet ihren Grund sowohl in Artikel 2 Absatz 2 Satz 1 des Grundgesetzes, Artikel 8 Absatz 1 Satz 1 der Verfassung des Landes Brandenburg als auch in Artikel 1 Absatz 1 Satz 2 des Grundgesetzes, Artikel 7 Absatz 1 Satz 2 der Verfassung des Landes Brandenburg.

Die Befugnis zur Identitätsfeststellung ist geeignet, diesen ihr zugedachten Zweck zu erfüllen. Die Identitätsfeststellung ist in erster Linie eine Maßnahme der Gefahrenforschung. Sie dient in präventiver Hinsicht dazu, die Polizei in die Lage zu versetzen, durch einen Abgleich der festgestellten Identität mit polizeilichen Datenbeständen eine von der kontrollierten Person möglicherweise ausgehende oder sonst mit ihr zusammenhängende Gefahr durch weitergehende Maßnahmen abzuwehren. Auch können anlässlich der Identitätskontrolle Auffälligkeiten registriert werden, die weitergehende Maßnahmen – wie etwa Durchsuchungen – nach sich ziehen. Außerdem kann die Aufhebung der Anonymität einen potenziellen Störer dazu bewegen, auf Aktivitäten zu verzichten. Zugleich entfaltet die Befugnis zur Feststellung der Identität eine vom einzelnen Zugriff unabhängige generalpräventive Wirkung. Durch die Präventionsplanung wird zudem erreicht, dass die eingeräumte Befugnis zielgerichtet eingesetzt wird.

Die gesetzliche Regelung ist erforderlich. Ein gleich wirksames, die betroffenen Grundrechte weniger beeinträchtigendes Mittel steht nicht zur Verfügung. Ein auf das Grenzgebiet reduzierter Kontrollraum der Schleierfahndung wäre nicht in gleicher Weise wirksam und die polizeilichen Befugnisse würden dabei von Zufällig-

keiten abhängen. Eine Regelung als eigenständige Maßnahme der Befragung und in Augenscheinnahme ist im Hinblick auf mögliche Folgemaßnahmen ebenfalls nicht in gleicher Weise wirksam. Eine örtliche Begrenzung auf sogenannte Durchgangsstraßen würde den Kriminellen und Straftätern eine Landkarte der Schleierfahndung in die Hand geben, was aus polizeitaktischer Sicht nicht sinnvoll ist. Darüber hinaus ließe sich diese Maßnahme dann nur schwerlich auf andere Kriminalitätsphänomene als die Grenzüberschreitende Kriminalität ausrichten.

Die Gesetzesänderung der verdachts- und ereignisunabhängigen Kontrolle ist auch verhältnismäßig im engeren Sinn. Der Verhältnismäßigkeitsgrundsatz verlangt, dass die Einbußen an grundrechtlich geschützter Freiheit nicht in unangemessenem Verhältnis zu den legitimen Gemeinwohlzwecken stehen, denen die Grundrechtsbeschränkung dient. Gemeinschaftsbezogenheit und -gebundenheit der Person führen dazu, dass der Einzelne Einschränkungen seiner Grundrechte hinzunehmen hat, wenn überwiegende Allgemeininteressen dies rechtfertigen. Es müssen jedoch die Allgemein- und Individualinteressen angemessen ausgeglichen werden. Dabei spielt auf grundrechtlicher Seite eine Rolle, unter welchen Voraussetzungen welche und wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind. Kriterien sind also die Gestaltung der Eingriffsschwelle, die Zahl der betroffenen Personen und die Intensität der Beeinträchtigungen. Auf Seiten der Gemeinwohlinteressen ist das Gewicht der Ziele und Belange maßgeblich, denen die Identitätskontrolle dient.

Eine Identitätskontrolle greift nur sehr geringfügig in die allgemeine Handlungsfreiheit und das Recht auf informationelle Selbstbestimmung ein. Dies gilt auch für das Anhalten im Hinblick auf die Freiheit der Person. Der Eingriff erschöpft sich in einem Anhalten und Befragen sowie der Verpflichtung, ein mitgeführtes Ausweispapier zur Prüfung auszuhändigen und sich dabei erkennen zu geben. Soweit sich an dabei getroffene Feststellungen weitere, über die Identitätsfeststellung hinausgehende Maßnahmen anschließen, beruhen diese nicht mehr auf § 15 Absatz 2 Satz 2 BbgPolG, sondern auf anderen Normen.

Die Eingriffsschwelle der Identitätskontrolle mittels Schleierfahndung ist niedrig ausgestaltet. Das Gesetz sieht eine Befugnis zur Identitätsfeststellung vor, ohne an eine konkrete Gefahr oder eine besondere Gefahrennähe anzuknüpfen. Die Befugnis ist also, verdachts- und ereignisunabhängig. Das bedeutet aber nicht, dass das Gesetz generell ein vollkommen willkürliches, durch kein Ziel bestimmtes Kontrollieren ermöglicht. Die Polizei ist schon durch die Kontrollziele verpflichtet, den Kontrollen wenigstens allgemeine Lageerkenntnisse oder einschlägige polizeiliche Erfahrung zu Grunde zu legen. Die Gesetzesvorschrift lässt Identitätskontrollen zwar im ganzen öffentlichen Verkehrsraum zu. Durch die Präventionsplanung werden diese aber auf Bereiche mit einem abstrakten Gefahrenpotenzial beschränkt und zugeschnitten. Mithin wird die abstrakte Kontrollwahrscheinlichkeit im Einzelfall deutlich herabgesetzt. Insgesamt ergibt sich das Bild einer geringfügigen Grundrechtsbeeinträchtigung. Andererseits dient die Identitätskontrolle dem Schutz bedeutsamer Güter, deren Verletzung strafbewehrt ist.

Bei einer abwägenden Gegenüberstellung der Grundrechtsbeeinträchtigung und des damit verfolgten präventiven Gefahrenschutzes überwiegen die Grundrechtsbeeinträchtigungen nicht das allgemeine Interesse an einem präventiven Gefahrenschutz. Der staatliche Schutzauftrag wäre ohne Kontrollbefugnisse von vornherein nur unvollkommen zu erfüllen. Auch auf dem Feld der vorsorgenden selektiven Kriminalprävention sind Grundrechtseingriffe nicht schlechthin unzulässig.

Zwar knüpft das Polizeirecht Eingriffsbefugnisse der Polizei traditionell an eine konkrete Gefahr, die einem Handlungs- oder Zustandsstörer zugerechnet wird und Maßnahmen gegen ihn rechtfertigen kann. Die Identitätskontrolle ist zwar im Fall der konkreten Gefahr (§ 15 Absatz 1 Nummer 1 BbgPolG), aber auch an Orten möglich, die eine besondere Gefahrennähe haben (§ 15 Absatz 1 Nummer 2 und 3 BbgPolG). All das beugt unverhältnismäßigen Beschränkungen der Grundrechte vor, besagt aber noch nicht, dass jenseits einer solchen Gefahr oder eines derartigen Verdachts die Verhältnismäßigkeit generell nicht mehr gewahrt ist. Beim Gesundheits-, Arbeits- und Umweltschutz ist die Gefahrenvorsorge seit langem anerkannt. Sie muss nach Umfang und Ausmaß dem Gefahren- oder Risikopotenzial, dem sie gilt, angemessen sein. Die Identitätskontrolle nach § 15 Absatz 1 Nummer 6, Absatz 2 BbgPolG dient demgegenüber dazu, in einem Raum mit einem abstrakten Gefahrenpotenzial vor dem Hintergrund wenigstens allgemeiner Lageerkenntnisse und polizeilicher Erfahrung zu erforschen, ob eine auch personell konkretisierbare und damit zurechenbare Gefahr besteht. Damit hat die Identitätskontrolle eine Zielsetzung von verfassungsrechtlichem Gewicht. Sie erfasst wegen ihrer tatbestandlichen Weite, insbesondere der Unabhängigkeit von konkreten Gefahren, potenziell viele Unbeteiligte und erlaubt daher nur geringfügige Grundrechtseingriffe. Darüber geht diese auf die Kontrolle der Identität beschränkte Befugnisnorm nicht hinaus. Es ist daher angemessen, wenn das Gesetz jedermann die geringfügige Pflicht auferlegt, zur Minimierung der genannten Risiken in dem durch die operative Präventionsplanung festgelegten Kontrollraum gegebenenfalls seine Personalien zu nennen und ein mitgeführtes Ausweispapier zur Prüfung auszuhändigen.

§ 15 Absatz 1 Nummer 6, Absatz 2 Satz 3 BbgPolG gibt der Polizei die Befugnis, die betroffene Person sowie die von ihr mitgeführten Sachen zu durchsuchen. Diese Duldungspflicht berührt – über die von den Maßnahmen nach § 15 Absatz 2 Satz 2 BbgPolG betroffenen grundrechtlichen Schutzgüter hinaus – den Schutzbereich der allgemeinen Handlungsfreiheit. Die Befugnis zur Durchsuchung ist jedoch nur eröffnet, wenn die Identität auf andere Weise nicht oder nur unter Schwierigkeiten festgestellt werden kann. Der Grundsatz der Verhältnismäßigkeit ist eingehalten. Die Regelung ist aus den bereits genannten Gründen geeignet und erforderlich, um die Kontrollziele zu verfolgen. Im Übrigen hängt die Intensität des Grundrechtseingriffs bei einer Durchsuchung weitgehend von den Umständen des Einzelfalls ab. Dem hat die Polizei im Einzelfall und unter sachgerechter Ausübung ihres Ermessens Rechnung zu tragen.

Die Befugnisse zum Festhalten und Verbringen in eine Dienststelle sind nach § 15 Absatz 2 Satz 3 BbgPolG nur eröffnet, wenn Maßnahmen nach Satz 2 oder sonstige mildere Mittel (z.B. auch eine Durchsuchung nach Satz 3) erfolglos geblieben sind. Das Festhalten und das Verbringen in eine Dienststelle berühren über die von Maßnahmen nach Satz 2 betroffenen grundrechtlichen Schutzgüter hinaus das Grundrecht der Freiheit der Person in der Form einer Freiheitsentziehung (Artikel 2 Absatz 2 Satz 2 in Verbindung mit Artikel 104 Absatz 2 des Grundgesetzes, Artikel 9 Absatz 1 und 2 der Verfassung des Landes Brandenburg). Eine Einschränkung dieses Grundrechts muss durch gewichtige Gründe des Gemeinwohls gerechtfertigt sein. Maßnahmen auf der Grundlage des § 15 Absatz 1 Nummer 6 BbgPolG dienen gewichtigen Gründen des Gemeinwohls. Eine § 15 Absatz 2 Satz 2 BbgPolG in jeder Hinsicht vergleichbare Befugnis zum verdachts- und ereignisunabhängigen Festhalten oder Verbringen auf eine Dienststelle wäre mit dem Grundsatz der Verhältnismäßigkeit aber nicht zu vereinbaren. Insbesondere wäre das Festhalten oder Verbringen unzulässig, wenn es nur der letzten Vergewisse-

nung über das dienen soll, was der Polizei auf der Grundlage des Satz 2 bereits zur Kenntnis gelangt ist. § 15 Absatz 2 Satz 3 BbgPolG hat hinsichtlich des Festhaltens und Verbringens einen enger umrissenen Anwendungsbereich. In diesem Rahmen ist es eine Frage der Verhältnismäßigkeit im Einzelfall, ob diese Maßnahmen möglich sind und wie weit sie reichen können. Bei einer Gesamtabwägung der maßgebenden Kriterien ist daher auch § 15 Absatz 1 Nummer 6, Absatz 2 Satz 3 BbgPolG in dem festgestellten einfachrechtlichen Anwendungs- und Wirkungsbereich verfassungsgemäß ausgestaltet.

Zu Nummer 16 (§ 16 Erkennungsdienstliche Maßnahmen)

Im neuen § 16 BbgPolG wird in Absatz 2 Nummer 1 nun das Tatbestandsmerkmal „dies zur Abwehr einer konkreten Gefahr erforderlich ist“ eingeführt. Die bisherige Nummer 1 wird die Nummer 2.

Nummer 3 regelt klarstellend, dass erkennungsdienstliche Maßnahmen auch dann durchgeführt werden können, wenn weiterhin nach einer gemäß § 15 BbgPolG getroffenen Maßnahme der Identitätsfeststellung Zweifel über die Person oder die Staatsangehörigkeit bestehen.

In der Nummer 4 werden die vorbeugende Bekämpfung von Kriminalitätsphänomenen verankert und auch betroffene Personen erfasst, die verdächtig sind, eine Straftat begangen, veranlasst oder unterstützt zu haben.

Der neue Absatz 3 regelt die unter Richtervorbehalt stehende DNA-Untersuchung, wenn die Identitätsfeststellung und andere erkennungsdienstliche Maßnahmen nicht hinreichend sind. Die Feststellung des DNA-Identifizierungsmusters und des Geschlechts der Person können erfolgen, wenn dies zur Abwehr einer erheblichen konkreten Gefahr erforderlich ist, die Person vermisst wird, es sich bei der Person um einen unbekannten Toten handelt oder sich die Person erkennbar in einem die freie Willensbestimmung ausschließenden Zustand oder sich sonst in einer hilflosen Lage befindet.

Bereits auf Grund der strengen Voraussetzungen wird es sich dabei nicht um ein regelhaftes präventiv-erkennungsdienstliches Instrument handeln. Gerade bei Personen, von denen ein erhebliches Gefahrenpotential ausgeht, kann dies aber zur sicheren, nachhaltigen Identifizierbarkeit erforderlich sein. Bislang war umstritten, ob und in welchen Fällen präventivpolizeiliche DNA-Untersuchungen auf Grundlage der polizeilichen Generalklauseln zulässig sind. Deshalb ist eine ausdrückliche Regelung geboten.

Wenn die Abwehr einer erheblichen konkreten Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre, dürfen durch die molekulargenetische Untersuchung des aufgefundenen Spurenmaterials unbekannter Herkunft genetische Daten festgestellt werden. Genetische Daten umfassen nach der Definition im neuen § 3 BbgPolG das DNA-Identifizierungsmuster, das Geschlecht, die Augen-, Haar- und Hautfarbe, das biologische Alter und die biogeographische Herkunft des Spurenverursachers. Auf Grund des mit einer solchen Maßnahme einhergehenden Eingriffs in das Recht auf informationelle Selbstbestimmung verbieten sich darüber hinausgehende Feststellungen. Rückschlüsse auf persönlichkeitsrelevante Merkmale wie Erbanlagen, Charaktereigenschaften oder Krankheiten der betroffenen Person, also ein Persönlichkeitsprofil, werden damit nicht ermöglicht.

Ein körperlicher Eingriff darf nur von einer Ärztin oder einem Arzt vorgenommen werden. Die entnommenen Körperzellen und das in sonstiger Weise sichergestellte DNA-Material sind unverzüglich nach der Untersuchung zu vernichten, soweit diese nicht nach anderen Rechtsvorschriften aufbewahrt werden dürfen. Für die Durchführung der Untersuchungen gilt § 81f Absatz 2 der Strafprozessordnung entsprechend.

Absatz 4 regelt unterstützende und besondere datenverarbeitende Maßnahmen. Für Maßnahmen nach den Absätzen 2 und 3 gilt § 15 Absatz 2 Satz 3 BbgPolG entsprechend. Die Daten der erkennungsdienstlichen Unterlagen und die genetischen Daten können zum Zweck des Abgleichs in einer Datei gespeichert und ausschließlich für Gefahrenabwehr verwendet werden. Die erkennungsdienstlichen Unterlagen, die genetischen Daten und die angelegte Datei sind unverzüglich zu vernichten und zu löschen, wenn die Voraussetzungen nach Absatz 2 oder 3 entfallen sind.

Absatz 5 regelt eine besondere Belehrungs- und Mitteilungspflicht gegenüber der betroffenen Person.

Zu Nummer 17 (§ 17 Prüfung von Berechtigungsscheinen und sonstigen Urkunden)

In der Nummer 17 erfolgen eine Anpassung der Paragrafennummerierung, grammatikalische Anpassungen sowie die Erweiterung der Vorschrift des neuen § 17 BbgPolG auf Bescheinigungen, Nachweise oder sonstige Urkunden.

Zu Nummer 18 (§ 18 Vorladung)

In Nummer 18 erfolgen eine Anpassung der Paragrafennummerierung und grammatikalische Anpassungen.

Es wird eine Erweiterung des neuen § 18 BbgPolG um die elektronische Aufenthaltsüberwachung in Absatz 1 Nummer 2 und Absatz 3 Satz 1 Nummer 2 vorgenommen. Die Vorladung wegen der elektronischen Aufenthaltsüberwachung erfolgt etwa zum Zwecke der Anlegung oder Überprüfung der technischen Überwachungsmittel, insbesondere der am Bein der betroffenen Person zu befestigenden „Fußfessel“ und ggf. des zugehörigen Mobiltelefons.

In Absatz 3 Satz 1 Nummer 1 werden zudem die Wörter „Gefahr für Leib, Leben oder Freiheit einer Person“ durch die Wörter „konkreten Gefahr“ ersetzt. Dies erhöht die Durchsetzbarkeit der Vorladung.

Zu Nummer 19 (§§ 19 und 20)

Zu § 19 (Meldeauflage)

Meldeauflagen können bislang bereits aufgrund der polizeilichen Generalklausel angeordnet werden. Dadurch wird sichergestellt, dass die betroffene Person einen gewissen Aktionsradius nicht überschreiten kann. Dies ist bei Störern im Allgemeinen, insbesondere aber auch rund um Sportveranstaltungen bei sogenannten „Hooligans“, ein effektives Mittel. Zwar greift eine Meldeauflage nicht unerheblich in die allgemeine Handlungsfreiheit der betroffenen Person ein, indem sie diese dazu zwingt, sich – unter Umständen mehrere Tage lang – bei der Polizei zu melden, und ist zudem regelmäßig mit einer Beschränkung der Freizügigkeit verbun-

den. Der Grundrechtseingriff bleibt jedoch vergleichsweise gering. Insbesondere sind diese an Intensität nicht mit einem Freiheitsentzug im Sinne von Artikel 104 GG zu vergleichen.

Der neue § 19 BbgPolG regelt nun ausdrücklich die Meldeaufgabe. Die Polizei kann eine Meldeaufgabe zur Abwehr einer konkreten Gefahr oder zur Verhütung oder vorbeugenden Bekämpfung von Ordnungswidrigkeiten von erheblicher Bedeutung, Straftaten oder Kriminalitätsphänomenen anordnen. Sie ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Anordnungsvoraussetzungen weiterhin vorliegen. Die Verlängerung steht unter einem Richtervorbehalt.

Zu § 20 (Platzverweisung, Kontaktverbot, Aufenthaltsanordnung und Wohnungsaufenthaltsverbot)

Im neuen § 20 BbgPolG wird in Absatz 1 die Platzverweisung geregelt. Tatbestandsvoraussetzung ist die Abwehr einer konkreten Gefahr oder die Verhütung oder vorbeugende Bekämpfung von Ordnungswidrigkeiten, Straftaten oder Kriminalitätsphänomenen. Die Platzverweisung kann ferner gegen Personen angeordnet werden, die den Einsatz der Feuerwehr oder von Hilfs- oder Rettungsdiensten behindern.

Das Kontaktverbot, Aufenthaltsverbot und Aufenthaltsgebot werden in Absatz 2 Satz 1 Nummer 1 bis 3 unter den Tatbestandsvoraussetzungen der Abwehr einer konkreten Gefahr oder der Verhütung oder vorbeugenden Bekämpfung von Straftaten oder von Kriminalitätsphänomenen geregelt. Die betroffene Person ist verpflichtet, der Polizei zum Zwecke der Zustellung der Anordnungen unverzüglich eine Anschrift oder eine zustellungsbevollmächtigte Person zu benennen. Die Polizei übermittelt diese Angaben an gefährdete Personen. Die Wahrnehmung berechtigter Interessen der betroffenen Person und Dritter ist zu berücksichtigen. Die Anordnungen nach Satz 1 dürfen die Dauer von drei Monaten nicht überschreiten und können um jeweils längstens einen Monat verlängert werden. Die Vorschriften des Versammlungsrechts bleiben unberührt.

Die Anordnungen müssen dem Gebot der Verhältnismäßigkeit genügen und sind daher örtlich wie zeitlich beschränkt. Ferner handelt es sich nicht um apodiktische, ausnahmslose Ge- und Verbote. Sie stehen vielmehr im polizeilichen Einzelfallermessen. Durch eine einzelfallgerechte Ermessensausübung können Unzumutbarkeiten verhindert werden. So muss es der betroffenen Person beispielsweise weiterhin möglich sein, einen Arzt, Rechtsanwalt, soziale Einrichtungen oder Behörden aufzusuchen oder Gerichtstermine wahrzunehmen. Kontaktverbote werden bisher vor allem in Fällen von Gewalt im sozialen Nahraum oder Stalking angeordnet, kommen aber auch dann in Betracht, wenn die betroffene Person Kontakt zu anderen gefährlichen Personen oder Gruppierungen sucht, etwa um konspirativ die Begehung von Straftaten vorzubereiten oder zu planen. Bei Aufenthaltsge- und -verboten handelt es sich insbesondere nicht um freiheitsentziehende Maßnahmen. Unter Freiheit der Person ist nur die körperliche Freiheit, also der Schutz vor Verhaftungen, Festnahmen und ähnlichen Eingriffen zu verstehen, so dass entsprechend beschränkte Maßnahmen keine unzulässige Einschränkung der Freiheit einer Person darstellen. Soweit das grundrechtlich geschützte Recht auf Freizügigkeit nach Artikel 11 Absatz 2 des Grundgesetzes, Artikel 17 der Verfassung des Landes Brandenburg betroffen ist, ist gesetzlich gewährleistet, dass solche von Vorneherein nur in Betracht kommen können, wenn die Rechtsgutgefährdung

im Zusammenhang mit einer konkreten Gefahr steht. Dem Absatz 2 ähnliche Regelungsbefugnisse finden sich zudem in verschiedenen Landespolizeigesetzen und unterliegen auch dort keinem Richter- oder sonst qualifizierten Anordnungsvorbehalt. Auf Grund der Vielgestaltigkeit der Maßnahmen wäre dies auch nicht generell zu rechtfertigen.

In Absatz 3 wird das Wohnungsaufenthaltsverbot geregelt, das bisher im alten § 16a stand. Tatbestandsvoraussetzung ist die Abwehr einer erheblichen konkreten Gefahr. Absatz 2 Satz 2 bis 4 gelten entsprechend. Die Anordnungen nach Satz 1 dürfen die Dauer von einem Monat nicht überschreiten. Stellt die gefährdete Person während der Dauer des Wohnungsaufenthaltsverbots einen Antrag auf zivilrechtlichen Schutz vor Gewalt oder Nachstellungen mit dem Ziel des Erlasses einer einstweiligen Anordnung, endet das Wohnungsaufenthaltsverbot mit dem Tag der gerichtlichen Entscheidung, spätestens jedoch mit Ablauf der festgelegten Frist. Das Gericht hat der Polizei die Beantragung zivilrechtlichen Schutzes sowie die gerichtliche Entscheidung unverzüglich mitzuteilen. Die Polizei hat gefährdete Personen und die betroffene Person unverzüglich über die Dauer des Wohnungsaufenthaltsverbots in Kenntnis zu setzen.

Zu Nummern 20 bis 23 (§§ 21 bis 24)

Im neuen § 21 BbgPolG wird der Gewahrsam geregelt. Absatz 1 Nummer 3 wird angepasst und erfasst die Meldeauflage, die Platzverweisung, das Kontaktverbot, die Aufenthaltsanordnung, das Wohnungsaufenthaltsverbot und die elektronische Aufenthaltsüberwachung. Als Nummer 4 wird die Tatbestandsvoraussetzung der Abwehr einer erheblichen konkreten Gefahr eingefügt.

Der neue § 22 BbgPolG regelt die Richterliche Entscheidung und der neue § 23 BbgPolG die Behandlung festgehaltener Personen. Es erfolgen Anpassungen bei den Paragrafenverweisen sowie grammatikalische Anpassungen.

Im neuen § 24 BbgPolG wird die mögliche Dauer der Freiheitsentziehung durch richterliche Entscheidung ausgedehnt. Sie darf nicht mehr als einen Monat betragen und kann jeweils um längstens einen Monat verlängert werden. Bisher war die Höchstdauer auf vier Tage und durch weitere Voraussetzungen begrenzt. Die bisherige absolute gesetzliche Obergrenze für eine richterlich festzusetzende Höchstdauer einer Freiheitsentziehung ist verfassungsrechtlich durch Artikel 104 Absatz 2 des Grundgesetzes, Artikel 9 Absatz 2 der Verfassung des Landes Brandenburg nicht geboten. Obergrenzen sind dort nur für das Festhalten auf Grundlage nichtrichterlicher Anordnung geregelt. Die polizeilichen Regelungen in Schleswig-Holstein (§ 204 Absatz 5 Satz 2 LVwG), Bayern (Artikel 20 BayPAG) und Bremen (§ 18 Absatz 1 BremPolG) enthalten in ihrer derzeitigen Fassung insoweit keine oder eine erweiterbare dreimonatige gesetzliche Höchstfrist. In Schleswig-Holstein und Bremen wird durch den Verweis auf das Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit sichergestellt, dass bei erstmaliger Anordnung eine Höchstdauer von einem Jahr keinesfalls überschritten werden darf (§ 425 Absatz 1 FamFG), die richterliche Entscheidung bei Wegfall der Anordnungsvoraussetzungen auch vor Fristablauf von Amts wegen aufzuheben ist (§ 426 Absatz 1 FamFG) und die von einer Ingewahrsamnahme betroffene Person die richterliche Überprüfung der Anordnung beantragen kann (§ 426 Absatz 2 FamFG).

Zu Nummern 24 bis 27 (§§ 25 bis 28)

Der neue § 25 BbgPolG regelt die Durchsuchung von Personen. Es erfolgen grammatikalische und paragrafenverweisliche Anpassungen. In Absatz 1 Nummer 1 wird festgelegt, dass im Falle des § 15 Absatz 1 Nummer 4 oder 6 bereits das Bestehen einer erhöhten abstrakten Gefahr ausreicht. Nach Nummer 5 wird eine neue Nummer 6 mit der Tatbestandsvoraussetzung einer konkreten Gefahr eingefügt. Die bisherige Nummer 6 wird Nummer 7.

Der neue § 26 BbgPolG regelt die Durchsuchung von Sachen. Es erfolgen grammatikalische und paragrafenverweisliche Anpassungen. In Absatz 1 Nummer 6 wird im Hinblick auf § 15 Absatz 1 Nummer 4 und 6 BbgPolG zumindest das Bestehen einer erhöhten abstrakten Gefahr vorausgesetzt. Außerdem kann sich die Durchsuchung auch auf die mit dem Fahrzeug in einem räumlichen Zusammenhang stehenden Sachen erstrecken.

Der neue Absatz 2 Satz 1 bezieht sich auf die Durchsuchung eines elektronischen Speichermediums, das auch vom Durchsuchungsobjekt räumlich getrennt sein kann. Die Regelung ist an § 110 Absatz 3 der Strafprozessordnung angelehnt, die eine rechtsklare ausdrückliche Regelung zur Durchsuchung von Datenbeständen auf elektronischen Speichermedien trifft. Dadurch wird zum einen klargestellt, dass sich eine vom Grundsatz offene Durchsuchungsmaßnahme nach Absatz 1 auch auf Daten beziehen darf. Zum anderen wird der Zugriff auf vom primären Durchsuchungsobjekt aus verfügbare, aber dort selbst nicht unmittelbar gespeicherte Daten geregelt. Entsprechend dem Stand der Technik ist damit auch der Zugriff auf von der benutzten Endeinrichtung der betroffenen Person entfernte Speicherorte zulässig. Es kann keinen Unterschied machen, ob sich die zu durchsuchenden Inhalte auf lokalen oder auf über Netzwerkverbindungen, etwa auf einer serverbasierten Cloud, erreichbaren Speichermedien befinden. Das Bundesverfassungsgericht hat in seinem BKAG-Urteil vom 20.04.2016 den Zugriff auf vernetzte fremde Computer (etwa in Form von Cloud-Diensten) als grundsätzlich zulässig erachtet.

Satz 2 bringt zum Ausdruck, dass sich eine, über die im Rahmen der Durchsuchung erfolgte bloße Kenntnisnahme hinausgehende, weitere Verarbeitung personenbezogener Daten nach gesonderten Vorschriften richtet, wobei je nach Fall die Sicherstellung von Daten oder eine Datenverarbeitung nach Kapitel 2 Abschnitt 2 in Betracht kommen kann. Letztlich sind die bezeichneten Abgrenzungen stets nach den Umständen des Einzelfalls zu treffen.

Für die Durchsuchung von Personen nach § 25 BbgPolG und Sachen nach § 26 BbgPolG unter den Voraussetzungen des § 15 Absatz 1 Nummer 6 BbgPolG ist es nicht notwendig, dass Tatsachen die Annahme rechtfertigen, man werde auch tatsächlich etwas finden. Unter dem Gesichtspunkt der Verhältnismäßigkeit im engeren Sinn sind jedoch strengere Anforderungen an solche Durchsuchungen zu stellen als bei bloßen Identitätskontrollen, weil es sich um wesentlich intensivere Grundrechtseingriffe handelt. Die Durchsuchungen stellen regelmäßig einen erheblichen Eingriff in die Privat- und Intimsphäre der betroffenen Person dar, so dass nicht schon jegliches abstraktes Gefahrenpotenzial im Sinne des Sicherheits- und Polizeirechts ausreicht. Dies muss zu einem strengeren Regelungsstandard bei den Eingriffsschwellen für solche Durchsuchungen führen. Bei einer Gesamt abwägung der Schwere des mit der Durchsuchung verbundenen Eingriffs und bei dem Gewicht der ihn rechtfertigenden Gründe des Gemeinwohls ist die Grenze des zumutbaren Grundrechtseingriffs nur gewahrt, wenn im Hinblick auf die Kontrollziele des § 15 Absatz 1 Nummer 6 BbgPolG eine Eingriffsschwelle in der Ge-

stalt eines erhöhten abstrakten Gefahrenpotenzials beachtet wird (vgl. BayVerfGH, Entscheidung vom 7. Februar 2006, Vf. 69-VI-04).

Ein erhöhtes abstraktes Gefahrenpotenzial setzt insbesondere voraus, dass solche Durchsuchungen nicht aufgrund einer ungesicherten oder nur diffusen Tatsachenbasis erfolgen dürfen. Die präventivpolizeiliche Durchsuchung bereits im Vorfeld konkreter Gefahren darf nicht bloß ein allgemeiner Gefahrerforschungseingriff sein. Dies wäre auch im Hinblick auf die Schwere des Eingriffs, die mit einer solchen Durchsuchung verbunden ist, unverträglich. Der Aufenthalt der zu durchsuchenden Person in den Bereichen des § 15 Absatz 1 Nummer 6 BbgPolG reicht deshalb als solcher ebenso wenig aus wie bloße Vermutungen über abstrakte Gefahren, die nicht durch ein Mindestmaß an Indizien untermauert sind. Die Tatsachenbasis braucht aber nicht so konkret zu sein, dass eine Verletzung der Schutzgüter des § 15 Absatz 1 Nummer 6 BbgPolG bereits als wahrscheinlich erscheint. Über allgemeine Lageerkenntnisse oder polizeiliche Erfahrungssätze hinaus müssen jedenfalls tatsächliche Anhaltspunkte bestehen, die den Schluss auf ein erhöhtes abstraktes Gefahrenpotenzial bezüglich der Kontrollziele zulassen. Dabei kann es sich etwa um durch Indizien angereicherte, also um hinreichend gezielte Anhaltspunkte oder um das Vorliegen von Täterprofilen oder Fahndungsrastern handeln, die beispielsweise auch im Rahmen internationaler Zusammenarbeit der Polizei- und Sicherheitsbehörden gewonnen werden. Für eine solche Prognose eines erhöhten abstrakten Gefahrenpotenzials können naturgemäß aber auch Eindrücke verarbeitet werden, die die handelnden Polizeibeamten bei einer vorausgehenden Identitätskontrolle gewinnen, wenn sie beispielsweise irgendwelche Auffälligkeiten registrieren.

Wird diese Eingriffsschwelle beachtet, sind die Eingriffsbefugnisse zur Durchsuchung von Personen und Sachen an den in § 15 Absatz 1 Nummer 4 und 6 BbgPolG durch eine Präventionsplanung konkretisierten Orten durch hinreichende Gründe des Gemeinwohls – dem Interesse an der Sicherheit des Staates und dem Schutz seiner Bevölkerung – getragen. Der betroffenen Person ist die Durchsuchung trotz der Schwere des damit verbundenen Eingriffs unter solchen Umständen zumutbar.

Im neuen § 27 BbgPolG zum Betreten und Durchsuchen von Wohnungen wird in Absatz 1 Satz 1 Nummer 4 die „gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person oder für Sachen von bedeutendem Wert“ durch die „erhebliche konkrete Gefahr“ ersetzt.

Die neue Nummer 5 dient der Sicherstellung des Eingriffs in informationstechnische Systeme nach § 49 Absatz 2 BbgPolG. Das Betreten und Durchsuchen von Wohnungen und anderen Räumen kann erforderlich sein, um Eingriffe in informationstechnische Systeme vorzubereiten und zu ermöglichen, damit beispielsweise informationstechnische Systeme gefunden werden.

In Absatz 2 wird das Tatbestandsmerkmal der „Abwehr einer dringenden konkreten Gefahr“ eingefügt.

In Absatz 3 Nummer 2 werden den Wörtern „der Prostitution“ die Wörter „einem schwerwiegenden Kriminalitätsphänomen oder“ vorangestellt.

Im neuen § 28 BbgPolG zum Verfahren bei der Durchsuchung von Wohnungen werden grammatikalische Anpassungen vorgenommen und in Absatz 2 ein Satz

angefügt, der das Anwesenheitsrecht in den Fällen des § 27 Absatz 1 Satz 1 Nummer 5 BbgPolG einschränkt. Um den Zweck des Eingriffs in informationstechnische Systeme nicht zu gefährden, ist vor der Wohnungsinhaberin bzw. dem Wohnungsinhaber und ihr bzw. ihm nahestehenden Personen das Betreten und die Durchsuchung der Wohnung geheim zu halten. Die Vorfeldmaßnahmen müssen zwingend verdeckt erfolgen. Die Auswirkungen auf die Regelungen zu Niederschriften müssen durch keine Änderungen abgebildet werden, weil keine zeitliche Aussage getroffen wird und somit auch eine zeitliche Verschiebung der schriftlichen Bestätigung gegenüber der betroffenen Person eröffnet ist, die dann zeitgleich mit der Benachrichtigung über die Maßnahme nach § 49 Absatz 2 BbgPolG erfolgen kann.

Zu Nummern 28 bis 31 (§§ 29 bis 32)

Im neuen § 29 BbgPolG zur Sicherstellung wird in Absatz 1 Nummer 1 die erhebliche konkrete Gefahr eingefügt. Die neue Nummer 2 umfasst die Verhütung oder vorbeugende Bekämpfung von Straftaten, Ordnungswidrigkeiten oder Kriminalitätsphänomenen, wenn Tatsachen die Annahme rechtfertigen, dass sie zur Begehung, Veranlassung oder Unterstützung von Straftaten oder Ordnungswidrigkeiten oder für ein Kriminalitätsphänomen gebraucht oder verwertet werden soll. Weitere numerische und grammatikalische Anpassungen werden vorgenommen.

In Absatz 2 wird eine ausdrückliche Regelung zur Sicherstellung durch Pfändung von unbaren Vermögensrechten wie Forderungen, elektronischem Geld und digitalen Zahlungsmitteln (z.B. Bitcoins) geschaffen. In den Polizeigesetzen von Bayern und Baden-Württemberg ist bereits die Möglichkeit der Beschlagnahme von Forderungen oder anderen Vermögensrechten durch Pfändung entsprechend den Vorschriften der Zivilprozessordnung enthalten. Auf Grund des bestehenden rechtspraktischen Bedürfnisses für die präventivpolizeiliche Sicherstellung auch unbarer Vermögenswerte ist eine explizite und zugleich den aktuellen Stand von Wirtschaft und Technik (z.B. Kryptowährungen) abbildende, zukunfts offene Sicherstellungsregelung zu schaffen. Der Landesgesetzgeber hat die entsprechende Gesetzgebungskompetenz, da es sich um eine polizeirechtliche vorläufige und nicht um eine straf- und strafverfahrensrechtliche endgültige (vgl. § 76a Absatz 4 StGB und §§ 435 ff. StPO) Vermögensabschöpfung handelt.

Im neuen Absatz 3 Satz 1 wird die Sicherstellung von Daten und Datenbeständen geregelt, wenn andernfalls die Abwehr der Gefahr, die Verhütung oder vorbeugende Bekämpfung von Straftaten, Ordnungswidrigkeiten oder Kriminalitätsphänomenen oder der Schutz vor Verlust oder die Verhinderung der Verwendung aussichtslos oder wesentlich erschwert wäre. Hierunter fallen auch die Sicherstellung und die Entziehung von Zugangsdaten außerhalb eines laufenden Telekommunikationsvorgangs. Eine derartige Sicherstellung erfolgt entsprechend der Grundkonzeption der Sicherstellungsregelungen als grundsätzlich offene Maßnahme. § 26 Absatz 2 Satz 1 BbgPolG und § 34 BbgPolG gelten nach Satz 2 entsprechend. So ist auch hier, soweit erforderlich, die Sicherstellung von Daten, die sich an von der benutzten Endeinrichtung der betroffenen Person entfernten Speicherorten (etwa auf serverbasierten Clouds) befinden, zulässig. Zudem wird angesichts der möglichen Eingriffstiefe auf die Regelung zum Schutz von Berufsgeheimnisträgern und zum Kernbereich privater Lebensführung ausdrücklich hingewiesen. Die Daten sind besonders zu kennzeichnen. Daten, die nach diesen Vorschriften nicht weiterverarbeitet werden dürfen, sind zu löschen, soweit es sich nicht um Daten handelt, die zusammen mit dem Datenträger sichergestellt wur-

den, auf dem sie gespeichert sind. Löschungen sind zu dokumentieren. Die Bestimmungen in den §§ 30, 31 Absatz 4 und § 32 Absatz 1 BbgPolG hinsichtlich Verwahrung, Benachrichtigung, Vernichtung und Herausgabe gelten unter Berücksichtigung der unkörperlichen Natur von Daten sinngemäß.

Im neuen § 30 BbgPolG erfolgen grammatikalische Anpassungen.

Im neuen § 31 BbgPolG werden grammatikalische und inhaltliche Anpassungen vorgenommen. In Absatz 3 Satz 1 wird die Angabe „§ 979 Abs. 1“ durch die Wörter „§ 979 Absatz 1 bis 1 Buchstabe b“ des Bürgerlichen Gesetzbuches ersetzt. Weiterhin wird geregelt, dass bei der Verwertung von Datenträgern sicherzustellen ist, dass zuvor personenbezogene Daten dem Stand der Technik entsprechend gelöscht wurden. Ein Zuschlag bei der öffentlichen oder der im Internet allgemein zugänglichen Versteigerung, der freihändige Verkauf oder die Zuführung zu einem gemeinnützigen Zweck ist zu versagen, wenn dadurch die Voraussetzungen der Sicherstellung erneut eintreten würden.

Im neuen § 32 BbgPolG erfolgen grammatikalische, paragrafenverweisliche und inhaltliche Anpassungen. Absatz 2 begrenzt die Sicherstellung von Vermögensrechten im Sinne des § 29 Absatz 2 BbgPolG grundsätzlich auf ein Jahr mit jeweils entsprechender Verlängerungsmöglichkeit, wenn andernfalls die Sicherstellungsvoraussetzungen erneut eintreten würden. Um den von einer derartigen Sicherstellung betroffenen Personen in ausreichendem Maße effektiven Rechtsschutz zu gewähren, ist in diesen Verlängerungsfällen eine gerichtliche Zustimmung erforderlich.

Zu Nummer 32 (§§ 33 bis 67)

Kapitel 2 Abschnitt 2 zur Datenverarbeitung wird neu gefasst. In diesem Abschnitt werden die EU-Datenschutzrichtlinie für den Bereich der Polizei und Rechtsprechung des Bundesverfassungsgerichtes umgesetzt sowie neue Befugnisnormen eingeführt bzw. bestehende abgeändert. Der Abschnitt ist in die folgenden fünf Unterabschnitte unterteilt:

- Unterabschnitt 1 – Allgemeine Vorschriften zur Datenverarbeitung und zum Datenschutz (§§ 33-41 BbgPolG),
- Unterabschnitt 2 – Datenerhebung (§§ 42-55 BbgPolG),
- Unterabschnitt 3 – Datenspeicherung, Datenveränderung und Datennutzung (§§ 56-59 BbgPolG),
- Unterabschnitt 4 – Datenübermittlung (§§ 60-66 BbgPolG),
- Unterabschnitt 5 – Datenberichtigung, Datenlöschung und Datensperrung (§ 67 BbgPolG).

Zu § 33 (Grundsätze der Datenverarbeitung)

Der neue § 33 BbgPolG stellt in Absatz 1 Satz 1 klar, dass die Regelungen des Abschnitts 2 vorbehaltlich abweichender Regelungen grundsätzlich für alle Datenverarbeitungen der Polizei nach dem Polizeigesetz gelten, unabhängig davon, innerhalb welcher Strukturen die Verarbeitung personenbezogener Daten erfolgt (z. B. in Akten, Dateien oder anderweitigen Informationssystemen). Diese Regelung

trägt dem Umstand Rechnung, dass sich die Neufassung des BKAG etwa in den §§ 13 ff. sowie in § 29 BKAG, mit Relevanz insbesondere auch für den Bundesländer-Datenverbund, des Begriffs des Informationssystems bedient. Außerdem sind die materiell-rechtlichen Vorgaben des EU-Datenschutzrechts wie auch des Bundesverfassungsgerichtes unabhängig von der technischen Umsetzung und Bezeichnung des Speicherorts umzusetzen. Satz 2 stellt klar, dass die Polizei personenbezogene Daten nur verarbeiten darf, soweit dies durch dieses Gesetz oder andere Rechtsvorschriften über die Datenverarbeitung der Polizei zugelassen ist.

Absatz 2 verankert die Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten des Artikels 4 Absatz 1 der EU-Datenschutzrichtlinie für den Bereich der Polizei im Polizeigesetz. Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollen gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Diese Richtlinie soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts beitragen. Der freie Verkehr personenbezogener Daten zwischen den zuständigen Behörden zum Zwecke der Verhütung und vorbeugenden Bekämpfung von Straftaten, Ordnungswidrigkeiten und Kriminalitätsphänomenen sowie des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit und der Verfolgung von Straftaten innerhalb der Union und die Übermittlung solcher personenbezogener Daten an Drittländer und internationale Organisationen, soll erleichtert und dabei gleichzeitig ein hohes Schutzniveau für personenbezogene Daten gewährleistet werden.

Die Grundsätze des Datenschutzes sollen für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollen alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollen alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologischen Entwicklungen zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollen daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht mehr identifiziert werden kann.

Jede Verarbeitung personenbezogener Daten muss auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffenen natürlichen Personen nachvollziehbaren Weise erfolgen, und die Daten dürfen nur für bestimmte, durch Rechtsvorschriften geregelte Zwecke verarbeitet werden. Dies steht an sich der Durchführung von verdeckten Maßnahmen oder Videoüberwachung nicht entgegen. Diese Maßnahmen können zwecks Verhütung oder vorbeugender Bekämpfung von Straftaten, Ordnungswidrigkeiten oder Kriminalitätsphänomenen sowie des Schutzes vor oder 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 natürlichen Person gebührend berücksichtigt werden. Natürliche Personen sollen

über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können. Insbesondere sollen die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt deren Erhebung feststehen. Die personenbezogenen Daten sollen für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sein. Es soll insbesondere sichergestellt werden, dass nicht übermäßige personenbezogene Daten erhoben werden und sie nicht länger aufbewahrt werden, als dies für den Zweck, zu dem sie verarbeitet werden, erforderlich ist. Personenbezogene Daten sollen nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Um sicherzustellen, dass die Daten nicht länger als nötig gespeichert werden, soll der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen. Es sollen geeignete Garantien für den Fall festgelegt werden, dass personenbezogene Daten für die Archivierung im öffentlichen Interesse und die wissenschaftliche, statistische oder historische Verwendung für längere Zeiträume gespeichert werden.

Die Polizei muss personenbezogene Daten, die im Zusammenhang mit der Verhütung oder vorbeugenden Bekämpfung von Straftaten, Ordnungswidrigkeiten oder Kriminalitätsphänomenen sowie dem Schutz vor oder der Abwehr von Gefahren für die öffentliche Sicherheit erhoben wurden, auch in einem anderen Kontext verarbeiten können, um sich ein Bild von den kriminellen Handlungen machen und Verbindungen zwischen verschiedenen aufgedeckten Straftaten, Ordnungswidrigkeiten und Kriminalitätsphänomenen herstellen zu können.

Um stets eine sichere Verarbeitung zu gewährleisten und Verarbeitungen, die gegen diese Vorschriften verstoßen, zu verhindern, sollen personenbezogene Daten so verarbeitet werden, dass ein Maß an Sicherheit und Vertraulichkeit gegeben ist, wozu auch gehört, dass unbefugte Personen keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können, und dass die Verarbeitung den Stand der verfügbaren Technik, die Kosten für ihre Einführung im Verhältnis zu den von der Verarbeitung ausgehenden Risiken und die Art der zu schützenden personenbezogenen Daten berücksichtigt.

Personenbezogene Daten sollen für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht zu Zwecken verarbeitet werden, die nicht mit den Zwecken der Verhütung oder vorbeugenden Bekämpfung von Straftaten, Ordnungswidrigkeiten oder Kriminalitätsphänomenen, des Schutzes vor oder der Abwehr von Gefahren für die öffentliche Sicherheit oder der Verfolgung von Straftaten zu vereinbaren sind. Werden personenbezogene Daten von demselben oder einem anderen Verantwortlichen für einen anderen der genannten Zwecke als den, für den sie erhoben wurden, verarbeitet, so soll diese Verarbeitung erlaubt sein, unter der Bedingung, dass diese Verarbeitung nach den geltenden Rechtsvorschriften zulässig ist und dass sie für diesen anderen Zweck erforderlich und verhältnismäßig ist.

Der Grundsatz der sachlichen Richtigkeit der Daten soll unter Berücksichtigung von Art und Zweck der jeweiligen Verarbeitung angewandt werden. Aussagen, die personenbezogene Daten enthalten, basieren auf der subjektiven Wahrnehmung von natürlichen Personen und sind nicht immer nachprüfbar. Infolgedessen soll sich der Grundsatz der sachlichen Richtigkeit nicht auf die Richtigkeit einer Aus-

sage beziehen, sondern lediglich auf die Tatsache, dass eine bestimmte Aussage gemacht worden ist.

Die zuständigen Behörden sollen dafür sorgen, dass personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht übermittelt oder bereitgestellt werden. Um den Schutz natürlicher Personen, die Richtigkeit, die Vollständigkeit oder den Aktualitätsgrad sowie die Zuverlässigkeit der übermittelten oder bereitgestellten personenbezogenen Daten zu gewährleisten, sollen die zuständigen Behörden möglichst bei allen Übermittlungen personenbezogener Daten die erforderlichen Informationen beifügen.

Durch Absatz 3 wird Artikel 6 der EU-Datenschutzrichtlinie für den Bereich der Polizei zur Unterscheidung verschiedener Kategorien betroffener Personen umgesetzt. Bei der Verarbeitung personenbezogener Daten geht es naturgemäß um betroffene Personen verschiedener Kategorien. Daher soll gegebenenfalls und so weit wie möglich klar zwischen den personenbezogenen Daten der einzelnen Kategorien betroffener Personen unterschieden werden wie verdächtige Personen, verurteilte Personen, Opfer und andere Personen, beispielsweise Zeugen, Personen, die über einschlägige Informationen verfügen, oder Personen, die mit Verdächtigen oder verurteilten Straftätern in Kontakt oder in Verbindung stehen.

Durch Absatz 4 wird Artikel 7 Absatz 1 der EU-Datenschutzrichtlinie für den Bereich der Polizei zur Erkennbarkeit tatsachen- oder einschätzungsbasierter personenbezogener Daten umgesetzt.

In Absatz 5 werden Grunddaten festgelegt, die stets zur Identitätsfeststellung verarbeitet werden dürfen: Familiennamen, Vornamen, Geburtsnamen, sonstige Namen und andere Namensschreibweisen, Geschlecht, Geburtsdatum, Geburtsort, Geburtsstaat, derzeitige und frühere Staatsangehörigkeiten, gegenwärtige und frühere Aufenthaltsorte, Wohnanschrift sowie Sterbedatum.

Absatz 6 Satz 1 regelt die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten entsprechend Artikel 10 der EU-Datenschutzrichtlinie für den Bereich der Polizei. Besondere Kategorien personenbezogener Daten sind nach der Definition des neuen § 3 BbgPolG solche, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Feststellung der Identität einer Person, Gesundheitsdaten und Daten zum Sexualleben oder der sexuellen Orientierung. In der polizeilichen Praxis sind in diesem Zusammenhang beispielsweise bestimmte personenbezogene Hinweise hinsichtlich der Zugehörigkeit etwa zu gefährlichen, extremistischen politischen Gruppierungen von hoher Relevanz. Ein anderes Praxisbeispiel sind im Einzelfall zur Eigensicherung von Polizeibeamten erforderliche Hinweise auf ein gravierendes gesundheitliches Ansteckungsrisiko einer Person. Derartige personenbezogene Hinweise sollen auch weiterhin möglich sein, zumal sie bereits jetzt nur unter engen Voraussetzungen erfolgen dürfen. Satz 2 regelt eine regelmäßige Kennzeichnungspflicht der Daten und besondere Ausgestaltung des Zugriffs auf diese, soweit dies zum Schutz der betroffenen Personen erforderlich ist. Insoweit bedarf es einer näheren Prüfung der Schutzbedürftigkeit der jeweiligen Daten in Verbindung mit dem entsprechenden Verarbeitungsvorgang. Von der in Absatz 6 enthaltenen Regelung unberührt bleiben dabei gesetzliche Spezialregelungen, die den Umgang mit bestimmten Daten, die besonderen Kategorien zugehören, regeln: So sind etwa bei Erfüllung der strengen Voraussetzun-

gen einer erkenntnisdienlichen Behandlung auch die Kriterien für eine Verarbeitung von Daten im Sinne des Absatzes 6 erfüllt. Zudem erfährt eine Datenerhebung im Sinne von Satz 1, die zugleich dem in besonderen Datenerhebungsvorschriften geregelten Kernbereichsschutz unterfällt, bereits nach diesem einen besonderen gesetzlichen Schutz. Ist eine solche Datenerhebung und ggf. auch (weitere) Datenverarbeitung nach den Kernbereichsregelungen ausnahmsweise zulässig, ist damit eine nochmalige Prüfung der Datenverarbeitung nach Absatz 6 nicht mehr geboten.

Absatz 7 setzt die Regelung des Artikels 11 der EU-Datenschutzrichtlinie für den Bereich der Polizei zur automatisierten Entscheidungsfindung im Einzelfall um. Der Einsatz von Systemen der automatischen Datenverarbeitung zur automatisierten Entscheidungsfindung, an den sich eine nachteilige Rechtsfolge für die betroffene Person knüpft oder der diese erheblich beeinträchtigt, kann durch Regelungen in diesem Gesetz erlaubt werden, wenn die Entscheidung durch den zuständigen Entscheidungsträger überprüft und im Rahmen einer umfassenden und schriftlich zu dokumentierenden Abwägung die Rechte und Freiheiten der betroffenen Person hinreichend berücksichtigt werden. Bei Gefahr im Verzug kann zunächst eine dokumentierte summarische Abwägung vorgenommen werden; die Abwägung nach Satz 1 wird unverzüglich nachgeholt. Die betroffene Person soll das Recht haben, keiner Entscheidung zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die nachteilige rechtliche Wirkung für sie entfaltet oder sie in erheblichem Maße beeinträchtigt. In jedem Fall soll eine solche Verarbeitung mit geeigneten Garantien verbunden sein, einschließlich der spezifischen Unterrichtung der betroffenen Person und des Rechts, das Eingreifen einer Person zu erwirken, insbesondere auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung oder auf Anfechtung der Entscheidung.

Zu § 34 (Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung)

Im neuen § 34 BbgPolG werden die bislang in einzelnen Befugnisnormen enthaltenen Vorschriften zum Schutz von nach der Strafprozessordnung zeugnisverweigerungsberechtigten Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung an zentraler Stelle zusammengeführt und das Schutzniveau an die verfassungsgerichtlichen Vorgaben angepasst und ausgeweitet. Die Regelungen beziehen sich auf die Datenverarbeitung insgesamt.

Absatz 1 regelt den Schutz von Berufsgeheimnisträgern. Ist oder wird bei Maßnahmen der Datenverarbeitung erkennbar, dass in ein durch ein Berufsgeheimnis nach den §§ 53, 53a der Strafprozessordnung geschütztes Vertrauensverhältnis eingegriffen wird, ist die Datenverarbeitung insoweit unzulässig, es sei denn, die Maßnahmen richten sich gegen den Berufsgeheimnisträger selbst oder in diesem Gesetz werden abweichende Regelungen getroffen. Eine bereits laufende Datenverarbeitung ist unverzüglich und solange erforderlich zu unterbrechen oder zu beenden. Erlangte Erkenntnisse dürfen nicht weiter verarbeitet werden.

In Absatz 2 wird der Kernbereichsschutz geregelt insbesondere die Unzulässigkeit der Datenverarbeitung bei Kernbereichsbetroffenheit, deren Einschränkungen und Ausnahmen.

Absatz 3 regelt für die Daten nach den Absätzen 1 und 2, die nicht verarbeitet werden dürfen, die Löschung und deren Protokollierung.

Das Bundesverfassungsgericht hat in seiner Entscheidung zum Bundeskriminalamtgesetz vom 20. April 2016 den Schutz des Kernbereichs privater Lebensgestaltung gestärkt. Der Gesetzgeber schafft dementsprechend Regelungen, die einen wirksamen Schutz normenklar gewährleisten. Der alte § 29 Absatz 6 BbgPolG hat dies bereits für die Datenerhebung normiert. Der Kernbereichsschutz gilt jedoch für die weitere Datenverarbeitung. Die strengeren Maßstäbe des Bundesverfassungsgerichtes werden nun gesetzlich umgesetzt:

- Sichtung der erfassten Daten durch eine unabhängige Stelle, welche die kernbereichsrelevanten Informationen herausfiltert,
- Kontrolle durch externe, nicht mit Sicherheitsaufgaben betraute Personen,
- sofortige Löschung von gegebenenfalls erfassten höchstpersönlichen Daten und Ausschluss jeglicher Verarbeitung und
- Protokollierung der Löschung, die eine spätere Kontrolle ermöglicht.

Zu § 35 (Benachrichtigungspflichten)

Im neuen § 35 BbgPolG werden die größtenteils bereits vorhandenen Regelungen zu Benachrichtigungspflichten nach Durchführung von Datenerhebungsmaßnahmen in einer zentralen Vorschrift zusammengeführt, vereinheitlicht und für die Datenverarbeitung insgesamt geregelt. Insoweit erfolgt eine Orientierung an bestehenden strafprozessualen Benachrichtigungsregelungen.

Absatz 1 enthält die Benachrichtigungs- und Nachforschungspflicht, Einschränkungen und Ausnahmen von diesen sowie Sonderregelungen für minderjährige Personen (vgl. § 101 StPO und §§ 74 ff. BKAG).

Absatz 2 legt den Inhalt der Benachrichtigung sowie das Zustimmungserfordernis für Daten von oder an die deutschen Nachrichtendienste fest.

Absatz 3 regelt die Besonderheiten bei einem strafrechtlichen Ermittlungsverfahren einschließlich des Abstimmungserfordernisses mit der Staatsanwaltschaft.

Absatz 4 umfasst die Zurückstellung und das Unterbleiben der Benachrichtigung auf Grundlage einer richterlichen Zustimmung sowie daran anknüpfende Vorgaben zur Datenlöschung und deren Dokumentation.

Zu § 36 (Auskunftsrecht, Akteneinsicht)

Durch den neuen § 36 BbgPolG werden das Auskunftsrecht und die Akteneinsicht des alten § 71 BbgPolG übernommen und teilweise erweitert bzw. modifiziert. Dies dient im Wesentlichen der Umsetzung von Artikel 14 und 15 der EU-Datenschutzrichtlinie für den Bereich der Polizei.

Das Auskunftsrecht wird in Absatz 1 geregelt. Die Erteilung der Auskunft hat nach Artikel 12 Absatz 4 Satz 1 der EU-Datenschutzrichtlinie unentgeltlich zu erfolgen. Die Auskunft beinhaltet zunächst eine Bestätigung, ob personenbezogene Daten der betroffenen Person verarbeitet werden. Der Inhalt der Auskunft wird in Umset-

zung der EU-Datenschutzrichtlinie detailliert bestimmt. Auskunft wird dabei nur in dem Umfang gewährt, der sich aus dem Auskunftsverlangen selbst ergibt.

Absatz 2 regelt die Akteneinsicht und erfasst nunmehr neben den nichtelektronischen Akten und Dateien auch die elektronischen.

Absatz 3 schränkt die Auskunftserteilung und die Gewährung von Akteneinsicht ein, indem diese durch die Polizei unter den dort bestimmten Voraussetzungen verweigert werden kann.

Absatz 4 die Pflicht zur Unterrichtung im Falle keiner unverzüglichen Entscheidung über die Anträge nach Absatz 1 oder Absatz 2 sowie das Unterbleiben der Unterrichtung unter den dort bestimmten Voraussetzungen.

Absatz 5 umfasst die Dokumentation der Gründe für die Ablehnung eines Antrags und das Unterbleiben einer Unterrichtung sowie deren Zurverfügungstellung für die Kontrolle der oder des Landesbeauftragten. Eine Mitteilung der oder des Landesbeauftragten an die betroffene Person im Beschwerdeverfahren darf keine Rückschlüsse auf den Erkenntnisstand der Polizei zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

Absatz 6 regelt die Zustimmungserfordernisse der deutschen Nachrichtendienste, der Behörden des Bundesministeriums der Verteidigung, der Staatsanwaltschaften und der Steuerbehörden.

Zu § 37 (Verzeichnis von Verarbeitungstätigkeiten, Protokollierung, Kontrolle durch die oder den Landesbeauftragten)

Der neue § 37 Absatz 1 bis 3 BbgPolG dient der Umsetzung des Artikels 24 der EU-Datenschutzrichtlinie für den Bereich der Polizei. Die Behördenleitung der Polizei oder die auftragsverarbeitende Stelle führen ein Verzeichnis aller Kategorien von Tätigkeiten, die ihrer Zuständigkeit unterliegen. Sie sind verpflichtet, mit der oder dem Landesbeauftragten zusammenzuarbeiten und dieser auf Anfrage das Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieses Verzeichnisses kontrolliert werden können.

Die Protokollierung in Absatz 4 ist eine wirksame Methode zum Nachweis der Rechtmäßigkeit der Datenverarbeitung, zur Ermöglichung der Eigenüberprüfung und zur Sicherstellung der Integrität und Sicherheit der Daten. Diese dient auch dazu, die sachhaltige Prüfung durch die oder den Landesbeauftragten zu ermöglichen. Sie ist daneben aber auch die Datengrundlage, die erforderlich ist, um die Benachrichtigungspflichten zu erfüllen. Die Protokollierung verbessert die Nachvollziehbarkeit der Datenverarbeitung durch die Polizei.

Absatz 5 statuiert in Anlehnung an die Maßgaben des Bundesverfassungsgerichts im BKAG-Urteil eine Prüfpflicht der oder des Landesbeauftragten im Abstand von längstens zwei Jahren hinsichtlich der Datenverarbeitung der Polizei. Das Verzeichnis der Verarbeitungstätigkeit und die Protokollierungen sowie von Dokumentationen über Datenlöschungen und Vernichtung von Unterlagen sind in praktikabel auswertbarer Weise zur Verfügung zu stellen. Da es sich um Kontrollen handelt, wird keine umfassende Prüfung aller Datenbestände abverlangt.

Zu § 38 (Automatisierte Verfahren der Datenverarbeitung)

Der alte § 49 BbgPolG zum automatisierten Abrufverfahren wird durch den neuen § 38 BbgPolG ersetzt, durch den eine Reihe von Regelungen der EU-Datenschutzrichtlinie für den Bereich der Polizei umgesetzt wird.

So erfolgt in Absatz 1 bis 3 eine Anpassung an Artikel 25 EU-Datenschutzrichtlinie für den Bereich der Polizei. Insbesondere die Zulässigkeit automatisierter Verfahren der Datenverarbeitung, die Verarbeitungsvorgänge, die mindestens protokolliert werden müssen, und die Verwendungszwecke werden bestimmt. In automatisierten Verarbeitungssystemen werden zumindest über folgende Verarbeitungsvorgänge Protokolle geführt: Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlungen, Kombination oder Löschung. Die Identifizierung der Person, die personenbezogene Daten so verwendet, samt Geschäftszeichen soll protokolliert werden und aus dieser Identifizierung soll sich die Begründung für die Verarbeitungsvorgänge ableiten lassen. Die Protokolle sollen ausschließlich zum Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, einschließlich der Eigenüberwachung, der Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten, der Verhütung, vorbeugenden Bekämpfung, Unterbindung oder Verfolgung von Straftaten, Ordnungswidrigkeiten und Kriminalitätsphänomenen oder der Kontrolle durch die oder den Landesbeauftragten verwendet werden. Die Eigenüberwachung umfasst auch interne Disziplinarverfahren der zuständigen Behörden.

Absatz 4 legt ausdrücklich fest, dass die Polizei mit anderen Ländern und dem Bund einen Datenverbund vereinbaren kann.

Durch Absatz 5 wird Artikel 29 der EU-Datenschutzrichtlinie für den Bereich der Polizei zur Sicherheit der Verarbeitung personenbezogener Daten umgesetzt. Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung rechtswidriger Verarbeitung solle die Behördenleitung oder die auftragsverarbeitende Stelle die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen. Solche Maßnahmen sollen unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau – auch hinsichtlich der Vertraulichkeit – gewährleisten, das dem von der Verarbeitung ausgehenden Risiko und der Art der zu schützenden personenbezogenen Daten angemessen ist. Bei der Bewertung der Datensicherheitsrisiken sollen die mit der Datenverarbeitung verbundenen Risiken berücksichtigt werden, wie etwa Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte. Die Behördenleitung und die auftragsverarbeitende Stelle sollen sicherstellen, dass personenbezogene Daten nicht durch Unbefugte verarbeitet werden. Um dies zu erreichen, wird der Katalog an Sicherheitsmaßnahmen aus der Richtlinie übernommen.

Absatz 6 regelt die Vorgaben des Artikels 30 der EU-Datenschutzrichtlinie für den Bereich der Polizei zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die oder den Landesbeauftragten. Eine Verletzung des Schutzes personenbezogener Daten kann – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudo-

nymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene Person. Deshalb soll die Behördenleitung, sobald ihr eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die oder den Landesbeauftragten von der Verletzung des Schutzes personenbezogener Daten unverzüglich und, falls möglich, binnen höchstens 72 Stunden nachdem ihr die Verletzung bekannt wurde, unterrichten, es sei denn die Behördenleitung kann im Einklang mit dem Grundsatz der Rechenschaftspflicht nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt. Falls diese Benachrichtigung nicht binnen 72 Stunden erfolgen kann, sollen in ihr die Gründe für die Verzögerung angegeben werden, und die Informationen können schrittweise ohne unangemessene weitere Verzögerung bereitgestellt werden.

Absatz 7 umfasst die Regelung des Artikels 31 der EU-Datenschutzrichtlinie für den Bereich der Polizei zur Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person. Natürliche Personen, sollen unverzüglich benachrichtigt werden, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt, damit sie die erforderlichen Vorkehrungen treffen können. Die Benachrichtigung soll eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene natürliche Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung enthalten. Die Benachrichtigung der betroffenen Person soll stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der oder dem Landesbeauftragten und nach Maßgabe der von dieser oder diesem oder von anderen zuständigen Behörden erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, sollte die betroffene Person sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder ähnliche Verletzungen des Schutzes von Daten zu treffen. In den bezeichneten Ausnahmefällen kann die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen natürlichen Person unterbleiben.

Zu § 39 (Errichtungsanordnung für Dateien, Datenschutz-Folgenabschätzung)

Der neue § 39 BbgPolG regelt nunmehr die Errichtungsanordnung und die Datenschutz-Folgenabschätzung.

Absatz 1 hat das Instrument der Errichtungsanordnung für den erstmaligen Einsatz von automatisierten Verfahren zum Regelungsgegenstand. Errichtungsanordnungen sind weder in der EU-Datenschutzrichtlinie für den Bereich der Polizei noch in der EU-Datenschutz-Grundverordnung vorgesehen. Gleichwohl hat sich dieses Instrument der Planung und des Datenschutzes beispielsweise in Bayern in der Praxis bewährt. Errichtungsanordnungen dienen als wesentlicher Maßstab, um zu beurteilen, welchem Zweck gespeicherte Daten im Einzelfall dienen sollen und ob sie dafür erforderlich sind. Damit sind sie gleichzeitig wesentliche Grundlage für die Selbstkontrolle der Polizei und für die Datenschutzkontrolle. Dadurch kann die Einhaltung insbesondere der in § 33 Absatz 2 BbgPolG niedergelegten

Grundsätze in der polizeilichen Praxis gewährleistet werden. Darüber hinaus wird dadurch auch eine mögliche Datenschutz-Folgeabschätzung erleichtert.

Absatz 2 regelt die von Artikel 27 der EU-Datenschutzrichtlinie für den Bereich der Polizei vorgegebene Datenschutz-Folgeabschätzung. Eine Datenschutz-Folgeabschätzung, die sich insbesondere mit den Maßnahmen, Garantien und Verfahren befasst, die geplant sind, den Schutz personenbezogener Daten zu gewährleisten, soll durch die Behördenleitung durchgeführt werden, wenn die Verarbeitungsvorgänge aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge haben. Datenschutz-Folgeabschätzungen sollen auf maßgebliche Systeme und Verfahren im Rahmen von Verarbeitungsvorgängen abstellen, nicht jedoch auf Einzelfälle.

Zu § 40 (Anwendung des Brandenburgischen Datenschutzgesetzes)

In Umsetzung der EU-Datenschutzrichtlinie für den Bereich der Polizei regelt das Brandenburgische Polizeigesetz insbesondere in Kapitel 2 Abschnitt 2 Unterabschnitt 1 bereichsspezifisch den Datenschutz, dessen Vorschriften dem Brandenburgischen Datenschutzgesetz vorgehen. Dies gilt nach § 40 BbgPolG jedenfalls insoweit, als die Vorschriften des Brandenburgischen Polizeigesetzes eine eigene abschließende Regelung enthalten und nicht andere Spezialvorschriften greifen. Punktuell werden die Vorschriften auch durch die allgemeinen Vorschriften des Brandenburgischen Datenschutzgesetzes ergänzt. § 28 des Brandenburgischen Datenschutzgesetzes zur Videoüberwachung gilt ausschließlich in Ausübung des Hausrechts bei der Polizei. Die Videoüberwachung zur Erfüllung polizeilicher Aufgaben richtet sich hingegen nach den Vorschriften dieses Gesetzes.

Zu § 41 (Parlamentarische Kontrolle)

Der neue § 41 BbgPolG weitert die bisher in einzelnen Befugnisnormen verankerte parlamentarische und öffentliche Kontrolle auf alle Maßnahmen nach Kapitel 2 Abschnitt 2 Unterabschnitt 2 und die mit diesen im Zusammenhang stehenden weiteren Maßnahmen aus. Durch den Gesetzgeber wird ein Mindestmaß an Angaben vorgegeben, die sich in dem Bericht wiederfinden müssen. Hierbei sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren.

Zu § 42 (Grundsätze der Datenerhebung)

Der neue § 42 BbgPolG knüpft an den alten § 29 BbgPolG an. Insbesondere im Hinblick auf die neue Systematik mit einem allgemeinen Unterabschnitt zur Datenverarbeitung und im Hinblick auf die EU-Datenschutzrichtlinie für den Bereich der Polizei erfolgen kleinere Anpassungen. Außerdem wird die Vorschrift übersichtlicher strukturiert.

Absatz 1 übernimmt leicht angepasst die Vorschrift des alten Absatzes 2.

Absatz 2 regelt in Modifizierung des alten Absatzes 4 die offene Datenerhebung unter Berücksichtigung der Vorgaben aus Artikel 12 und 13 der EU-Datenschutzrichtlinie für den Bereich der Polizei über die einer betroffenen Person zur Verfügung zu stellenden oder zu erteilenden Informationen. Das Informieren kann dabei insbesondere durch eine allgemein zugängliche Veröffentlichung in schriftlicher oder elektronischer Form erfolgen. Das Informieren kann in den Fällen des Absat-

zes 3 Satz 1 Nummer 1 bis 3 zunächst unterbleiben. Sind die Voraussetzungen für das Unterbleiben entfallen, ist unverzüglich zu informieren.

Absatz 4 umfasst den Ausnahmefall der – nicht in besonderen Vorschriften geregelt – verdeckten Datenerhebung. Die Vorschrift wird an Artikel 13 Absatz 3 der EU-Datenschutzrichtlinie für den Bereich der Polizei angepasst. Eine solche Datenerhebung ist zulässig, wenn

- dies durch Gesetz bestimmt wird,
- die Erfüllung polizeilicher Aufgaben oder behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren auf andere Weise gefährdet oder behindert würden,
- anzunehmen ist, dass dies überwiegenden Interessen oder schutzwürdigen Belangen der betroffenen Personen dient oder
- dies dem Schutz der Rechte und Freiheiten Dritter dient.

Sind die Voraussetzungen für eine verdeckte Datenerhebung entfallen, erfolgt eine Benachrichtigung der betroffenen Person und Dritter nach § 35 BbgPolG.

Zu § 43 (Allgemeine Befugnis zur Datenerhebung)

Der neue § 43 BbgPolG orientiert sich weitgehend am alten § 30 BbgPolG. In Absatz 1 werden Paragrafenverweise angepasst sowie die Begriffe „Kriminalitätsphänomenen“ und „Personenschutz“ eingefügt. In Absatz 2 werden eine neue Nummer 2 „verantwortliche Personen für Veranstaltungen in der Öffentlichkeit“, die nicht dem Versammlungsgesetz unterliegen, und die Wörter „akademische Grade“ eingefügt.

Zu § 44 (Offene Bild- und Tonaufnahmen oder -aufzeichnungen)

Absatz 1:

Der neue § 44 Absatz 1 BbgPolG wird gegenüber dem alten § 31 Absatz 1 BbgPolG hinsichtlich der Tatbestandsvoraussetzungen und Rechtsfolgen weiterentwickelt und neu strukturiert.

Der Anwendungsbereich des Versammlungsgesetzes wird nicht erweitert, da die erfassten öffentlichen Veranstaltungen und Ansammlungen nicht dem Versammlungsgesetz unterliegen dürfen. Öffentliche Veranstaltungen sind solche zu denen der Zutritt nicht auf einen namentlich oder individuell bestimmbar Personenkreis beschränkt, sondern einer unbestimmten Anzahl von Menschen gestattet ist, an einer Veranstaltung teilzunehmen (z.B. Sportveranstaltungen, Volks- und Bürgerfeste, Weihnachtsmärkte und kulturelle Veranstaltungen). Die Erhebung von Eintrittsgeldern, der Ausschluss bestimmter Personen oder Personengruppen, lediglich die Bezeichnung als „nichtöffentlich“ und ein Veranstaltungsort in geschlossenen Räumen lassen den öffentlichen Charakter einer Veranstaltung nicht automatisch entfallen. Ansammlungen sind ungeplante Zusammenkünfte von mehreren Personen, die in der Regel keinen gemeinschaftlich verfolgten Zweck haben, keiner vorherigen Absprache bedurften und bei denen keine kollektiven Aussagen zu öffentlichen Angelegenheiten gemacht werden.

Die Polizei kann vor, bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, personenbezogene Daten nach Nummer 1 durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen über für eine Gefahr verantwortliche Personen und Teilnehmer erheben. Zeitlich kann im Vorfeld einer Veranstaltung die Bild- und Tonüberwachung eingesetzt werden, um insbesondere Vorbereitungshandlungen für Straftaten oder terroristische Anschläge zu erkennen. Dies bezieht sich nicht nur auf die An- und Abreise zur Veranstaltung. Räumlich kann die Bild- und Tonüberwachung auf den Veranstaltungs- oder Ansammlungsort sowie auf die nähere im Zusammenhang stehende Umgebung ausgerichtet werden. Unter technischen Mitteln sind alle diejenigen zu verstehen, die die genannten Bild- und Tonaufnahmen sowie -aufzeichnungen zulassen.

In Nummer 2 wird eine ausdrückliche Regelung betreffend die Fertigung von Übersichtsaufnahmen oder -aufzeichnungen, einschließlich der gezielten Feststellung der Identität einer auf der Übersichtsaufzeichnung abgebildeten Person, bei öffentlichen Veranstaltungen und Ansammlungen getroffen, wenn dies aufgrund der Größe oder Unübersichtlichkeit der Örtlichkeit geboten ist. Auf Grund der noch größeren Bandbreite und, gerade was Ansammlungen betrifft, der deutlich geringeren Vorhersehbarkeit des Verhaltens einzelner Teilnehmer, sowie der im Gegensatz zu Versammlungen geringeren Grundrechtsrelevanz sind die Tatbestandsvoraussetzungen gelockert. Ob es neben Aufnahmen zur Übertragung und Beobachtung in Echtzeit auch der Speicherung in Form einer Übersichtsaufzeichnung bedarf, wird im jeweiligen Einzelfall unter Beachtung des Grundsatzes der Verhältnismäßigkeit zu entscheiden sein. Auf Grund der Größe und Unübersichtlichkeit kann sich das Erfordernis zur Fertigung von Bildaufnahmen insbesondere dann ergeben, wenn die Veranstaltung oder Ansammlung von zentral postierten Polizeibediensteten durch die Zahl der Teilnehmer oder der Beschaffenheit des Orts nicht überblickt werden kann. Die Identifizierung einzelner Personen in Form des „Hineinzoomens in die Übersichtsaufzeichnung“ ist erlaubt.

Voraussetzung für solche Maßnahmen sind Tatsachen, die die Annahme rechtfertigen, dass bei öffentlichen Veranstaltungen oder Ansammlungen Straftaten oder Ordnungswidrigkeiten begangen werden oder diese im Zusammenhang mit Kriminalitätsphänomenen stehen.

Absatz 2:

Der neue § 44 Absatz 2 BbgPolG wird gegenüber dem alten § 31 Absatz 2 BbgPolG hinsichtlich der Tatbestandsvoraussetzungen weiterentwickelt und neu strukturiert. Die Polizei kann durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen offen Personen beobachten und personenbezogene Daten erheben. Die Bild- und Tonüberwachung kann durch stationäre und mobile Anlagen erfolgen.

Tatbestandsvoraussetzung für solche Maßnahmen war nach der bisherigen Regelung aufgrund von Lageerkenntnissen das Vorliegen von Tatsachen, die die Annahme rechtfertigen, dass an diesen Orten vermehrt Straftaten drohen oder wenn sich diese an oder in besonders gefährdeten Objekten im Sinne des alten § 12 Absatz 1 Nummer 3 BbgPolG befinden.

Im Neuen Absatz 2 werden nunmehr in den Nummern 1 bis 5 die Tatbestandsvarianten systematisch und übersichtlich gegliedert:

- Abwehr einer konkreten Gefahr,
- an öffentlich zugänglichen Orten, bei denen Tatsachen die Annahme rechtfertigen, dass dort vermehrt Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung drohen,
- an den im neuen § 15 Absatz 1 Nummer 2 BbgPolG genannten öffentlich zugänglichen Orten,
- an oder in besonders gefährdeten öffentlich zugänglichen Objekten im Sinne des neuen § 15 Absatz 1 Nummer 3 BbgPolG oder in deren unmittelbarer Nähe oder
- zur Verhütung oder vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen, sofern diesbezüglich zumindest eine erhöhte abstrakte Gefahr besteht.

Zur Abwehr einer konkreten Gefahr können jetzt, durch die Nummer 1 ausdrücklich geregelt, (mobile) Aufnahmegeräte eingesetzt werden.

Nummer 2 entspricht der bisherigen Regelung der ersten Variante, erweitert um Ordnungswidrigkeiten von erheblicher Bedeutung. An diesen Orten muss mit einer erhöhten Kriminalitäts- oder Handlungsbelastung zu rechnen sein. Es dürfen nicht nur vereinzelt Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung drohen. Die Annahme eines Kriminalitäts- oder Handlungsschwerpunktes setzt voraus, dass sich die Kriminalitäts- oder Handlungsbelastung des Ortes deutlich von der an anderen Orten abhebt. Hierfür bedarf es einer Erforderlichkeitsprognose, in die Vergleichsorte einbezogen werden. Dies kann durch Lagebilder in nachvollziehbarer Weise dokumentiert werden.

Nummer 3 mit dem Verweis auf den neuen § 15 Absatz 1 Nummer 2 BbgPolG wird neu eingefügt.

Nummer 4 entspricht der bisherigen Regelung der zweiten Variante mit der Klarstellung, dass auch in unmittelbarer Nähe der Objekte Aufnahmen durchgeführt werden können. Orte und Objekte sind öffentlich zugänglich, wenn der Zutritt nicht auf einen namentlich oder individuell bestimmbar Personenkreis beschränkt, sondern einer unbestimmten Anzahl von Menschen gestattet ist.

Die Nummer 5 ermöglicht im Rahmen von kriminalpräventiven Handlungskonzepten und operativer Präventionsplanungen den gelockerten Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen bereits bei einer erhöhten abstrakten Gefahr zur Verhütung oder vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen. So können diese technischen Mittel zur selektiven Kriminalprävention beispielsweise im ländlichen Raum gegen Vieh- und Landmaschinen-diebstähle organisierter und transnationaler Tätergruppen eingesetzt werden. Dies gilt auch für die Bekämpfung von Wohnungseinbruchsdiebstählen auf Grundlage voraussetzender Analysen zu gefährdeten Bereichen. Die Vorschrift ermöglicht auch der Polizei durch den Einsatz (vorübergehend) stationärer Aufnahmegeräte potenzielle Ziele terroristischer Anschläge zu überwachen. Dadurch können Orte und Objekte geschützt werden, die keine Kriminalitätsschwerpunkte sind, aber für die ein erhöhtes abstraktes Gefahrenpotenzial im Hinblick auf solche Straftaten

oder terroristische Anschläge besteht. Dabei reicht es aus, sich auf Indizien zu stützen. Diese können beispielsweise auf Informationen von anderen Sicherheitsbehörden oder auf allgemein zugänglichen Informationen beruhen.

Im Fall des Anschlags auf dem Berliner Weihnachtsmarkt im Dezember des Jahres 2016 hatte es bereits vorher nachrichtendienstliche Informationen gegeben, dass Weihnachtsmärkte als weiche Anschlagssziele besonders gefährdet sind. Außerdem hatte der Islamische Staat in der zuvor im November veröffentlichten dritten Ausgabe seiner Zeitschrift „Rumiya“ eine ausführliche taktische Anweisung veröffentlicht, Lastkraftwagen als Waffe gegen die Bevölkerung einzusetzen. In dieser wurden ausführlich die Auswahl des Tatmittels, die Geeignetheit der Anschlagssziele sowie die Planung und Vorbereitungsmaßnahmen beschrieben. Insbesondere wurde darauf Wert gelegt, den Anschlagsort vorher aufzuklären. Solche Informationen ermöglichen es der Polizei im Rahmen der Präventionsplanung geeignete Orte für die Videoüberwachung auszuwählen, um Gefährder im Rahmen der Gefahrenvorsorge möglichst vor einem Anschlag beispielsweise bei Vorbereitungshandlungen zu identifizieren und ihre Straftat zu verhindern. Neben der Videoüberwachung können natürlich auch weitere präventive Maßnahmen durchgeführt werden, wie zum Beispiel die Sicherung bestimmter Angriffspunkte an einem Ort durch Hindernisse.

Absatz 3:

Der neue § 44 Absatz 3 BbgPolG übernimmt die Regelung des alten § 31a Absatz 1 BbgPolG mit einigen Modifikationen. Die Polizei kann im Rahmen der Erfüllung ihrer Aufgaben zum Zwecke der Eigensicherung oder des Schutzes Dritter gegen eine konkrete Gefahr durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen in Fahrzeugen der Polizei offen personenbezogene Daten erheben. Die „Erfüllung ihrer Aufgaben“ umfasst sowohl die Gefahrenabwehr als auch die Verfolgung von Straftaten oder Ordnungswidrigkeiten.

Absatz 4:

Der neue § 44 Absatz 4 BbgPolG ermöglicht es der Polizei sogenannte „Bodycams“ zu tragen und im Rahmen der Erfüllung ihrer Aufgaben offen personenbezogene Daten zu erheben. Die „Erfüllung ihrer Aufgaben“ umfasst sowohl die Gefahrenabwehr als auch die Verfolgung von Straftaten oder Ordnungswidrigkeiten. Der offene Einsatz ist deshalb von entscheidender Bedeutung, weil nur so eine deeskalierende Wirkung erzielt werden kann. Die Erwartung, dass die Maßnahme gerade auch präventiv wirkt, stützt sich auf Erfahrungen der hessischen Polizei. Diese konnte bei einem über einen Zeitraum von einem Jahr angelegten Pilotprojekt im Frankfurter Stadtteil Alt-Sachsenhausen einen Rückgang der Angriffe gegen Polizeibeamte feststellen – entgegen einer ansonsten generell steigenden Anzahl von Angriffen. Zudem wurden dort eine deutlich gestiegene Kooperationsbereitschaft der kontrollierten Personen und ausbleibende Solidarisierungseffekte durch Dritte beobachtet. Andere Bundesländer wie Bayern, Hessen, Baden-Württemberg, das Saarland und Nordrhein-Westfalen haben den Einsatz körpernah getragener Aufnahme- und Speichergeräte in ihren Polizeigesetzen geregelt. Bayern und Nordrhein-Westfalen bereits auch für die Verwendung in Wohnungen.

Der Einsatz ist an oder in öffentlich zugänglichen Orten oder Objekten zulässig (z. B. Straßen, Wege, Plätze, Ladenpassagen sowie Bereiche des Öffentlichen Personennahverkehrs). Eine anlasslose Aufzeichnung bei einer normalen Streifenförtigkeit erfolgt nicht. Voraussetzung des Einsatzes ist eine konkrete Gefahr. Es ist sicherzustellen, dass im Falle einer kurzfristigen technischen Erhebung, an die sich keine verlängerte Speicherung anschließt, die betroffenen personenbezogenen Daten unverzüglich gelöscht werden. Bei der kurzfristigen technischen Erfassung handelt es sich also um den Fall des sogenannten Pre-Recording. Dabei werden die Bild- und Tonsequenzen auf einem flüchtigen Speichermedium mit begrenzter Speicherkapazität abgelegt, welches grundsätzlich permanent überschrieben beziehungsweise bei Abschaltung des Geräts gelöscht wird und auf das kein isolierter Zugriff möglich ist.

Die Speicherung der erlangten Daten für eine Dauer von mehr als 90 Sekunden ist zulässig, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz von Polizeivollzugsbediensteten oder Dritten gegen eine erhebliche konkrete Gefahr erforderlich ist. Nur im Fall der aktiven Betätigung der Aufnahmetaste wird eine bestimmte vorgelagerte Zeitspanne von bis zu 90 Sekunden der verwertbaren Aufzeichnung hinzugefügt. Die Pre-Recording-Funktion erfüllt damit den Zweck, eine möglichst umfassende Dokumentation auch der unmittelbaren Vorgeschichte einer konkreten Konfliktsituation zu gewährleisten. Außerdem vermindert sie die Gefahr von Fehlaufnahmen, da die Polizeibeamten mehr Zeit für die Einschätzung haben, ob sich eine gefährliche Lage tatsächlich in der erwarteten Weise entwickelt. Mithin werden dadurch auch die Eingriffe in das Recht auf informationelle Selbstbestimmung der betroffenen Personen minimiert.

In Wohnungen dürfen diese Maßnahmen nur zur Abwehr einer dringenden konkreten Gefahr für Leib, Leben oder Freiheit einer Person erfolgen, sofern damit nicht die Überwachung der Wohnung verbunden ist. Hier darf zudem keine kurzfristige technische Erhebung ohne unverzügliche Fertigung verarbeitungsfähiger Aufzeichnungen erfolgen. Insoweit gilt es, einerseits einem besonderen Bedürfnis der polizeilichen Praxis, andererseits dem auch insoweit gültigen Maßstab des Artikels 13 Absatz 7 des Grundgesetzes beim Betreten von Wohnungen Rechnung zu tragen. Denn anders als beim verdeckten Einsatz von technischen Überwachungsmitteln in Wohnungen nach Artikeln 13 Absatz 4 oder 5 des Grundgesetzes durchbricht die offene Aufzeichnung in Gegenwart der Polizei den speziell geschützten Bereich nicht, sondern dokumentiert lediglich das Geschehen in dem durch die Polizeipräsenz bereits durchbrochenen Rahmen (vgl. Landtag Nordrhein-Westfalen, Drucksache 16/12361, zur Regelung in § 15c des Polizeigesetzes des Landes Nordrhein-Westfalen). Schranke für den Grundrechtseingriff ist ausschließlich Artikel 13 Absatz 7 des Grundgesetzes, der den Einsatz technischer Mittel nicht ausschließt (vgl. Landtag Nordrhein-Westfalen, Drucksache 16/13556). Selbstverständlich darf nicht die Überwachung der Wohnung, sondern ausschließlich die Abwehr einer dringenden Gefahr für Leben, Gesundheit oder Freiheit einer Person Ziel der Maßnahme sein. Von einer solchen polizeilichen Maßnahme werden nicht nur Polizeibeamte, sondern auch die in der Wohnung aufhaltigen Privatpersonen geschützt – wie etwa in Fällen häuslicher Gewalt. Darüber hinaus gelten die Regelungen des § 34 BbgPolG zum Berufsgeheimnisträger- und Kernbereichsschutz. Eines zusätzlichen Richtervorbehalts bedarf es angesichts der strengen Grundvoraussetzungen und der flankierenden Maßnahmen nicht. Denn in den denkbaren praktischen Anwendungsfällen liegt hier ohnehin regelmäßig Gefahr im Verzug vor, und gerade beim Einsatz in häuslichen Situati-

onen erfolgt die weitere Verwendung – wenn überhaupt – zu Strafverfahrenszwecken, die ohnehin umfassender richterlicher Kontrolle unterliegen.

Über die Anfertigung der technischen Aufnahmen oder Aufzeichnungen entscheidet der das Aufnahmegerät tragende Polizeivollzugsbedienstete anhand der konkreten Umstände des Einzelfalls.

Durch die Regelung des Absatzes 4 wird selbstverständlich der Einsatz der Systeme unter den anderweitigen Voraussetzungen und zu den Zwecken der Absätze 1 und 2 nicht ausgeschlossen.

Absatz 5:

Nach dem neuen § 44 Absatz 5 BbgPolG kann die Polizei eine in Gewahrsam genommene Person durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen offen beobachten und personenbezogene Daten erheben, soweit dies zu ihrem oder zum Schutz des zur Durchführung des Gewahrsams eingesetzten Personals oder zur Verhütung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung in polizeilich genutzten Räumen erforderlich ist. Diese Regelung zielt insbesondere darauf ab Unfälle, Eigenverletzungen und Suizidversuche insbesondere von betrunkenen, medikamenten- oder rauschgiftabhängigen Personen sowie Gewalttaten zu verhindern. Die Überwachung ist auf das absolut Notwendige zu beschränken.

Absatz 6:

Der neue § 44 Absatz 6 BbgPolG ermöglicht bei Maßnahmen nach den Absätzen 1 und 2 auf Anordnung der Behördenleitung und mit Zustimmung des für Inneres zuständigen Ministeriums die Verwendung von Systemen zur automatischen Erkennung und Auswertung von Mustern bezogen auf Personen und Gegenstände einschließlich der automatischen Systemsteuerung zu diesem Zweck, soweit dies die Gefahrenlage auf Grund entsprechender Erkenntnisse erfordert. Die Gefahrenlagen werden durch die Absätze 1 und 2 eingegrenzt.

Hierdurch wird eine Rechtsgrundlage für die intelligente Videoüberwachung geschaffen. Intelligente Videoüberwachungsanlagen haben Mustererkennungsfunktionen, wie die Erkennung von Gesichtern, die Analyse von Verhaltensmustern und das Verfolgen von Personen oder Objekten. Das Bild- und Tonmaterial wird in Echtzeit durch das System automatisiert ausgewertet. Es gibt eine dezentrale Lösung, bei der jede der Kameras speichern und analysieren kann. Die zentrale Lösung führt die Daten aller Kameras in einem Speicher zusammen, bevor die Analyse erfolgt. Neben dem Bild- und Tonspeicher gibt es noch einen Metadatenpeicher. Durch die Einstellung der Parameter und die zugrundeliegenden Algorithmen können die Funktionen der intelligenten Videoüberwachung verfeinert und an die Gefahrenlage („soweit“) angepasst werden.

Die durch die Bild- und Tonüberwachung erfassten Daten werden automatisiert durch einen selbstständig ablaufenden Datenverarbeitungsprozess ausgewertet. Das Bild- und Tonmaterial wird aufgearbeitet und dann auf Basis von Algorithmen eine bestimmte Person oder Objekt durch das sogenannte Trackingverfahren aufgespürt. Es wird durch Tracking-Algorithmen ein Bewegungsablauf erstellt. Durch Mustererkennung wird nach bestimmten optischen und akustischen Strukturen gesucht, die auf die Gefahrenvorsorge und -abwehr ausgerichtet sind. Die Person

oder das Objekt werden klassifiziert und gegebenenfalls identifiziert. Weitere Eigenschaften und Verhaltensmuster lassen sich unter Umständen feststellen. Verdächtige Personen oder Objekte können durch Fortbewegungserkennung verfolgt werden. Durch den Einsatz mehrerer Kameras kann die Observation von einem zum anderen Sektor weitergereicht werden. Das System löst schließlich einen Alarm aus und bereitet die Verdachtsinformationen auf, so dass der Polizeioperator das Bild- und Tonmaterial im Rahmen einer Kontrolle sichten, weiter analysieren und bewerten kann, um eine Einsatzentscheidung zu treffen. Das schnelle Erlangen von Informationen kann der Polizei einen zusätzlichen zeitlichen Spielraum für weitere Eingriffsmaßnahmen eröffnen.

Der Verwendung dieser Systeme muss eine operative Präventionsplanung auf Grundlage eines kriminalpräventiven Handlungskonzepts zugrunde liegen. Diese dienen der strategischen und operativen Ausrichtung der Maßnahmen sowie der Dokumentation im Hinblick auf die Selbstkontrolle der Polizei und etwaige Gerichtsverfahren. § 4 Absatz 2 bis 5 BbgPolG gilt entsprechend.

Die längerfristige Verwendung dieser Systeme für mehr als einen Monat ist durch ein Monitoring zu begleiten und jährlich zu evaluieren. Die Verwendung ist auf höchstens zwei Jahre zu befristen. Nach einem Bericht des für Inneres zuständigen Ministeriums an den Landtag und dessen für Inneres zuständigen Ausschuss sowie nach einer positiven auf Tatsachen beruhenden Einschätzung über die Verwendung solcher Systeme im konkreten Einzelfall kann die Maßnahme um jeweils längstens zwei Jahre verlängert werden. Dadurch wird die Polizei angehalten, das automatisierte Verfahren kritisch zu begleiten, auszuwerten und zu verbessern.

Absatz 7:

Der neue § 44 Absatz 7 BbgPolG legt fest, dass die Polizei bei Maßnahmen nach den Absätzen 1 bis 5 in geeigneter Weise auf die Bild- und Tonaufnahmen und -aufzeichnungen hinweist, soweit nicht Gefahr im Verzug besteht. Auf die Verwendung von Systemen im Sinne des Absatzes 6 ist dabei gesondert hinzuweisen. Auch beim Einsatz von Drohnen muss die Offenheit der Maßnahme gewahrt und auf die Verwendung von unbemannten Luftfahrtsystemen besonders hingewiesen werden.

Absatz 8:

Nach dem neuen § 44 Absatz 8 BbgPolG dürfen Maßnahmen nach den Absätzen 1 bis 6 auch dann durchgeführt werden, wenn Dritte unvermeidlich betroffen werden. Es dürfen also personenbezogene Daten über Dritte verarbeitet werden, soweit dies erforderlich ist, um eine Datenverarbeitung nach den Absätzen 1 bis 6 durchführen zu können.

Absatz 9:

Der neue § 44 Absatz 9 BbgPolG regelt die Löschungs- und Vernichtungsfristen. Dieser legt fest, dass Bild- und Tonaufnahmen oder -aufzeichnungen und daraus gefertigte Unterlagen spätestens einen Monat nach der Datenerhebung zu löschen oder zu vernichten sind, soweit diese nicht benötigt werden

- zur Verfolgung von Straftaten oder Ordnungswidrigkeiten,

- zur Überprüfung der Rechtmäßigkeit der polizeilichen Maßnahme, wenn eine solche Überprüfung zu erwarten steht, oder
- zum Zwecke der Benachrichtigung nach § 35 Absatz 1.

Die Löschung ist zu dokumentieren. § 58 Absatz 5 und 6 BbgPolG sowie § 67 Absatz 5 und 6 BbgPolG bleiben unberührt.

Die Monatsfrist wird einheitlich für alle Maßnahmen nach § 44 BbgPolG festgelegt. Für die Überwachung von Orten und Objekten galt nach der alten Regelung eine 48 Stundenfrist. Für die erhobenen Daten nach Absatz 4 gilt, dass diese spätestens nach 90 Sekunden automatisch zu löschen sind, sofern nicht zuvor die Voraussetzungen des Absatzes 4 Satz 2 vorliegen.

Verfassungsrechtliche Würdigung:

§ 44 BbgPolG ist verfassungsgemäß.

Gesetzgebungskompetenz:

Das Land Brandenburg hat für die Regelung des § 44 BbgPolG die Gesetzgebungskompetenz. Nach Artikel 70 Absatz 1 des Grundgesetzes verfügen die Länder über das Recht der Gesetzgebung, soweit die Gesetzgebungsbefugnis nicht dem Bund zugewiesen ist. Zu den Ländermaterien gehört unter anderem das Recht der Gefahrenabwehr. § 44 BbgPolG dient der Gefahrenabwehr und der Verhütung von Straftaten, Ordnungswidrigkeiten und von terroristischen Anschlägen. Zur Aufgabe der Gefahrenabwehr gehört auch die Gefahrenvorsorge, bei der bereits im Vorfeld konkreter Gefahren staatliche Aktivitäten entfaltet werden, um die Entstehung von Gefahren zu verhindern beziehungsweise eine wirksame Bekämpfung sich später realisierender, momentan aber noch nicht konkret drohender Gefahren zu ermöglichen. Die offene ausgewiesene Videoüberwachung soll potentielle Straftäter von der Begehung einer Straftat abschrecken und diese dadurch verhindern. Bild- und Tonaufzeichnungen erhöhen die Effektivität der Abschreckung, weil der potentielle Täter damit rechnen muss, dass seine Tat aufgezeichnet und die Aufzeichnung nicht nur für seine Identifizierung, sondern auch als Beweismittel in einem Strafverfahren zur Verfügung stehen wird. Die Vorschrift ermöglicht auch deshalb die Sicherung von Beweismaterial zur Strafverfolgung. Die Beobachtung ermöglicht es zudem den damit betrauten Beamten, sich anbahnende Gefahrenlagen, aus denen sich typischerweise Straftaten entwickeln können, rechtzeitig zu erkennen und Beamte vor Ort gezielt einzusetzen. Schließlich können auch wichtige Informationen zu in der Zukunft liegenden möglichen Straftaten gewonnen werden, wenn beispielsweise Gefährder bei der Aufklärung ihres Anschlagziels entdeckt werden. Es besteht dann die Möglichkeit durch weitergehende polizeiliche Maßnahmen gegen die Gefahr vorzugehen.

Die Strafverfolgungsvorsorge ist kompetenzmäßig dem „gerichtlichen Verfahren“ im Sinne des Artikel 74 Absatz 1 Nummer 1 des Grundgesetzes zuzuordnen, nämlich der Sicherung von Beweismitteln für ein künftiges Strafverfahren. Die Daten werden zu dem Zweck der Verfolgung einer in der Zukunft möglicherweise verwirklichten konkreten Straftat und damit letztlich nur zur möglichen Verwertung in einem künftigen Strafverfahren erhoben. Eine Verwertung der erhobenen Daten für diesen Zweck kommt erst in Betracht, wenn tatsächlich eine Straftat begangen wurde und daraus strafprozessuale Konsequenzen gezogen werden. Im Bereich

der konkurrierenden Gesetzgebung sind die Länder nach Artikel 72 Absatz 1 des Grundgesetzes von der Gesetzgebung ausgeschlossen, solange und soweit der Bund von seiner Gesetzgebungszuständigkeit Gebrauch gemacht hat. Inwieweit bundesgesetzliche Regelungen erschöpfend sind, kann nicht allgemein, sondern nur anhand der einschlägigen Bestimmungen und des jeweiligen Sachbereichs festgestellt werden. Die Regelungen des Bundes auf dem Gebiet der Strafverfolgungsvorsorge sind nicht so dicht, dass sie abschließend wirken. § 6 EGStPO erstreckt sich nicht auf die Strafverfolgungsvorsorge, denn es geht insoweit nicht um Maßnahmen, die vom Bestehen eines Anfangsverdachts einer Straftat abhängen. Dies ist anders zu sehen, soweit der Bundesgesetzgeber strafprozessuale Ermächtigungen zur Strafverfolgungsvorsorge geschaffen hat, wie beispielsweise in § 81b Alternative 2, § 81g und § 484 der Strafprozessordnung. Die davon erfassten Maßnahmen können nicht zugleich auf landespolizeigesetzliche Ermächtigungsgrundlagen gestützt werden. Ein Spielraum bleibt allenfalls für landesgesetzliche Zuständigkeitsregelungen. Der Bundesgesetzgeber hat aber keine allgemeine abschließende Regelung hinsichtlich der Strafverfolgungsvorsorge getroffen. So bestimmt denn auch § 484 Absatz 4 der Strafprozessordnung ausdrücklich, dass sich die Verwendung personenbezogener Daten, die für Zwecke künftiger Strafverfahren in Dateien der Polizei gespeichert sind oder werden, grundsätzlich nach den Polizeigesetzen richtet. Ausgenommen hiervon wird nur die Verwendung für Zwecke eines Strafverfahrens. Zu beachten ist zudem, dass selbst in Fällen, in denen der Bundesgesetzgeber polizeiliche Befugnisse auf dem Gebiet der Strafverfolgungsvorsorge normiert hat, dies nicht ausschließt, dass der Landesgesetzgeber entsprechende Befugnisse zum Zwecke der mit der Strafverfolgungsvorsorge häufig parallel laufenden Gefahrenvorsorge vorsieht.

Die Bildaufzeichnung berührt zwar in gewisser Weise den Regelungsbereich des § 81b Alternative 2 der Strafprozessordnung, der die Aufnahme von Lichtbildern eines Beschuldigten für Zwecke künftiger Strafverfolgung ermöglicht. Die Vorschrift regelt aber nicht abschließend, unter welchen Voraussetzungen Bilder für Zwecke künftiger Strafverfolgung angefertigt werden dürfen. Aus dem Regelungsinhalt des § 81b Alternative 2 der Strafprozessordnung tritt kein Wille des Bundesgesetzgebers hervor, landesrechtliche Regelungen auszuschließen, die nach dem Muster des § 44 BbgPolG gestaltet sind. Die Vorschrift ist primär auf die Gefahrenabwehr und die Verhütung von Straftaten ausgerichtet. Dasselbe gilt mit Blick auf § 100h und § 163f der Strafprozessordnung. Bei der Observation nach diesen Bestimmungen handelt es sich um eine verdeckte, auf bestimmte Zielpersonen fokussierte Ermittlungsmaßnahme, die im Hinblick auf ihr äußeres Gepräge, ihren Einsatzzweck und die grundrechtliche Betroffenheit der observierten Person bedeutsame Unterschiede zur offenen Beobachtung mittels Bild- und Tonübertragung oder -aufzeichnung im Rahmen der Gefahrenvorsorge aufweist. Durch die Einführung der automatisierten Auswertung wird zudem das Element der Gefahrenabwehr in dieser Vorschrift noch einmal gestärkt.

Bestimmtheitsgrundsatz:

Die Vorschrift des § 44 BbgPolG genügt dem verfassungsrechtlichen Gebot hinreichender Bestimmtheit. Beschränkungen von Grundrechten bedürfen einer verfassungsmäßigen gesetzlichen Grundlage, die dem verfassungsrechtlichen Gebot der Normenklarheit und dem Grundsatz der Verhältnismäßigkeit entsprechen muss. Die bestehende gesetzliche Grundlage wird durch diese Gesetzesänderung erweitert. Für die automatisierte Auswertung des Bild- und Tonmaterials wird nun eine gesetzliche Regelung geschaffen.

Das Bestimmtheitsgebot soll sicherstellen, dass der betroffene Bürger sich auf belastende Maßnahmen einstellen kann, dass die gesetzesausführende Verwaltung für ihr Verhalten steuernde und begrenzende Handlungsmaßstäbe vorfindet und dass die Gerichte die Rechtskontrolle durchführen können. Der Anlass, der Zweck und die Grenzen des Eingriffs müssen in der Ermächtigung bereichsspezifisch, präzise und normenklar festgelegt werden. Für Ermächtigungen zu Überwachungs- und Auswertungsmaßnahmen verlangt das Bestimmtheitsgebot zwar nicht, dass die konkrete Maßnahme für den Betroffenen vorhersehbar ist, wohl aber, dass die betroffene Person grundsätzlich erkennen kann, bei welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung oder automatisierten Auswertung verbunden ist. Da bei Maßnahmen zur Verhütung von Straftaten das Risiko einer Fehlprognose besonders hoch ist, sind bei entsprechenden Regelungen hohe Anforderungen an den Bestimmtheitsgrundsatz zu stellen. Ermächtigt eine gesetzliche Regelung zu einem Eingriff in das Grundrecht auf informationelle Selbstbestimmung, so hat das Gebot der Bestimmtheit und Klarheit auch die bereichsspezifische Funktion, eine Umgrenzung des Anlasses der Maßnahme und auch des möglichen Verwendungszwecks der betroffenen Information sicherzustellen. Ist der Zweck nicht festgelegt, entsteht das Risiko einer Nutzung der Daten für Zwecke, für die sie nicht erhoben wurden.

Die Norm des § 44 BbgPolG genügt auch diesen rechtsstaatlichen Bestimmtheitsanforderungen. Die Gefahrenabwehr, die Verhütung von Straftaten und die subsidiäre Vorsorge für die Verfolgung künftiger Straftaten sind legitime Ziele der Bild- und Tonüberwachung. Ebenfalls hinreichend bestimmt geregelt sind die Zwecke, für die die gewonnenen Daten künftig verwendet einschließlich der automatisierten Auswertung und weiter übermittelt werden dürfen, sowie die Voraussetzungen, die hierbei einzuhalten sind. Die verwendeten Begriffe können durch Rechtsprechung und Literatur ausgelegt werden, ohne dass dabei die bundes- und verfassungsrechtlichen Grenzen überschritten werden, die der Bestimmtheitsgrundsatz einer möglichen Auslegung zieht.

Grundrechtseingriff und Rechtfertigung:

Die Bild- und Tonüberwachung greift jedenfalls insoweit in das Recht auf informationelle Selbstbestimmung gemäß Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes, Artikel 11 Absatz 1 der Verfassung des Landes Brandenburg ein, als sie mittels Bild- und Tonaufzeichnung erfolgt. Dies wäre möglicherweise anders zu beurteilen, wenn die aufgezeichneten Bilder unmittelbar nach der Aufzeichnung – wie in Absatz 3 bei körpernah getragenen Aufnahme- und Speichergeräten geregelt – wieder gelöscht würden. Bei einer Bildübertragung (das sog. Kamera-Monitor-Prinzip) ist dies umstritten. Im Vergleich zur Aufzeichnung würde die einfache Übertragung aber regelmäßig einen Grundrechtseingriff von geringerer Intensität darstellen. Darüber hinaus kann das aufgezeichnete Bild- und Tonmaterial bis zu einem Monat lang aufbewahrt und automatisiert ausgewertet werden. Eine derartige Speicherung greift insbesondere dann in das Grundrecht auf informationelle Selbstbestimmung ein, wenn sie zur Vorbereitung von belastenden Maßnahmen gegen Personen dienen sollen. Die algorithmenbasierte Bild- und Tonanalyse ist rechtlich als automatisierte Datenverarbeitung zu werten und stellt deshalb einen zusätzlichen Grundrechtseingriff dar. Diese Maßnahmen greifen in das Recht auf informationelle Selbstbestimmung ein. Ob auch das Recht am eigenen Bild durch die Aufzeichnung betroffen ist, wird in der Literatur unterschiedlich beurteilt. Jedenfalls können auch Eingriffe in das Recht am ei-

genen Bild nach ähnlichen Maßgaben wie das informationelle Selbstbestimmungsrecht gerechtfertigt werden.

Da das Recht auf informationelle Selbstbestimmung nicht nur den Schutz der Privat- und Intimsphäre gewährleistet, sondern auch den informationellen Schutzinteressen desjenigen Rechnung trägt, der sich in die Öffentlichkeit begibt, entfällt der Eingriff in den Schutzbereich nicht dadurch, dass lediglich Daten über Verhaltensweisen im öffentlichen Raum erhoben und ausgewertet werden. Es ist nicht als eine den Eingriff ausschließende Einwilligung in die Informationserhebung und -auswertung zu werten, wenn sich die betroffenen Personen in den Erfassungsbereich der Videokameras begeben, obwohl sie aufgrund der Hinweise wissen, dass sie gefilmt und gegebenenfalls analysiert werden. Das Unterlassen eines ausdrücklichen Protests kann nicht mit einer Einverständniserklärung gleichgesetzt werden.

Das Grundrecht auf informationelle Selbstbestimmung wird jedoch nicht schrankenlos gewährleistet. Die beschränkende Vorschrift des § 44 BbgPolG wahrt den Verhältnismäßigkeitsgrundsatz. Dieser verlangt, dass ein Grundrechtseingriff einem legitimen Zweck dient und als Mittel zu diesem Zweck geeignet, erforderlich und angemessen ist (vgl. BVerwG, Urteil vom 25.01.2012 - 6 C 9.11).

Legitimer Zweck:

Die Bild- und Tonüberwachung sowie die automatisierte Auswertung dienen dem legitimen Zweck der Gefahrenabwehr, der Verhütung von Straftaten, Ordnungswidrigkeiten und von terroristischen Anschlägen. Darüber hinaus dient die automatisierte Auswertung der vorbeugenden Bekämpfung der Kriminalitätsphänomene der Grenzüberschreitenden, Organisierten, Politisch-motivierten einschließlich der terroristischen sowie der schwerwiegenden Wirtschafts- und Cyberkriminalität. Die damit beabsichtigte Gefahrenvorsorge gilt insbesondere dem Schutz von Personen und Sachen. Die Bild- und Tonüberwachung sowie die automatisierte Auswertung ermöglichen eine rasche Erkennung von Gefahrensituationen und daran anknüpfend den schnellen Einsatz von Polizeibeamten zur Abwehr der Gefahr. Das Bild- und Tonmaterial kann zudem wichtige Informationen enthalten, um zukünftige Straftaten und Anschläge abzuwenden. Die außerdem bezweckte subsidiäre Strafverfolgungsvorsorge ermöglicht die Aufbereitung von Beweismitteln für den Fall geschehener Rechtsverletzungen und deren Verwendung für die Strafverfolgung. Dies sichert den staatlichen Strafverfolgungsanspruch.

Geeignetheit:

Die Bild- und Tonüberwachung sowie die automatisierte Auswertung sind auch geeignete Mittel zur Erreichung der legitimen Ziele. Sie dient der selektiven Kriminalprävention. Neben der kriminalpräventiven Umweltgestaltung eignen sich die Maßnahmen mit der voranschreitenden technischen Entwicklung auch immer mehr für eine individuelle Kriminalprävention. Zum einen soll die Kriminalität durch ihre mittelbare Wirkung reduziert werden. Zum anderen ermöglichen sie andere hoheitliche Eingriffsmaßnahmen. Dabei steht die Interventionswirkung im Vordergrund, als das frühzeitige Erkennen von Gefahrenlagen insbesondere für Personen oder Sachen und das Abwenden von Schadensereignissen. Außerdem können durch die Aufnahmen bestimmte Gegenstände erfasst werden, die hoheitlich sichergestellt werden sollen. Dafür muss das Bild- und Tonmaterial fortlaufend ausgewertet werden und Einsatzkräfte vor Ort verfügbar sein, die schnell reagie-

ren können. Dies erfordert einen hohen Personalaufwand. Die Erzielung einer Interventionswirkung hängt also von räumlichen, technischen und organisatorischen Faktoren ab.

Die mittelbare kriminalpräventive Funktion der Bild- und Tonüberwachung ist weit- hin anerkannt. Sie wird jedoch von einigen bestritten. Jedenfalls hat die Überwachungsanlage den Zweck, auf das räumlich-soziale Umfeld einzuwirken und potentielle Straftäter von der Straftat abzuhalten. Darüber hinaus zeigt sie der Allgemeinheit, dass die Polizei erhöhte Sicherheitsmaßnahmen für den konkreten Ort ergriffen hat. Dies kann das Sicherheitsgefühl der Bürger stärken und ihre Aufmerksamkeit erhöhen. Diese Wirkung kann durch die Offenheit, die Ausnutzung bestimmter räumlicher und sozialer Kontexte sowie durch die technische und organisatorische Ausgestaltung der Anlage erzielt werden.

Der Bild- und Tonüberwachung sowie der automatisierten Auswertung liegen bei Einsätzen nach Absatz 1 regelmäßig ein Einsatzbefehl und eine entsprechende Einsatzplanung zugrunde, bei Absatz 2 eine Analyseplanung bzw. eine spezifische operative Präventionsplanung und ein kriminalpräventives Handlungskonzept. Dadurch wird eine operative und strategische Ausrichtung der Überwachungsmaßnahmen gewährleistet. Bei Maßnahmen nach Absatz 3 und Absatz 4 besteht bereits eine konkrete Gefahrenlage, in der schnelles polizeitaktisches Handeln gefragt ist und es weniger auf ein strategisches Planen ankommt. Darüber hinaus haben die Überwachungsanlagen eine Dokumentationswirkung, indem Geschehensabläufe am Überwachungsort aufgezeichnet werden. Das Bild- und Tonmaterial kann als Beweismittel neue Ermittlungsansätze eröffnen. Die Effektivität hängt vielfach von der Qualität der Bild- und Tonaufnahmegeräte ab.

Das Zusammenführen und automatisierte Auswerten des Bild- und Tonmaterials mit informationstechnischen Mitteln eröffnet mit fortschreitender technischer Entwicklung die Möglichkeit einer gezielten Überwachung. Durch das automatisierte Erkennen von Personen und Sachen sowie das Verfolgen ihrer Bewegungen können objekt- oder ereignisbezogene Analysen gefertigt werden, die die hergebrachte kriminalpräventive Funktion der Bild- und Tonüberwachung verstärken. Die Merkmale von Personen oder Objekten können mit dem polizeilichen Datenbestand abgeglichen werden. Es laufen bereits öffentlich finanzierte Forschungsprojekte zur intelligenten Videoüberwachung, um verschiedene Anwendungen zu entwickeln. Ziele sind beispielsweise das Erkennen von Gewalttaten in Menschenmengen, von bevorstehenden Suizidversuchen an Bahngleisen oder die Überwachung von besonders gefährlichen Straftätern und Gefährdern. Das effektive Aufdecken von Vorhaben gefährlicher Straftäter und Gefährder würde das Zusammenführen und automatisierte Auswerten der von ihnen erfassten Daten zahlreicher Überwachungsanlagen, eine Verkoppelung mit anderen Identifikations- und Analysesystemen und die Verwendung privater Datenbestände beispielsweise der sozialen Netzwerke erfordern. Intelligente Videoüberwachung verspricht also ein quantitativ und qualitativ gesteigertes Überwachungspotential, das eine effizientere und weniger personalintensive Überwachung, eine größere räumliche Abdeckung und die Aufdeckung verdächtiger Verhaltensmuster ermöglicht. Dadurch kann zeitnah in Kausalverläufe eingegriffen werden. Die Interventionswirkung wird durch intelligente Videoüberwachung verstärkt.

Erforderlichkeit:

Die erweiterten Befugnisse sind auch erforderlich. Insbesondere ist ein milderes, gleichermaßen wirksames Mittel als die erweiterte Bild- und Tonüberwachung des öffentlichen Raums und die automatisierte Auswertung zur Gefahrenabwehr und Gefahrenvorsorge nicht ersichtlich. Der stattdessen erwägenswerte größere Personaleinsatz der Polizei würde diese in anderen Bereichen weiter schwächen und stößt auch auf Finanzierungsgrenzen. Außerdem stockt das Land Brandenburg nur langsam die Anzahl der Polizisten aufgrund der begrenzten Ausbildungskapazitäten auf. Die technische Beschaffenheit der Kameras einschließlich Zoomfunktion und der erhöhten Perspektive verhilft darüber hinaus zu einer größeren Übersicht. Außerdem können größere Flächen beobachtet und die Polizeibeamten gezielter und effektiver eingesetzt werden. Dieses unterstützende Potential wird durch die intelligente Videoüberwachung noch verstärkt, insbesondere um den Faktor der Schnelligkeit.

Verhältnismäßigkeit:

Die Vorschrift des § 44 BbgPolG ist auch verhältnismäßig im engeren Sinne. Einbußen an grundrechtlich geschützter Freiheit dürfen nicht in unangemessenem Verhältnis zu den Zwecken stehen, denen die Grundrechtsbeschränkung dient. Gemeinschaftsbezogenheit und -gebundenheit der Person führen zwar dazu, dass der Einzelne Einschränkungen seiner Grundrechte hinzunehmen hat, wenn überwiegende Allgemeininteressen dies rechtfertigen. Der Gesetzgeber muss aber zwischen Allgemein- und Individualinteressen einen angemessenen Ausgleich herstellen. Dabei spielt auf grundrechtlicher Seite eine Rolle, unter welchen Voraussetzungen welche und wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind. Maßgebend sind also insbesondere die Gestaltung der Einschreitschwellen, die Zahl der betroffenen Personen und die Intensität der Beeinträchtigungen.

Die Videoüberwachung stellt einen erheblichen Grundrechtseingriff dar, insbesondere für Menschen, die aus persönlichen oder beruflichen Gründen gezwungen sind, sich dieser Beobachtung häufig auszusetzen. Die mit § 44 BbgPolG verfolgten Gesetzeszwecke der Gefahrenvorsorge und -abwehr sowie der subsidiären Strafverfolgungsvorsorge dienen jedoch in ebenso großem Maße nicht nur dem öffentlichen Interesse an der Sicherheit, sondern auch dem Individualrechtsschutz. Insbesondere sollen damit Eingriffe in hochwertige Rechtsgüter wie Leben und körperliche Unversehrtheit abgewehrt werden. Die Betroffenen trifft somit selbst die Schutzwirkung der Kameraüberwachung.

Das Recht auf informationelle Selbstbestimmung ist ein durch die Menschenwürde aufgeladenes Grundrecht. Die Vorschrift des § 44 BbgPolG verletzt aber nicht die Menschenwürde aus Artikel 1 Absatz 1 des Grundgesetzes, Artikel 7 Absatz 1 der Verfassung des Landes Brandenburg von den durch die Bild- und Tonüberwachung betroffenen Personen. Eine Überwachung der Intimsphäre wird durch die Vorschrift nicht erlaubt. Im Hinblick auf die Erstellung von Persönlichkeitsprofilen ist die Menschenwürde nur dann verletzt, wenn durch längerfristige Überwachung nahezu alle Bewegungen und Lebensäußerungen der betroffenen Person registriert und diese zur Grundlage eines solchen Profils werden können. Die offene Überwachung bestimmter Bereiche gemäß § 44 BbgPolG kann nicht ein solches Potential entfalten. Dies ist allenfalls im Zusammenwirken mit anderen Maßnahmen möglich und dann eine Frage des Einzelfalls, der gerichtlich überprüfbar ist. Schließlich wird auch kein flächendeckender Einsatz der Bild- und Tonüberwachung ermöglicht, weil die Norm auf Einzelveranstaltungen, -ansammlungen, -orte

und -objekte ausgerichtet ist, die bestimmte Eigenschaften oder Voraussetzungen erfüllen, also zumindest bei Zugrundelegung bestimmter Überwachungsziele ein erhöhtes abstraktes Gefahrenpotenzial aufweisen. Ebenso wenig stellt die biometrische Erfassung und Identifizierung per se eine Verletzung der Menschenwürde dar. Der durch sie ermittelbare Informationsgehalt ist für sich genommen geringer als bei der Identitätsfeststellung mittels Personalausweis. Gleiches gilt für die automatisierte Verhaltensanalyse und das Tracking als Observationsinstrument. Diese Mittel zur automatisierten Auswertung können ausnahmsweise im Einzelfall bei entsprechenden Einsatzmodalitäten und einer erheblichen Intensität die Menschenwürde verletzen. Dies ist gerichtlich feststellbar. Daraus folgt jedoch nicht, dass die Regelungen in § 44 BbgPolG gegen die Menschenwürde verstoßen. Der Überwachungsanlass muss zudem in verfassungskonformer Weise im Rahmen der Einsatzplanung bzw. operativen Präventionsplanung dokumentiert werden.

Die Vorschrift des § 44 BbgPolG zur Bild- und Tonüberwachung und zur automatisierten Auswertung ist darüber hinaus auch angemessen, weil die einzelnen Regelungen den jeweiligen Überwachungsanlass und die Auswertungsbefugnisse klar eingrenzen. Dies verhindert eine grenzenlose Ausdehnung der Überwachung im Land Brandenburg und somit ein andernfalls drohendes Übermaß an Überwachung. Gemildert wird in diesem Zusammenhang das Gewicht des staatlichen Eingriffs durch die Offenheit seiner Durchführung. Durch intelligente Videoüberwachung können zudem Dokumentationen erstellt werden, ohne dass das Bild- und Tonmaterial aufgezeichnet oder gespeichert werden muss. Nicht relevante Daten können sofort wieder automatisch gelöscht werden, ohne dass sie ein Mensch zu Gesicht bekommt oder diese ausgewertet werden. Für die Gefahrenvorsorge und -abwehr relevante Sachverhalte können herausgefiltert werden. Dadurch kann die Intensität und Streubreite von grundrechtsrelevanten Eingriffen verringert werden. Die verbleibenden Eingriffe fallen unter ein Verdachtsmuster und sind mithin nicht anlasslos. Durch die Speicherung des Bild- und Tonmaterials und die Identifizierung der betroffenen Personen steigt die Eingriffsintensität, insbesondere bei einem weitergehenden Datenabgleich oder einer Datenverknüpfung. Die konkreten Einsatzmodalitäten können im jeweiligen Einzelfall die Persönlichkeitsrelevanz steigern und zu einer höheren Einsatzschwelle führen, die gerichtlich überprüfbar ist. Der verfassungsgemäße Einsatz der Maßnahmen nach § 44 BbgPolG wird durch die Einsatzplanung bzw. die operative Präventionsplanung angeleitet, innerhalb derer gesteigerte organisatorische und verfahrensrechtliche Anforderungen zu berücksichtigen sind. Dies stärkt die Legitimation dieser Maßnahmen.

Schließlich müssen sich auch die konkreten Analyse Kriterien der automatisierten Auswertung an den Differenzierungsverboten des Artikels 3 des Grundgesetzes messen lassen. Eine weitergehende präventive oder repressive Nutzung kommt – über die zunächst erfolgende Beobachtung bzw. allgemeine Aufzeichnung hinaus – nur im echten Trefferfall in Betracht. Dies setzt eine entsprechende Verifizierung voraus. Bewegungsbilder entstehen allerdings bei einem automatisierten Tracking im Trefferfall zwangsläufig, sind jedoch auf den Erfassungsbereich des Systems begrenzt. Sollte sich später ein „unechter Treffer“ herausstellen, so ist dies auch insoweit – schon auf Grund des Übermaßverbotes – unverzüglich zu löschen. Näheres ist in der Systemeinsatzbeschreibung und der Errichtungsanordnung bzw. im Rahmen der Folgenabschätzung zu regeln, die der Einsatzplanung bzw. dem präventiven Handlungskonzept und der operativen Präventionsplanung zugrunde gelegt werden.

Die grundsätzliche Aufbewahrungsfrist von einem Monat nach der Datenerhebung genügt den Bearbeitungsanforderungen bei der Auswertung eines täglichen Datenvolumens von 24 Stunden Beobachtungszeit aus mehreren Kameras. Straftaten werden zum Teil erst verzögert angezeigt, so dass eine schnelle Löschung die Aufklärung des angezeigten Sachverhaltes unnötig erschweren würde. Sie belastet die einzelne Person in vertretbarem Maße, insbesondere weil diese regelmäßig nicht in individualisierter Weise mit den Aufnahmen festgehalten wird, sondern als Teil einer grundsätzlich anonymen Menge von Passanten oder Teilnehmern. Die Begrenzung der Aufbewahrungsfrist auf einen Monat verhindert ferner, dass eine Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbareren Zwecken entstehen kann. Für körpernah getragene Aufnahmegeräte gelten zudem restriktivere Vorgaben zur Speicherfrist und zur weiteren Verarbeitung der Daten. Die Möglichkeit einer zeitlich darüber hinaus gehenden Aufbewahrung zur Verfolgung von Straftaten und Ordnungswidrigkeiten sowie zur Gefahrenvorsorge ist auch verhältnismäßig. Das staatliche Verfolgungs- und Gefahrenabwehrinteresse überwiegt das Interesse der betroffenen Personen an der sofortigen Löschung des erhobenen Bild- und Tonmaterials. Außerdem kann durch intelligente Videoüberwachung die große Anzahl aufgezeichneter nicht relevanter Sachverhalte unverzüglich wieder gelöscht werden.

Zu § 45 (Elektronische Aufenthaltsüberwachung, Strafvorschrift)

Der neue § 45 BbgPolG ermöglicht auf Antrag der Behördenleitung und mit Zustimmung des für Inneres zuständigen Ministeriums die elektronische Aufenthaltsüberwachung einer Person zur Abwehr einer erheblichen konkreten Gefahr oder zur Verhütung oder vorbeugenden Bekämpfung von besonders schweren Straftaten oder schwerwiegenden Kriminalitätsphänomenen.

Es bedarf zwingend einer landesrechtlichen präventivpolizeilichen Regelung für die Anordnung einer (offenen) elektronischen Aufenthaltsüberwachung, um eine in zahlenmäßig größerem Maße personell nicht zu leistende konventionelle Dauerüberwachung von besonders gefährlichen Personen gewährleisten zu können. Als Adressat einer solchen Maßnahme kommen Personen in Betracht, die aktuell noch nicht straffällig oder trotz Verbüßung ihrer Strafe, ggf. einschließlich Maßnahmen der Führungsaufsicht, noch immer akut gefährdend erscheinen. Die elektronische Aufenthaltsüberwachung ist zudem auch eine adäquate Alternative zur Verhängung einer unter noch strengeren Voraussetzungen stehenden präventiven Ingewahrsamnahme. Die konkreten Bestimmungen in § 45 BbgPolG orientieren sich unbeschadet des grundlegend anderen, weil präventivpolizeilichen Ansatzes soweit möglich gerade in verfahrensmäßiger Hinsicht an den Regelungen in § 68b des Strafgesetzbuches und § 463a der Strafprozessordnung.

In Absatz 1 wird die Grundanordnung des Anbringens und betriebsbereiten Tragens einer „Fußfessel“ ähnlich wie in § 68b Abs. 1 Satz 1 Nr. 12 StGB geregelt. Die Maßnahme wird auf den Schutz wichtiger Rechtsgüter, die Verhinderung besonders schwerer Straftaten und die vorbeugende Bekämpfung von schwerwiegenden Kriminalitätsphänomenen beschränkt. Außerdem wird eine Verbindung zu Aufenthaltsge- und verboten bzw. Kontaktverboten nach § 20 Absatz 2 BbgPolG hergestellt. Derartige Aufenthaltsbestimmungen, aber auch schlichte Meldeaufgaben können Teil einer Anordnung der elektronischen Aufenthaltsüberwachung sein, müssen es aber nicht.

Absatz 2 regelt die elektronische Verarbeitungsbefugnis der Polizei einschließlich der Erstellung von Bewegungsbildern. In diesem Zusammenhang sind die Vorgaben des neuen § 38 BbgPolG zu beachten. Gerade wenn der Polizei die Möglichkeit zur Verfügung steht, die Aufenthaltsorte gefährlicher Personen zu einem Bewegungsbild zu verbinden, entfaltet die Maßnahme der elektronischen Aufenthaltsüberwachung ihre präventive Zielsetzung besonders, da hiermit ein erhebliches Potential zur Aufdeckung terroristischer oder sonst extremistischer Strukturen entsteht. Soweit es technisch möglich ist, ist sicherzustellen, dass innerhalb der Wohnung der verantwortlichen Person keine über den Umstand ihrer Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden.

Absatz 3 sieht aufgrund der Eingriffstiefe der Maßnahme einen Richtervorbehalt mit Eilfallkompetenz der Behördenleitung für Anordnungen der elektronischen Aufenthaltsüberwachung vor. Ferner werden darin das Verfahren und die Befristung derartiger Maßnahmen auf höchstens drei Monate einschließlich Verlängerungsmöglichkeit um jeweils bis zu drei Monate näher bestimmt. Der Inhalt der Anordnung wird näher bestimmt.

Absatz 4 sieht die Löschung der erhobenen Daten spätestens einen Monat nach Beendigung der Maßnahme vor, soweit die Daten nicht für zulässige anderweitige Zwecke verarbeitet werden. Die Löschung ist zu protokollieren.

Absatz 5 sieht eine Freiheitsstrafe von bis zu zwei Jahren oder eine Geldstrafe vor, wenn eine vorsätzliche Zuwiderhandlung bezüglich einer gerichtlichen Anordnung nach den Absätzen 1 und 3 begangen und dadurch ständig oder wiederholt die Feststellung des Aufenthaltsorts durch die Polizei verhindert wurde. Die Tat wird nur auf Antrag der Behördenleitung verfolgt. Die Vorschrift ist an § 145a des Strafgesetzbuchs sowie die bundesrechtliche Eingriffsnorm in § 87 BKAG angelehnt.

Der Bund besitzt nach Artikel 74 Absatz 1 Nummer 1 des Grundgesetzes die konkurrierende Gesetzgebungskompetenz für das Strafrecht. Die Länder haben jedoch eine Regelungsbefugnis für strafrechtliche Tatbestände (vgl. Art. 2 ff. EGStGB). Nach Artikel 72 Absatz 1 des Grundgesetzes gilt nur solange und soweit der Bund von seiner Gesetzgebungszuständigkeit nicht durch Gesetz Gebrauch gemacht hat oder dieses willentlich unterlässt. Mit § 87 BKAG hat der Bundesgesetzgeber jedoch nur eine Regelung zur Ahndung von Verstößen gegen bestimmte Maßnahmen nach dem BKAG getroffen. Eine gegenteilige Annahme ergibt sich weder aus dem Wortlaut noch der Gesetzesbegründung. Der Bundesminister des Innern hat wiederholt darauf hingewiesen, dass die Regelung in § 87 BKAG nur wenige Gefährder umfasse, weil die meisten dieser Personen nach Landesrecht überwacht würden (vgl. Pressemitteilung vom 01.02.2017). Deswegen sähe er diese Regelung des BKAG auch als dringende Anregung und Aufforderung an die Länder an, in ihren Polizeigesetzen ähnliche Regelungen vorzunehmen, da sie sonst ins Leere liefen. Im Ergebnis hat der Bund deshalb mit der Regelung in § 87 BKAG keine abschließende Regelung im Sinne des Artikels 72 Absatz 1 des Grundgesetzes getroffen.

Zu § 46 (Postsicherstellung)

Mit der neuen Regelung des § 46 BbgPolG wird unter strengen Voraussetzungen die Möglichkeit einer grundsätzlich richterlich angeordneten und überwachten präventivpolizeilichen Postsicherstellung eingeführt. Zudem wird ein Auskunftsrecht

gegenüber Postdienstleistern begründet. Die Vorschrift lehnt sich an den § 50 BKAG sowie an die §§ 99, 100 der Strafprozessordnung an. Zwar wird heutzutage viel über elektronische Medien, vor allem über das Internet kommuniziert und auch Güter über den Internet-Versandhandel geordert. Dennoch werden gerade auch konventionelle Postmedien (Briefe, Paketsendungen und ggf. auch Telegramme) nach wie vor zur konspirativen Kommunikation genutzt – insbesondere dann, wenn eine betroffene Person mit der technischen Überwachung ihrer übrigen Kommunikationsmittel rechnen muss. Gerade bei verdeckten Bestellungen über das sogenannte Darknet erfolgt die Lieferung zum Empfänger in vielen Fällen über den Postweg. Dies wurde sicher auch durch die Verbreitung der sogenannten Packstationen verstärkt, die eine Abholung und Abgabe von Sendungen zu jeder Tages- und Nachtzeit und damit auch weitgehend unerkannt ermöglichen, insbesondere wenn die zugehörigen Karten missbräuchlich unter Verwendung falscher Personalien erlangt wurden. Ferner kann es im Zuge bestimmter Überwachungsmaßnahmen auch im Übrigen präventivpolizeilich erforderlich sein, neben Telekommunikation auch den konventionellen Postverkehr zu überwachen.

Auf Grund des hohen Guts des Brief- und Postgeheimnisses (Artikel 10 Absatz 1 und Absatz 2 Satz 1 des Grundgesetzes) kommt eine Postsicherstellung nach Absatz 1 Satz 1 nur zur Abwehr einer erheblichen konkreten Gefahr, zur Verhinderung besonders schwerer Straftaten und zur Bekämpfung von schwerwiegenden Kriminalitätsphänomenen in Betracht. Neben den nach Nummern 1 und 2 verantwortlichen Personen werden auch Nachrichtenmittler nach Nummer 3 erfasst, die mutmaßlich in Zusammenhang mit der Gefahren- oder Kriminalitätslage stehen. Zudem muss die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert sein. Antragssteller ist die Behördenleitung mit Zustimmung des für Inneres zuständigen Ministeriums.

Satz 2 regelt die Auskunfts- und Mitwirkungspflicht der geschäftsmäßigen Post- oder Telekommunikationsdienstleister. Im Hinblick auf die Regelung des § 39 Absatz 3 Satz 3 des Postgesetzes ist eine ausdrückliche Regelung im Polizeigesetz vorzugswürdig. In Satz 2 wird zugleich die Verpflichtung zur Erteilung bestimmter Auskünfte über im Gewahrsam der Postdienstleister befindliche oder befundene bzw. über angekündigte Postsendungen geregelt. Ohne derartige Auskünfte dürfte oftmals das Erfordernis einer anschließenden oder einer weiteren Postsicherstellung nicht ausreichend zu klären sein.

Um der Bedeutung und dem Gewicht des Grundrechtseingriffs der Maßnahme Rechnung zu tragen sieht Absatz 2 einen grundsätzlichen Richtervorbehalt für die Anordnung einer Postsicherstellung vor, ergänzt durch eine Eilfallregelung, die eine Anordnung durch die Behördenleitung vorsieht. Außerdem werden Inhalt und Frist für die richterliche Anordnung (höchstens ein Monat, jeweils entsprechend verlängerbar) geregelt.

In Absatz 3 wird bestimmt, dass die Öffnung der Sendungen grundsätzlich nur durch das zuständige Amtsgericht erfolgt, wobei diese Kompetenz widerruflich der Polizei übertragen werden kann, wenn bei Gefahr im Verzug Gründe der Dringlichkeit dies erfordern. Bestehen Zweifel hinsichtlich der Verwertbarkeit der erlangten Erkenntnisse, hat die Entscheidung hierüber im Benehmen mit der oder dem Landesbeauftragten zu erfolgen.

Absatz 4 regelt schließlich die Weiterleitung von Sendungen an den Empfänger. Eine solche hat unverzüglich zu erfolgen, soweit die Öffnung nicht angeordnet

wurde oder nach einer Öffnung der Sendungen die Zurückbehaltung der gesamten Sendung oder eines Teils der Postsendung zu Gefahrenabwehrzwecken nicht mehr erforderlich ist.

Zu § 47 (Einsatz besonderer Mittel der Datenerhebung)

Im neuen § 47 BbgPolG werden die alten §§ 32 und 33 BbgPolG zusammengefasst. Absatz 1 legt die besonderen Mittel der Datenerhebung fest, zum einen die längerfristige und kurzfristige Observation und zum anderen den Einsatz technischer Mittel für Bild- und Tonaufnahmen und -aufzeichnungen außerhalb von Wohnungen sowie zur Feststellung des Standortes oder der Bewegungen einer Person oder einer beweglichen Sache. Die Dauer der kurzfristigen Observation wird angemessen auf 72 Stunden und maximal vier Tage erweitert. Observationen stellen ein wirksames Mittel dar, um im Rahmen der Verhütung und vorbeugenden Bekämpfung von Straftaten und Kriminalitätsphänomenen mögliche Tatvorbereitungshandlungen zu erkennen, Kriminalitätsstrukturen auszuleuchten und entstehende Gefahren zu verhindern. Die Erweiterung versetzt die Polizei in die Lage, Observationsmaßnahmen insbesondere über das Wochenende, aber auch über Feiertage eigenständig durchgängig durchzuführen und Informationsbrüche zu reduzieren. Die Erweiterung auf unterbrochene, jedoch an nicht mehr als vier Tagen vorgesehene oder tatsächlich durchgeführte und planmäßig angelegte Beobachtungen ist eine Folgeänderung, da eine durchgehende Beobachtung über zweiundsiebzig Stunden sich bereits über mindestens drei Tage erstrecken muss. Weiterhin wird die Verwendung von Systemen zur automatischen Erkennung und Auswertung von Mustern im Sinne des § 44 Absatz 6 und zum automatischen Datenabgleich ermöglicht.

Absatz 2 regelt einheitlich die Voraussetzungen für die Datenerhebung unter Verwendung der besonderen Mittel des Absatzes 1. Hierfür muss eine erhebliche konkrete Gefahr oder die Verhütung oder vorbeugende Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen vorliegen. Betroffene Personen können Verantwortliche für eine Gefahren- oder Kriminalitätslage sein. Damit im Zusammenhang stehende Kontakt- und Begleitpersonen oder notstandspflichtige Dritte werden auch erfasst. Diese besonderen Mittel der Datenerhebung kommen nur in Betracht, wenn die polizeiliche Aufgabenerfüllung auf andere Weise gefährdet oder wesentlich erschwert würde. Dabei dürfen auch personenbezogene Daten über andere Personen erhoben werden, soweit dies erforderlich ist, um eine Datenerhebung durchführen zu können, es sei denn, es handelt sich um Berufsgeheimnisträger gemäß §§ 53, 53a der Strafprozessordnung, zu denen ein Vertrauensverhältnis besteht. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34 BbgPolG. Die Benachrichtigung der betroffenen Person erfolgt nach § 35 BbgPolG. Bei dem Einsatz von Mitteln nach Absatz 1 Nummer 2 Buchstabe c gilt, soweit dieser nicht ausschließlich zum Schutz der bei einem polizeilichen Einsatz tätigen Personen erfolgt, § 45 Absatz 2 Satz 2 und 3 sowie Absatz 3 Satz 2 BbgPolG entsprechend.

In Absatz 3 werden auf Grund der Feststellungen des Bundesverfassungsgerichtes im BKAG-Urteil Richtervorbehalte für längerfristige Observationen und für bestimmte Fälle des Einsatzes technischer Mittel festgeschrieben. Außerdem ist eine entsprechende Eilfallkompetenz der Behördenleitung vorgesehen. Nicht zu beanstanden ist, dass für die Anfertigung von Bildaufnahmen sowie für nur kurzfristige Observationen – auch mittels Bildaufzeichnungen oder technischer Mittel wie Peil-

sender – ein Richtervorbehalt nicht vorgesehen ist. Bleiben die Überwachungsmaßnahmen in dieser Weise begrenzt, haben sie kein so großes Eingriffsgewicht, dass deren Anordnung durch eine Richterin oder einen Richter verfassungsrechtlich geboten ist. Demgegenüber ist eine unabhängige Kontrolle verfassungsrechtlich aber unverzichtbar, wenn Observationen längerfristig – zumal unter Anfertigung von Bildaufzeichnungen oder unter Nutzung besonderer technischer Mittel wie Peilsender – durchgeführt oder wenn nichtöffentliche Gespräche erfasst werden. Diese Maßnahmen dringen unter Umständen so tief in die Privatsphäre ein, dass deren Anordnung einer unabhängigen Instanz, etwa einem Gericht, vorbehalten bleiben muss. Insoweit reicht es nicht, die Anordnung der Maßnahmen zunächst der Sicherheitsbehörde selbst zu überlassen. Vom Richtervorbehalt wird daher der Einsatz besonderer Mittel nach Absatz 2 in Verbindung mit Absatz 1 Nummer 1 Buchstabe a oder Nummer 2 Buchstabe a oder Buchstabe b oder c erfasst. Für Nummer 2 Buchstabe b oder c gilt der Richtervorbehalt jedoch nur, soweit durchgehend länger als zweiundsiebzig Stunden oder an mehr als vier Tagen Bild-, Standort- oder Bewegungsaufzeichnungen bestimmter Personen angefertigt werden sollen. Im Übrigen können diese Maßnahmen durch die Behördenleitung angeordnet werden. Die Maßnahme ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Anordnungsvoraussetzungen fortbestehen. Sobald diese weggefallen sind, ist die Maßnahme unverzüglich zu beenden und das anordnende Gericht davon zu unterrichten.

Absatz 4 regelt die Voraussetzungen für eine kurzfristige Observation nach Absatz 1 Nummer 1 Buchstabe b. Durch diese kann die Polizei personenbezogene Daten über die in den §§ 7 und 8 BbgPolG genannten und über andere Personen nur erheben, wenn dies zum Zwecke der Gefahrenabwehr (§ 1 Absatz 1 BbgPolG) erforderlich ist und andernfalls die Erfüllung der polizeilichen Aufgaben gefährdet oder wesentlich erschwert würde. Wegen der immer noch verhältnismäßig kurzen Dauer einer kurzfristigen Observation ist eine Anordnung durch die Behördenleitung oder gar ein Gericht nicht erforderlich.

Zu § 48 (Einsatz technischer Mittel zur Überwachung von Wohnungen)

Der neue § 48 BbgPolG übernimmt weitgehend den alten § 33a BbgPolG. In Absatz 1 wird klargestellt, dass auch Systeme zur automatischen Steuerung verwendet werden können. Der Straftatenkatalog der alten Nummer 2 wird in der neuen Nummer 2 durch den Begriff der besonders schweren Straftaten, der im neuen § 3 BbgPolG definiert ist, erfasst. Die Nummer 2 stellt eine Konkretisierung der dringenden konkreten Gefahr dar. Außerdem werden nunmehr nicht nur die Begehung, sondern auch die Veranlassung und Unterstützung dieser Straftaten erfasst.

Absatz 2 legt den Kreis der betroffenen Personen bestimmter und klarer strukturiert als zuvor fest. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden, es sei denn, es handelt sich um Berufsgeheimnisträger gemäß §§ 53, 53a der Strafprozessordnung, zu denen ein Vertrauensverhältnis besteht. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34 BbgPolG. Die Benachrichtigung der betroffenen Person erfolgt nach § 35 BbgPolG.

Im Übrigen erfolgen kleinere Anpassungen sowie die Aufhebung der Absätze 3, 5, 6, 7 und 9 des alten § 33a BbgPolG, die von den allgemeinen Vorschriften im neuen Unterabschnitt 1 des Kapitels 2 Abschnitt 2 erfasst werden.

Zu § 49 (Eingriffe in die Telekommunikation und in informationstechnische Systeme, Verkehrs- und Nutzungsdatenauskunft)

Absatz 1:

Durch den neuen § 49 wird die Vorschrift des alten § 33b BbgPolG weiterentwickelt. Die Eingriffe in die Telekommunikation erhalten in Absatz 1 eigene Tatbestandsvoraussetzungen, weil sich im Hinblick auf den Einsatz technischer Mittel zur Überwachung von Wohnungen die grundrechtlichen Eingriffe bei der Telekommunikationsüberwachung insbesondere bezüglich des Artikels 13 des Grundgesetzes unterscheiden. Tatbestandsvoraussetzungen sind nunmehr eine erhebliche konkrete Gefahr oder die Verhütung oder vorbeugende Bekämpfung von besonders schweren Straftaten oder von schwerwiegenden Kriminalitätsphänomenen. Betroffene Personengruppen sind die für eine Gefahren- oder Kriminalitätslage verantwortlichen Personen oder notstandspflichtigen Personen sowie Kontakt- oder Begleitpersonen. Außerdem muss die Erfüllung der polizeilichen Aufgaben gefährdet oder wesentlich erschwert sein. Unter Kontakt- und Begleitpersonen fallen auch solche Personen, die nicht aktiv an der Telekommunikation mitwirken, aber deren Kommunikationssysteme zur Abwicklung benutzt werden, wenn diese mutmaßlich in Zusammenhang mit der Gefahren- oder Kriminalitätslage stehen.

Weiterhin wird klargestellt, dass auch visualisierte Darstellungen der Telekommunikation ausgeleitet und erhoben werden dürfen. Außerdem wird nun praxisbezogen gesetzlich berücksichtigt, dass die laufende Kommunikation auch unter Verwendung von Systemen, die von dem von betroffenen Personen physisch benutzen Kommunikationssystem entfernt sind (etwa entsprechende Server bei IP-basierter Telekommunikation), erfolgt, auf die sich im Rahmen der Möglichkeiten im Einzelfall ebenfalls eine Maßnahme der Telekommunikationsüberwachung erstrecken darf. Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.

Absatz 2:

Absatz 2 regelt die Eingriffe in informationstechnische Systeme durch den verdeckten Einsatz technischer Mittel unter den entsprechenden Voraussetzungen für die Telekommunikationsüberwachung, um die Durchführung von Maßnahmen nach Absatz 1 zu ermöglichen oder zu unterstützen, Zugangsdaten und gespeicherte Daten zu erheben, solche Daten zu löschen oder zu verändern oder sonstige Eingriffe vorzunehmen. Tatbestandsvoraussetzungen nach Absatz 1 Satz 1 sind eine erhebliche konkrete Gefahr oder die Verhütung oder vorbeugende Bekämpfung von besonders schweren Straftaten oder von schwerwiegenden Kriminalitätsphänomenen. Betroffene Personengruppen sind die für eine Gefahren- oder Kriminalitätslage verantwortlichen Personen oder notstandspflichtigen Personen sowie Kontakt- oder Begleitpersonen. Außerdem muss die Erfüllung der polizeilichen Aufgaben gefährdet oder wesentlich erschwert sein. Absatz 1 Satz 2 bis 4 gilt entsprechend. Vorgenommene Eingriffe nach Absatz 2 Satz 1 sind, soweit technisch möglich, automatisiert rückgängig zu machen, wenn die Maßnahme beendet wird.

Die Eingriffe in informationstechnische Systeme dienen zum einen der Durchführung der Telekommunikationsüberwachung (Quellen-Telekommunikationsüberwachung). Viele Kommunikationsprogramme nutzen eine Verschlüsselung ihrer Kommunikationsdaten und -inhalte, die ohne aktives Handeln des Nutzers im Hin-

tergrund arbeitet. Telekommunikationsinhalte in verschlüsselter Form können in vielen Fällen durch die klassische Form der Telekommunikationsüberwachung nicht ausgewertet werden. Dies lässt die Maßnahmen der einfachen Telekommunikationsüberwachung bei der Abwehr von erheblichen konkreten Gefahren oder der Verhütung oder vorbeugenden Bekämpfung von besonders schweren Straftaten oder von schwerwiegenden Kriminalitätsphänomenen ins Leere laufen. Insbesondere für die Bekämpfung von Organisierter Kriminalität und terroristischer Straftaten ist daher die Form der Telekommunikationsüberwachung mittels Eingriffen in informationstechnische Systeme unerlässlich. Durch Eingriffe in informationstechnische Systeme kann die Kommunikation erfasst werden, bevor diese verschlüsselt wird oder nachdem diese entschlüsselt wurde, oder die Entschlüsselung ermöglichen. Es werden keine Informationen erlangt, die nicht auch durch eine „konventionelle“ Telekommunikationsüberwachung (z. B. Gesprächs- bzw. Chatprotokolle) erlangt würden. Die jeweilige Software wird erst nach einem umfangreichen Testverfahren und Feststellung der Konformität mit den rechtlichen Vorgaben sowie der „Standardisierenden Leistungsbeschreibung“ zum Einsatz freigegeben und in Abhängigkeit von der operativen Bedarfslage kontinuierlich weiterentwickelt.

Eingriffe in informationstechnische Systeme haben aber auch einen eigenen Anwendungsbereich (Online-Durchsuchung). Jenseits der Überwachung laufender verschlüsselter Telekommunikation stellt die Verschlüsselung von Daten seitens der Straftäter und der Kriminalität (z. B. bei Verschlüsselung eines Bereichs der Festplatte eines Computers oder einer externen Festplatte) die Sicherheitsbehörden zunehmend vor technische Herausforderungen. Um im Einzelfall verschlüsselte Daten als Spurenansätze zur Gefahrenabwehr auswerten zu können, ist die Online-Durchsuchung ein geeignetes Aufklärungsinstrument. Sie ermöglicht es den Gefahrenabwehrbehörden, aus den Systemen einer betroffenen Person im Rahmen der gesetzlichen Möglichkeiten gefahrenabwehrerhebliche Daten auszuweisen. Eingriffe in informationstechnische Systeme bieten aber auch die Möglichkeit durch das Löschen oder Verändern von Daten oder durch sonstige Eingriffe in informationstechnische Systeme auf Straftäter und Kriminalität zur Gefahrenabwehr einzuwirken. Sonstige Eingriffe sind beispielsweise die Unterbrechung, Verhinderung oder sonstige Störung der Verwendung informationstechnischer Systeme. Diese Maßnahmen können unter anderem zur aktiven Abwehr von Hackerangriffen oder gegen elektronische Geräte bei Terrorangriffen eingesetzt werden. Die Abwägung im Rahmen der Verhältnismäßigkeitsprüfung gebietet es der Polizei, das erforderliche Mittel auszuwählen. Das Löschen oder Verändern von Daten stellt in der Regel wohl einen schwereren Grundrechtseingriff als die Datenerhebung dar. Der Einsatz des jeweiligen Mittels hängt von den Umständen im Einzelfall ab.

Absatz 3:

Absatz 3 wird auf Eingriffe in informationstechnische Systeme ausgeweitet und um die technisch offene Variante der Störung in anderer geeigneter Weise erweitert.

Absatz 4:

Absatz 4 regelt den Richtervorbehalt für die Absätze 1 bis 3, einschließlich der Eilfallkompetenz der Behördenleitung. Die Befristung wird variiert im Falle des Absatz 3 Nummer 2 höchstens zwei Wochen, im Falle des Absatz 2 Satz 1 Nummer

4 oder Absatz 3 Nummer 3 höchstens drei Tage und in allen anderen Fällen höchstens einen Monat.

Absatz 5:

Absatz 5 regelt die Verkehrs- und Nutzungsdatenauskunft der telediensteanbietenden Personen unter den Tatbestandsvoraussetzungen des Absatzes 1 Satz 1. Die Beispielsaufzählungen zur Gefahr im Verzug werden um eine neue Variante nämlich der „Abwehr einer dringenden konkreten Gefahr“ erweitert.

Absatz 6:

Absatz 6 übernimmt die Regelung des alten Absatzes 7 zur Ermöglichung der Überwachungsmaßnahmen der Polizei durch telediensteanbietende Personen.

Absatz 7:

Absatz 7 regelt die Betroffenheit Dritter und Berufsgeheimnisträger. Die Daten Dritter sind nach Beendigung der Maßnahme unverzüglich zu löschen. Die Löschung ist zu dokumentieren. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34 BbgPolG. Die Benachrichtigung der betroffenen Person erfolgt nach § 35 BbgPolG.

Absatz 8:

Absatz 8 umfasst eine besondere Kennzeichnungs-, Datenschutz- und Protokollierungspflicht. Die Protokolldaten dürfen nur verwendet werden, um einer betroffenen Person, einer dazu befugten öffentlichen Stelle oder einem Gericht die Prüfung zu ermöglichen.

Absatz 9:

Absatz 9 enthält eine Sonderregelung zur Zweckänderung der nach den Absätzen 1, 2, 3 und 5 erlangten personenbezogenen Daten zur Gefahrenabwehr nach Absatz 1 Nummer 1 bis 3 oder für die Verfolgung von Straftaten von erheblicher Bedeutung.

Absatz 10:

Absatz 10 regelt ein Verwendungsverbot einschließlich der Ausnahmen, die Sperrung und die Löschung von personenbezogenen Daten.

Verfassungsmäßigkeit:

Die Regelungen zum Eingriff in die Telekommunikation und in informationstechnische Systeme sind verfassungsmäßig.

Bestimmtheitsgebot:

Die Regelungen sind hinreichend bestimmt. Das rechtsstaatliche Bestimmtheitsgebot verlangt, dass Gesetze so bestimmt sind, dass der Bürger erkennen kann, ob und inwiefern er von staatlichen Maßnahmen betroffen ist. Bei Eingriffsermächtigungen müssen insbesondere Tatbestand und Rechtsfolge klar formuliert sein. Je intensiver Eingriffe in ein Grundrecht sind, desto bestimmter muss die zu Ein-

griffen ermächtigende gesetzliche Grundlage sein. Die Regelungen werden auf bedeutsame Rechtsgüter, besonders schwere Straftaten und schwerwiegende Kriminalitätsphänomene beschränkt. Dem Gesetzgeber bleibt es auch unbenommen, solche Regelungen technikoffen zu formulieren („in anderer geeigneter Weise zu stören“ oder „sonstige Eingriffe in informationstechnische Systeme“).

Zitiergebot des Artikels 19 Absatz 1 Satz 2 des Grundgesetzes:

Das Zitiergebot wird gewahrt. Im neuen § 11 BbgPolG wird die Einschränkung der Grundrechte durch dieses Gesetz geregelt, insbesondere auch der Grundrechte der Unverletzlichkeit des Fernmeldegeheimnisses (Artikel 10 Absatz 1 des Grundgesetzes, Artikel 16 Absatz 1 der Verfassung des Landes Brandenburg) und des Datenschutzes (Artikel 11 der Verfassung des Landes Brandenburg). Die betroffenen und zu zitierenden Grundrechte werden im Gesetzestext ausdrücklich als eingeschränkt benannt.

Fernmeldegeheimnis (Artikel 10 Absatz 1 des Grundgesetzes, Artikel 16 Absatz 1 der Verfassung des Landes Brandenburg):

Der Schutz des Fernmeldegeheimnisses erfasst Telekommunikation unabhängig von der Übermittlungsart (Kabel oder Funk, analoge oder digitale Vermittlung) und der Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten). Der Schutzbereich erstreckt sich auch auf die Kommunikationsdienste des Internets. Darüber hinaus sind nicht nur die Inhalte der Telekommunikation vor einer Kenntnisnahme geschützt, sondern auch ihre Umstände.

Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff allein am Fernmeldegeheimnis zu messen.

Der Grundrechtsschutz erfasst nicht die polizeiliche Überwachung eines informationstechnischen Systems als solches oder die Durchsuchung von Speichermedien des Systems.

Das Fernmeldegeheimnis ist der Maßstab für die Beurteilung einer Ermächtigung zur „Quellen-Telekommunikationsüberwachung“, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dabei handelt es sich um gesicherte Kommunikationsinhalte, die die Polizei ohne oder gegen den Willen der betroffenen Personen erhebt. Geschützt wird das Vertrauen, dass eine Fernmeldekommunikation nicht von Dritten zur Kenntnis genommen wird.

Das heimliche Aufklären des Internets greift in das Fernmeldegeheimnis ein, wenn die Polizei zugangsgesicherte Kommunikationsinhalte überwacht, indem sie Zugangsschlüssel nutzt, die sie ohne oder gegen den Willen der Kommunikationsbeteiligten erhoben hat. So liegt es etwa, wenn ein mittels Keylogging erhobenes Passwort eingesetzt wird, um Zugang zu einem E-Mail-Postfach oder zu einem geschlossenen Chat zu erlangen.

Die Regelungen stehen mit dem Gebot der Verhältnismäßigkeit im engeren Sinne in Einklang.

Der Eingriff in das Fernmeldegeheimnis wiegt schwer. Auf der Grundlage der Regelungen kann die Polizei auf Kommunikationsinhalte zugreifen, die sensibler Art sein und Einblicke in die persönlichen Angelegenheiten und Gewohnheiten der betroffenen Personen zulassen können. Betroffen ist nicht nur derjenige, der den Anlass für die Überwachungsmaßnahme gegeben hat. Der Eingriff kann vielmehr eine gewisse Streubreite aufweisen, wenn Erkenntnisse nicht nur über das Kommunikationsverhalten desjenigen, gegen den sich die Maßnahme richtet, sondern auch über seine Kommunikationspartner gewonnen werden. Die Heimlichkeit des Zugriffs erhöht die Eingriffsintensität.

Die Regelungen dienen der effektiven Gefahrenabwehr und selektiven Kriminalprävention zum Schutz bedeutsamer Rechtsgüter. Diese Schutzzwecke sind legitim. Vor dem Hintergrund der Kriminalitätsentwicklungen vermögen die Regelungen diese Zielsetzungen zu fördern und sind mithin geeignet. Da keine gleich geeigneten mildereren Mittel zu Erreichung dieser Ziele ersichtlich sind – insbesondere wäre die offene Überwachung der Telekommunikation im Hinblick auf den Schutzzweck weniger effektiv – sind die Regelungen auch erforderlich.

Schließlich sind die Regelungen auch angemessen und verstoßen nicht gegen das Übermaßverbot, denn sie sind unter Berücksichtigung der Eingriffsintensität in das Fernmeldegeheimnis und der mit den Grundrechtseingriffen verfolgten Ziele noch zumutbar. Unter Abwägung des Schutzes des Fernmeldegeheimnisses und der verfolgten legitimen Ziele kann zwar keiner der beiden Seiten per se der Vorrang eingeräumt werden. Für die Angemessenheit der Regelungen spricht aber die präzise Ausrichtung auf die Bekämpfung schwerer Kriminalität. Ein derart schwerwiegender Grundrechtseingriff setzt unter Berücksichtigung des Gewichts der Ziele der Polizei grundsätzlich zumindest die Normierung einer qualifizierten materiellen Eingriffsschwelle voraus. Dieser Voraussetzung wird durch die Regelungen genüge getan. Sie werden dem Gebot der Normenklarheit und Normenbestimmtheit gerecht, denn die Eingriffsvoraussetzungen sind hinreichend präzise geregelt. Die Schutzgüter wurden in ausreichendem Maße eingegrenzt und das Anknüpfen an eine konkrete Gefahr ist ausreichend. Die Verhütung oder vorbeugende Bekämpfung von besonders schweren Straftaten oder von schwerwiegenden Kriminalitätsphänomenen muss sich am Maßstab der konkreten Gefahr messen lassen, die jedoch entsprechend der Ausführungen zum Begriff der konkreten Gefahr in § 3 BbgPolG im Kausalverlauf weit vorgelagert sein kann. Die Begrenzung auf Personen, die für eine erhebliche konkrete Gefahr oder besonders schwere Straftaten verantwortlich oder notstandspflichtig sind oder einem schwerwiegenden Kriminalitätsphänomen zugeordnet werden können, sowie auf deren Kontakt- oder Begleitpersonen schränkt die Streubreite dieser Regelungen hinreichend ein. Weiterhin bestehen weitreichende Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung.

Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes, Artikel 15 der Verfassung des Landes Brandenburg):

Der grundrechtliche Schutz der Wohnung vermittelt dem Einzelnen keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems, auch wenn sich dieses System in einer Wohnung befindet. Denn der Eingriff kann unabhängig vom Standort erfolgen, so dass ein raumbezogener Schutz nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren. Soweit die Infiltration die Verbindung des betroffenen Rechners zu einem Rechnernetzwerk ausnutzt, lässt sie

die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt. Der Standort des Systems wird in vielen Fällen für die Ermittlungsmaßnahme ohne Belang und oftmals für die Polizei nicht einmal erkennbar sein. Somit führt der raumbezogene Schutz der Wohnung nicht zu einem Schutz vor einer raumunabhängig vorgenommenen Infiltration eines informationstechnischen Systems durch die Polizei. Der Schutzbereich ist somit nicht eröffnet.

Allgemeines Persönlichkeitsrecht und Datenschutz (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes, Artikel 11 der Verfassung des Landes Brandenburg):

In seiner Ausprägung als Schutz der Privatsphäre gewährleistet das allgemeine Persönlichkeitsrecht dem Einzelnen einen räumlich und thematisch bestimmten Bereich, der grundsätzlich frei von unerwünschter Einsichtnahme bleiben soll.

Das Schutzbedürfnis des Nutzers eines informationstechnischen Systems beschränkt sich jedoch nicht allein auf Daten, die seiner Privatsphäre zuzuordnen sind. Eine solche Zuordnung hängt zudem häufig von dem Kontext ab, in dem die Daten entstanden sind und in den sie durch Verknüpfung mit anderen Daten gebracht werden. Dem Datum selbst ist vielfach nicht anzusehen, welche Bedeutung es für die betroffene Person hat und welche es durch Einbeziehung in andere Zusammenhänge gewinnen kann. Das hat zur Folge, dass mit der Infiltration des Systems nicht nur zwangsläufig private Daten erfasst werden, sondern der Zugriff auf alle Daten ermöglicht wird, so dass sich ein umfassendes Bild vom Nutzer des Systems ergeben kann. Somit ist der Schutz der Privatsphäre hier nicht einschlägig.

Das Recht auf informationelle Selbstbestimmung geht über den Schutz der Privatsphäre hinaus. Es gibt dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Es flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit, indem es ihn schon auf der Stufe der Persönlichkeitsgefährdung beginnen lässt. Der Schutzzumfang des Rechts auf informationelle Selbstbestimmung beschränkt sich dabei nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden. Auch der Umgang mit personenbezogenen Daten, die für sich genommen nur geringen Informationsgehalt haben, kann, je nach dem Ziel des Zugriffs und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten, grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit der betroffenen Person haben.

Jedoch trägt das Recht auf informationelle Selbstbestimmung den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit der betroffenen Person über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus.

Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgt ein grundrechtlich erhebliches Schutzbedürfnis. Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet.

Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ist anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten der betroffenen Person in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf Computer einer Person. Nicht nur bei einer Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung lässt sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen. Der spezifische Grundrechtsschutz erstreckt sich ferner beispielsweise auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können.

Geschützt ist zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.

Die vorliegenden Regelungen greifen in den Schutzbereich des Allgemeinen Persönlichkeitsrechts bzw. Datenschutzrechts in Gestalt des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme ein.

Die eingreifenden Regelungen sind jedoch gerechtfertigt. Obwohl das Allgemeine Persönlichkeitsrecht aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes abgeleitet wird, gilt für dieses nicht der Absolutheitsschutz der Menschenwürde. Als Schranke bleibt die verfassungsmäßige Ordnung. Der Einzelne muss dabei nur solche Beschränkungen seines Rechts hinnehmen, die auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen.

Die Regelungen verfolgen legitime Ziele, die durch diese erreicht werden können. Sie sind auch erforderlich. Eine Regelung ist erforderlich, wenn es keinen gleich geeigneten, aber grundrechtsschonenderen Weg zur Erreichung des Ziels gibt. Hier kommt dem Staat eine weite Einschätzungsprärogative zu. Denkbar wäre etwa eine offene Sicherstellung der Festplatten eines Computers oder eines USB-Sticks. Dies wäre grundrechtsschonender. Jedoch könnten so nicht die Veränderungen und die Arbeit auf dem Computer über längere Zeit beobachtet werden. Zudem wären andere Ermittlungen möglicherweise durch die Warnung der betroffenen Person vereitelt. Darüber hinaus können Datenträger so gut verschlüsselt sein, dass man an die Daten nur durch den Eingriff in informationstechnische Systeme oder wenn man die betroffene Person überwältigt, während sie den Da-

tenträger nutzt, in der Hoffnung, dass sie diesen nicht abziehen kann. Das Stürmen einer Wohnung durch eine polizeiliche Spezialeinheit und die Anwendung von körperlicher Gewalt, um einen Datenträger sicherzustellen, sind im Zweifel sogar ein schärferes Mittel als der Eingriff ins informationstechnische System. Im Bereich des Terrorismus oder der organisierten Kriminalität kann es auch zu bewaffneten Auseinandersetzungen kommen. Somit ist eine offene Maßnahme nicht gleich geeignet.

Mit Blick auf die zum Fernmeldegeheimnis gemachten Ausführungen sind die Regelungen auch hinsichtlich des Allgemeinen Persönlichkeitsrechts als angemessen zu betrachten. Die Regelungen enthalten zudem weitere Schutzmechanismen, wie den Richtervorbehalt sowie Kennzeichnungs-, Datenschutz- und Protokollierungspflichten. Darüber hinaus sind die Regelungen im Bereich der selektiven Kriminalprävention, also bei der Verhütung oder vorbeugenden Bekämpfung von besonders schweren Straftaten oder von schwerwiegenden Kriminalitätsphänomenen, an kriminalpräventive Handlungskonzepte und operative Präventionsplanungen gebunden, die die Streubreite dieser Regelungen weiter auf ein gezieltes Handeln der Polizei einschränken. Schließlich sind auch die allgemeinen datenschützenden Vorschriften in Kapitel 2 Abschnitt 2 Unterabschnitt 1 zu berücksichtigen.

Zu § 50 (Bestandsdatenauskunft)

Der neue § 50 BbgPolG übernimmt die Vorschrift des alten § 33c BbgPolG und orientiert sich bei den Änderungen an der Regelung des neuen § 49 BbgPolG.

Zu § 51 (Datenerhebung durch den Einsatz von Vertrauenspersonen)

Der neue § 51 BbgPolG regelt die Datenerhebung durch den Einsatz von Vertrauenspersonen. Der alte § 34 BbgPolG enthält Definitionen zu der Vertrauensperson sowie zu den Kontakt- oder Begleitpersonen, die sich nun im neuen § 3 BbgPolG wiederfinden. Aufgrund der Rechtsprechung des Bundesverfassungsgerichtes und der Erkenntnisse in der Aufarbeitung des NSU besteht ein gesteigertes rechtspraktisches Regelungserfordernisses für den Einsatz von Vertrauenspersonen flankierenden Regelungen.

Absatz 1 enthält als Tatbestandsvoraussetzungen die erhebliche konkrete Gefahr sowie die Verhütung oder vorbeugende Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen. Erfasst werden Personen, die für solche Gefahren oder Straftaten verantwortlich, die notstandspflichtig sind oder die einem solchen Kriminalitätsphänomen zugeordnet werden können, sowie deren Kontakt- oder Begleitpersonen. Die Erfüllung der polizeilichen Aufgaben muss ansonsten gefährdet oder wesentlich erschwert sein. Insoweit wird in die Einzelfallprüfung auch einzubeziehen sein, ob die Gefahrenabwehr nicht ebenso zweckerfüllend und vollständig durch andere (verdeckte) polizeiliche Maßnahmen erfolgen kann.

Es wird klargestellt, dass ein Einsatz von Vertrauenspersonen nicht vorliegt, soweit sich eine, auch wiederkehrende, polizeiliche Datenerhebung auf die Erlangung von bei dieser Person bereits vorhandenen und von dieser angebotenen Daten beschränkt.

Es dürfen auch personenbezogene Daten über andere Personen erhoben werden, soweit dies erforderlich ist, um eine Datenerhebung mit Vertrauenspersonen durchführen zu können, es sei denn, es handelt sich um Berufsgeheimnisträger gemäß §§ 53, 53a der Strafprozessordnung, zu denen ein Vertrauensverhältnis besteht. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34 BbgPolG. Die Benachrichtigung der betroffenen Person erfolgt nach § 35 BbgPolG.

Absatz 2 regelt nach Maßgabe des Bundesverfassungsgerichts im BKAG-Urteil den Richtervorbehalt mit Eilfallkompetenz der Behördenleitung. Die Anordnung ist auf höchstens sechs Monate zu befristen und kann um jeweils längstens sechs Monate verlängert werden. Sie kann insbesondere auch nähere Maßgaben zur Führung der Vertrauensperson enthalten (wie etwa 4-Augen- und/oder Rotationsprinzip etc.).

In Absatz 3 werden (nicht abschließend) zweckgebundene Einsatzverbote gesetzlich normiert, wie sie etwa auch in § 36 Absatz 3 des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung enthalten sind. In den Nummern 1 und 2 werden dabei die Grundsätze der Rechtsprechung für einen unzulässigen Lockspitzeinsatz (agent provocateur) im Hinblick auf das Verbot der An- und Aufstiftung ausdrücklich normiert. Auch dürfen Vertrauenspersonen nach Nummer 3 nicht eingesetzt werden, um Daten mit Mitteln oder Methoden zu erheben, die der Polizei selbst nicht zur Verfügung stehen (etwa durch Folter). Außerdem wird dadurch ausgeschlossen, dass die Einhaltung der Voraussetzungen anderweitiger polizeilicher Befugnisnormen durch den Einsatz von Vertrauenspersonen zielgerichtet umgangen wird.

In Absatz 4 werden – in Anlehnung an die Regelung in § 9b Absatz 2 Sätze 2 und 3 des Bundesverfassungsschutzgesetzes – personengebundene Einsatzverbote für Vertrauenspersonen normiert, unter deren Voraussetzungen die dort bezeichneten Personen von vornherein für den Einsatz als Vertrauenspersonen ausgeschlossen sind. So werden der Schutz von Minderjährigen, ausstiegswilliger Personen und der parlamentarischen Gesetzgeber umgesetzt. Ein Ausschlussgrund wegen bestimmter vorausgegangener Straftaten, die im Bundeszentralregister eingetragen sind (Totschlag oder einer allein mit lebenslanger Haft bedrohten Straftat). Da ein Zugang von Vertrauenspersonen in abgeschottete, konspirativ agierende Milieustrukturen den praktischen Erfahrungen nach oftmals nur jemandem gelingen kann, der in der Vergangenheit selbst einmal mit kriminellen Handlungen in Erscheinung getreten ist, führen strafrechtliche Voreintragungen bzw. die zurückliegende Verbüßung von Straftat ansonsten nicht von Vorneherein zum Ausschluss der Einsetzbarkeit einer Vertrauensperson.

Solche Straftaten sind jedoch im Rahmen der fortlaufenden Zuverlässigkeitsüberprüfung nach Absatz 5 einzubeziehen. Die durch eine Vertrauensperson gewonnenen Informationen sind nach Möglichkeit unverzüglich zu überprüfen. Bei begründeten Zweifeln ist der Einsatz einer Vertrauensperson entweder von vornherein nicht durchzuführen oder zu beenden. Es ist zu hinterfragen, inwieweit die Vertrauensperson aus wirtschaftlichen Gründen zu einer Zusammenarbeit mit der Polizei gedrängt sein könnte. Zu beachten ist zudem eine rechtskräftige, noch nicht getilgte Verurteilung wegen eines Verbrechens oder zu einer vollstreckenden Freiheitsstrafe. Derartige Eintragungen können im Einzelfall indizielle Wirkung für die mangelnde Eignung einer Vertrauensperson haben. Laufende Ermittlungs- oder Strafverfahren stehen – vor allem in Anbetracht der Unschulds-

vermutung – nicht generell einer Verwendung als Vertrauensperson entgegen. Die Begehung jeglicher Straftaten durch Vertrauensperson kann seitens der Polizei nicht geduldet werden. Bei bestehendem Anfangsverdacht der Begehung strafbarer Handlungen sind die polizeilichen Vertrauensperson-Führer auf Grund des Legalitätsprinzips nach §§ 152 Absatz 2, 163 Absatz 1 Satz 1 der Strafprozessordnung zur Einleitung eines strafrechtlichen Ermittlungsverfahrens gesetzlich verpflichtet. Kommen sie dem nicht nach, setzen sie sich selbst der Gefahr einer strafrechtlichen Verfolgung wegen Strafvereitelung im Amt nach §§ 258, 258a des Strafgesetzbuches aus.

Absatz 6 ermöglicht dem Führer einer Vertrauensperson, von einer Legendierung, insbesondere ggf. Tarnpapieren, zur Vorbereitung, Leitung und Absicherung des Einsatzes Gebrauch zu machen.

Zu § 52 (Datenerhebung durch den Einsatz verdeckt ermittelnder Personen)

Der neue § 52 BbgPolG regelt die Datenerhebung durch den Einsatz verdeckt ermittelnder Personen, die bisher im alten § 35 BbgPolG zu finden ist. Absatz 1 enthält Voraussetzungen wie § 51 BbgPolG.

Absatz 2 umfasst die Legendierung, die Ausstellung von Tarnpapieren, die Wohnungsbetretung und die Teilnahme am Rechtsverkehr. Außerdem wird wie im Bayerischen Polizeiaufgabengesetz eine Anwendung dieser Regelungen auf verdeckt ermittelnde Personen in elektronischen Medien und Kommunikationseinrichtungen sowie auf polizeiliche Führungspersonen verdeckt ermittelnder Person sichergestellt.

In Absatz 3 wird entsprechend den Feststellungen des Bundesverfassungsgerichtes im BKAG-Urteil und in Anlehnung an § 110b Strafprozessordnung sowie an den neugefassten § 45 Absatz 3 Satz 1 Nummer 5 BKAG ein grundsätzlicher Richtervorbehalt mit Eilfallkompetenz der Behördenleitung eingeführt, wenn sich der Einsatz verdeckt ermittelnder Personen gegen eine bestimmte Person richtet oder bei diesem die Vertrauensperson oder die verdeckt ermittelnde Person eine Wohnung betritt, die nicht allgemein zugänglich ist. Das Bundesverfassungsgericht setzt den Einsatz einer verdeckt ermittelnden Person maßgeblich in Zusammenhang mit dem Ausnutzen von Vertrauen, was erst bei einem zielgerichteten Einsatz zur personenbezogenen Datenerhebung angenommen werden kann. Bei anderen Fallkonstellationen kann die Behördenleitung diese Maßnahme anordnen. Bei dem Umfang und der Dauer der Maßnahme ist zu beachten, dass eine verdeckt ermittelnde Person zumeist erst „aufgebaut“ und an eine Zielperson herangeführt werden muss. Daher ist von vorneherein von längeren Einsatzdauern auszugehen.

Zu § 53 (Polizeiliche Ausschreibung)

Im neuen § 53 BbgPolG wird die bislang im alten § 36 BbgPolG enthaltene Regelung zur polizeilichen Ausschreibung geregelt. Die alten Absätze 1 und 1a werden zusammengeführt, so dass der neue Absatz 1 nunmehr die Ausschreibung in einer Datei zur polizeilichen Beobachtung, verdeckten Registrierung und gezielten Kontrolle (Artikel 99 des Schengener Durchführungsübereinkommens) regelt. Die Ausschreibung zur polizeilichen Beobachtung dient lediglich dem Zweck, polizeiliche Zufallserkenntnisse über das Antreffen einer bestimmten ausgeschriebenen Person zusammenzuführen und an die ausschreibende Dienststelle zu übermit-

teln, um dort insbesondere punktuell die Reisewege der Person sowie Zusammenhänge und Querverbindungen nachvollziehen zu können. Demgegenüber dient die verdeckte Registrierung und Ausschreibung zur gezielten Kontrolle darüber hinausgehend dem Zweck, Ausschreibungen mit der Intention zu veranlassen, dass bei Vorliegen der entsprechenden gesetzlichen Voraussetzungen weitergehende polizeiliche Maßnahmen der Identitätsfeststellungen sowie der Personen- und Sachdurchsuchung durch die kontrollierende Polizeidienststelle getroffen und auch die aus diesen Maßnahmen erlangten Erkenntnisse der ausschreibenden Dienststelle mitgeteilt werden. Hierdurch wird die Möglichkeit geschaffen, wichtige Informationen, wie z. B. schriftliche Unterlagen über Personenzusammenhänge und den Organisationsgrad extremistischer oder terroristischer Gruppierungen, potentielle Anschläge, Anschlagsvorbereitungen oder illegale Finanztransaktionen erheben zu können sowie in der offenen Ermittlungsphase den Druck zu erhöhen, potentielle Gefährder zu verunsichern und hierdurch ggf. von ihrem beabsichtigten Tun abzubringen.

Außerdem wird der bisherige Wortlaut dahingehend angepasst, dass nicht nur das amtliche Kennzeichen von Kraftfahrzeugen, sondern jegliche Kennzeichen sämtlicher, ggf. auch unmotorisierter Fahrzeuge Merkmale der Ausschreibung sein können.

Tatbestandsvoraussetzungen sind die Abwehr einer erheblichen konkreten Gefahr oder die Verhütung oder vorbeugende Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen. Der betroffene Personenkreis umfasst nach den §§ 7 oder 8 BbgPolG bzw. für solche Straftaten oder Kriminalitätsphänomene verantwortliche Personen sowie deren Kontakt- oder Begleitpersonen.

Absatz 2 übernimmt die Regelung des alten Absatzes 2 zur Konkretisierung der Datenerhebung und -übermittlung.

Absatz 3 entspricht dem alten Absatz 3, wobei die Anordnungsbefugnis durch den „Behördenleiter“ durch die „Behördenleitung“ ersetzt wurde.

Der alte Absatz 4 wird durch die allgemeinen Vorschriften zur Verarbeitung personenbezogener Daten erfasst. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34 BbgPolG. Die Benachrichtigung der betroffenen Person erfolgt nach § 35 BbgPolG.

Zu § 54 (Anlassbezogene automatische Kennzeichenfahndung)

Der neue § 54 BbgPolG ermöglicht die bisher in § 36a BbgPolG geregelte anlassbezogene automatische Kennzeichenfahndung. Erfasst werden durch Absatz 1 alle Fahrzeuge, nicht nur Kraftfahrzeuge. Die Polizei kann deren Kennzeichen sowie Ort, Datum, Uhrzeit und Fahrtrichtung durch den verdeckten Einsatz technischer Mittel automatisiert erfassen. Tatbestandsvoraussetzungen sind die Abwehr einer erheblichen konkreten Gefahr, das Vorliegen entsprechender Lageerkenntnisse in den Fällen des § 15 Absatz 1 Nummer 1 bis 6 oder die polizeiliche Ausschreibung der Person oder des Fahrzeuges nach § 53 Absatz 1 Satz 1. Dem § 15 Absatz 1 Nummer 4 bzw. 6 liegen eine erhöhte abstrakte bzw. eine abstrakte Gefahr zu Grunde. Diese Gefahrenbegriffe können aufgrund der Eingriffsintensität der verdeckten anlassbezogenen automatischen Kennzeichenfahndung keine

Eingriffsvoraussetzung sein. Es müssen vielmehr Lageerkenntnisse einer konkreten Gefahr vorliegen, die die Eingriffsgrundlage dieser Vorschrift bildet.

In den Fällen der polizeilichen Ausschreibung dürfen Einzelerfassungen zu einem Bewegungsbild verbunden werden. Die Kennzeichenerfassung darf nicht flächendeckend eingesetzt werden. Zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung gilt § 34 BbgPolG. Die Benachrichtigung der betroffenen Person erfolgt nach § 35 BbgPolG. Die anlassbezogene automatische Kennzeichenfahndung darf nur durch die Behördenleitung angeordnet werden.

Absatz 2 übernimmt die Regelung des alten Absatzes 2. Es wird jedoch klargestellt, dass auch ein Abgleich mit den Daten der polizeilichen Fahndungsbestände erfolgen kann. Polizeiliche Fahndungsbestände umfassen beispielsweise Fahrzeuge oder Kennzeichen, die durch Straftaten oder sonst abhanden gekommen sind oder hinsichtlich derer auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass sie bei der Begehung von Straftaten benutzt werden. Es gibt zudem Fahndungsbestände über Personen, die ausgeschrieben sind zur polizeilichen Beobachtung, gezielten Kontrolle oder verdeckten Registrierung, aus Gründen der Strafverfolgung, Strafvollstreckung, Auslieferung oder Überstellung, zum Zweck der Durchführung ausländerrechtlicher Maßnahmen oder wegen gegen sie veranlasster polizeilicher Maßnahmen der Gefahrenabwehr.

Zu § 55 (Einsatz und Abwehr unbemannter Luftfahrtsysteme)

Der neue § 55 BbgPolG regelt den Einsatz und die Abwehr unbemannter Luftfahrtsysteme.

Absatz 1 zum Einsatz unbemannter Luftfahrtsysteme orientiert sich an Artikel 47 BayPAG. Auf Grund der mit dem Einsatz von Drohnen einhergehenden, nicht unerheblichen zusätzlichen Eingriffsqualität wird eine gesetzliche Klarstellung normiert, was die Zulässigkeit deren Verwendung bei bestimmten Maßnahmen der Datenerhebung betrifft. Unter den Voraussetzungen der hier aufgeführten Befugnisnormen ist dabei auch ein Drohneneinsatz zur Datenerhebung zulässig. Das bedeutet zugleich, dass hiermit keine Ausweitung dieser Befugnisnormen erfolgt. Absatz 1 steht also in einem Akzessorietätsverhältnis zu den Befugnisnormen. Darüber hinaus gelten auch die allgemeinen Voraussetzungen über die Datenverarbeitung.

Verwiesen wird auf die Befugnisnormen

- für offene Bild- und Tonaufnahmen oder -aufzeichnungen nach § 44 Absatz 1 oder 2,
- des Einsatzes besonderer Mittel der Datenerhebung nach § 47 Absatz 2,
- des Einsatzes technischer Mittel in Wohnungen nach § 48 Absatz 1,
- der Eingriffe in die Telekommunikation und in informationstechnische Systeme nach § 49 Absatz 1 bis 3 und
- der anlassbezogenen automatischen Kennzeichenfahndung nach § 54 Absatz 1.

Bei Bild- und Tonaufnahmen oder -aufzeichnungen nach § 44 Absatz 1 oder 2 muss die Offenheit der Maßnahme gewahrt bleiben und die Polizei auf den Einsatz von unbemannten Luftfahrtsystemen gesondert hinweisen, etwa durch einen gut sichtbaren Hinweis auf der Kleidung des die Drohne steuernden Beamten, im Eingangsbereich von Veranstaltungen oder durch das feste Aufstellen von ausreichend Schildern beispielsweise bei einem kontinuierlichen Einsatz im Gebiet der Bundesgrenze bis zu einer Tiefe von dreißig Kilometern.

Die unbemannten Luftfahrtsysteme dürfen mit technischen Mitteln der Bild-, Ton- und Sensoraufklärung ausgestattet, nicht aber bewaffnet werden. Soweit eine richterliche Anordnung erforderlich ist, muss diese auch den Einsatz von unbemannten Luftfahrtsystemen umfassen.

In Absatz 2 wird die Abwehr unbemannter Luftfahrtsysteme einschließlich ihrer Kontrollstation oder unbemannter Fluggeräte zu Zwecken des Sports oder der Freizeitgestaltung geregelt. Voraussetzung ist, dass von diesen eine konkrete Gefahr ausgeht. Diese dürfen dann durch den Einsatz technischer oder anderer Mittel gestört, heruntergeholt oder in sonstiger Weise beeinflusst werden. Dabei muss die Polizei aber darauf vertrauen können, dass durch die Maßnahme das Leben von Menschen nicht gefährdet wird. Außerdem muss die Gefahr für die betroffenen Schutzgüter im Rahmen der Abwägung mit den Eingriffen in sonstige betroffene Rechtsgüter überwiegen.

Zu §§ 56 bis 59 (Datenspeicherung, Datenveränderung und Datennutzung)

Die neuen §§ 56 bis 59 BbgPolG regeln die bisher in den alten §§ 37 bis 40 BbgPolG (Unterabschnitt 3) enthaltene Datenspeicherung, Datenveränderung und Datennutzung. Es erfolgen einige grammatikalische und paragrafenverweisliche Anpassungen.

Im neuen § 58 Absatz 1 BbgPolG zur Speicherung, Veränderung und Nutzung von Daten wird klargestellt, dass die Benachrichtigung der betroffenen Person nach dem neuen § 35 BbgPolG erfolgt. In Absatz 3 wird geregelt, dass die Polizei über Kontakt- oder Begleitpersonen sowie über Auskunftspersonen personenbezogene Daten suchfähig in Dateien speichern, verändern und nutzen kann, soweit dies zur Abwehr einer erheblichen konkreten Gefahr oder zur Verhütung oder vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen erforderlich ist. In Absatz 4 wird bei den Ausnahmen des Löschens die Aufbewahrung der Aufzeichnungen von Anrufen über Notrufeinrichtungen auch bei Tatsachen zum Veranlassen oder Unterstützen von Straftaten sowie zur Verhütung oder vorbeugenden Bekämpfung von Straftaten oder Kriminalitätsphänomenen ermöglicht. Die Absätze 5 und 6 werden um die Pseudo-nymisierung erweitert und in Absatz 6 ein Nutzungsverbot von personenbezogenen Daten nur nach den §§ 48 und 49 Absatz 2 BbgPolG für polizeiliche Aus- und Fortbildungszwecke festgelegt.

Im neuen § 59 Absatz 1 BbgPolG zum Datenabgleich wird klargestellt, dass die betroffene Person für die Dauer des Datenabgleichs angehalten werden kann. Absatz 2 regelt, dass ein Datenabgleich nach Absatz 1 auch unter Verwendung bildverarbeitender Systeme und durch Auswertung biometrischer Daten erfolgen, wenn andernfalls die Erfüllung polizeilicher Aufgaben gefährdet oder wesentlich erschwert würde. Dies umfasst auch die sogenannte Gesichtsfeldererkennung, eine automatisierte Erkennung biometrischer Merkmale. Biometrische Daten gehören

grundsätzlich den besonderen Kategorien im Sinne des § 33 Absatz 6 BbgPolG an. Nicht davon erfasst ist ein normaler Lichtbildabgleich. Etwas anderes gilt aber dann, wenn wie bei der Gesichtsfeldererkennung eine spezielle technische Aufbereitung zur eindeutigen Identifizierung erfolgt. In diesen Fällen ist stets eine Datenschutzfolgenabschätzung vorzunehmen. Wenn eine automatisierte Entscheidungsfindung im Einzelfall stattfindet, muss § 33 Absatz 7 BbgPolG berücksichtigt werden. In der Regel dürfte aber eine natürliche Person zwischengeschaltet sein.

Zu §§ 60 bis 66 (Datenübermittlung)

Die neuen §§ 60 bis 66 BbgPolG regeln die bisher in den alten §§ 41 bis 46 BbgPolG (Unterabschnitt 4) enthaltene Datenübermittlung. Es erfolgen einige grammatikalische und paragrafenverweisliche Anpassungen. Darüber hinaus lässt sich aus der EU-Datenschutzrichtlinie für den Bereich der Polizei in Verbindung mit dem Rahmenbeschluss 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 und dem Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität das Ziel entnehmen, dass der freie Verkehr personenbezogener Daten zwischen den zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit innerhalb der Union und die Übermittlung solcher personenbezogener Daten an Drittländer und internationale Organisationen, erleichtert werden sollte. Dementsprechend werden Änderungen in den Paragrafen dieses Unterabschnitts vorgenommen. Schließlich werden die Regelung zur Rasterfahndung angepasst sowie Regelungen zum Profiling und zu projektbezogenen gemeinsamen Dateien mit dem Verfassungsschutz Brandenburg eingeführt.

Der neue § 61 BbgPolG zur Datenübermittlung zwischen Polizeibehörden verweist in Absatz 2 Satz 1 auf § 62 Absatz 5 und 6 BbgPolG.

Im neuen § 62 BbgPolG wird die Datenübermittlung an öffentliche Stellen, an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen geregelt. Der neue Absatz 4 enthält eine Regelung zur Übermittlung personenbezogener Daten an die Nachrichtendienste des Bundes und der Länder. Voraussetzung ist, dass die Daten zugleich konkrete Erkenntnisse zu einer Gefährdung der jeweiligen Rechtsgüter erkennen lassen, die für die Lagebeurteilung nach Maßgabe der Aufgaben dieser Behörden bedeutsam sind.

Der neue Absatz 5 legt fest, dass die Polizei wie im Inland personenbezogene Daten an öffentliche Stellen eines Mitgliedstaats der Europäischen Union, der Europäischen Union oder eines schengenassoziierten Staats übermitteln kann.

Nach dem neuen Absatz 6 kann die Polizei personenbezogene Daten an öffentliche Stellen von Drittstaaten sowie an über- und zwischenstaatliche Stellen übermitteln, wenn dies auf Grund eines konkreten Ermittlungsansatzes zur Verhütung, vorbeugenden Bekämpfung, Unterbindung oder Verfolgung von Straftaten oder Kriminalitätsphänomenen oder zur Abwehr von konkreten Gefahren erforderlich ist, die empfangende Stelle für diese Zwecke zuständig ist und

- die Europäische Kommission einen Beschluss gefasst hat, wonach der Drittstaat oder die über- oder zwischenstaatliche Stelle ein angemessenes Datenschutzniveau bietet,
- auf Grund völkerrechtlicher Vereinbarungen oder anderer geeigneter Garantien der Schutz personenbezogener Daten sichergestellt ist oder
- die Übermittlung erforderlich ist zur Abwehr von erheblichen oder gegenwärtigen konkreten Gefahren oder zur Wahrung schutzwürdiger Interessen oder Belange einer betroffenen Person, sofern Rechte oder Interessen Dritter nicht überwiegen.

Die Polizei kann personenbezogene Daten im Einzelfall bei Gefahr im Verzug unmittelbar an andere öffentliche Stellen in Drittstaaten übermitteln. Die Datenübermittlung unterbleibt, soweit Grund zu der Annahme besteht, dass dadurch gegen den Zweck eines deutschen Gesetzes oder einer Regelung der Europäischen Union oder der Konvention zum Schutz der Menschenrechte und Grundfreiheiten – insbesondere gegen Menschen- und Grundrechte, Datenschutzregelungen oder die Vorschriften zur Speicherungs-, Nutzungs- oder Übermittlungsbeschränkung oder zur Lösungsverpflichtung – verstoßen wird oder schutzwürdige Belange einer betroffenen Person, die das öffentliche Interesse an der Übermittlung überwiegen, beeinträchtigt werden.

Der neue § 63 BbgPolG regelt die Datenübermittlung an Personen oder an Stellen außerhalb des öffentlichen Bereichs und nunmehr in einem neuen Absatz 3 auch die Bekanntgabe personenbezogener Daten an die Öffentlichkeit. Diese Öffentlichkeitsfahndung zur effektiven Gefahrenabwehr ist eine wichtige präventiv-polizeiliche Maßnahme. In § 131b der Strafprozessordnung gibt es bereits eine Regelung zur repressiven Öffentlichkeitsfahndung. Diese Gesetzeslücke im präventiven Polizeirecht wird nun geschlossen, um die Bevölkerung möglichst wirksam vor Gefahren zu schützen.

Die Öffentlichkeitsfahndung dient der Ermittlung der Identität einer Person oder ihres Aufenthaltsortes oder der Warnung der Öffentlichkeit. So kann eine möglichst große Anzahl von Menschen schnell informiert werden, insbesondere über das Internet, die Presse, den Rundfunk und das Fernsehen. Rückinformationen aus der Öffentlichkeit werden angestrebt, um die Gefahr abzuwehren. Insbesondere Abbildungen der Person spielen hierbei eine wichtige Rolle. Die Bekanntgabe kann mit auf tatsächlichen Anhaltspunkten beruhenden wertenden Angaben über die Person verbunden werden.

Die Öffentlichkeitsfahndung stellt einen schwerwiegenden grundrechtlichen Eingriff dar, so dass bereits die Tatbestandsvoraussetzungen eine solche Maßnahme erheblich eingrenzen müssen. Tatbestandsvoraussetzungen sind daher die Unerlässlichkeit zur Abwehr einer dringenden konkreten Gefahr oder die tatsachenbasierte Annahme dass diese Person Straftaten von erheblicher Bedeutung begehen, veranlassen oder unterstützen wird, und die Verhütung oder vorbeugende Bekämpfung dieser Straftaten auf andere Weise nicht möglich erscheint oder wesentlich erschwert wird. Die Öffentlichkeitsfahndung darf nur durch die Behördenleitung angeordnet werden.

Der neue § 64 BbgPolG regelt die Datenübermittlung an die Polizei. Der neue Absatz 3 umfasst das Ersuchen bei den Nachrichtendiensten zur Übermittlung mit

nachrichtendienstlichen Mitteln erhobener personenbezogener Daten. Voraussetzungen sind die Abwehr einer erheblichen konkreten Gefahr oder die Möglichkeit der Erhebung der Informationen mit eigenen Befugnissen. In Absatz 4 wird nunmehr das Ersuchen an Drittstaaten oder an andere über- oder zwischenstaatliche Stellen als die Europäischen Union ausdrücklich eingeschränkt, soweit Grund zu der Annahme besteht, dass dadurch oder durch die Datenverarbeitung des Drittstaates oder der über- oder zwischenstaatlichen Stelle gegen den Zweck eines deutschen Gesetzes oder einer Regelung der Europäischen Union oder der Konvention zum Schutz der Menschenrechte und Grundfreiheiten – insbesondere gegen Menschen- und Grundrechte, Datenschutzregelungen oder die Vorschriften zur Speicherungs-, Nutzungs- oder Übermittlungsbeschränkung oder zur Löschungsverpflichtung – verstoßen wird oder schutzwürdige Belange einer betroffenen Person, die das öffentliche Interesse an dem Ersuchen überwiegen, beeinträchtigt werden.

Der neue § 65 BbgPolG regelt die Rasterfahndung und das Profiling. Tatbestandsvoraussetzungen nach Absatz 1 sind die Abwehr einer erheblichen konkreten Gefahr oder die Verhütung oder vorbeugende Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen. Profiling ermöglicht der Polizei, die Übermittlung personenbezogener Daten von öffentlichen Stellen und Stellen außerhalb des öffentlichen Bereichs zu verlangen und diese mit anderen Datenbeständen automatisiert zu verarbeiten, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu analysieren, zu bewerten oder vorherzusagen. Eine Maßnahme (Rasterfahndung oder Profiling), die zur Folge hat, dass natürliche Personen auf Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist verboten. Für den Einsatz von Systemen der automatischen Datenverarbeitung zur automatisierten Entscheidungsfindung gilt § 33 Absatz 7 BbgPolG. Die Benachrichtigung der betroffenen Person erfolgt nach § 35 BbgPolG.

In Absatz 2 wird klargestellt, dass zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung § 34 BbgPolG gilt.

In Absatz 4 werden das Antragsrecht der Behördenleitung, der Richtervorbehalt mit Eilfallkompetenz der Behördenleitung und die unverzügliche Unterrichtung der oder des Landesbeauftragten geregelt. Die Anordnung der Maßnahmen ist schriftlich zu erlassen und zu begründen. Sie muss die zur Übermittlung verpflichtete Person bezeichnen und ist auf die Daten und Prüfungsmerkmale zu beschränken, die für den Einzelfall benötigt werden. Von den Maßnahmen ist die oder der Landesbeauftragte unverzüglich zu unterrichten.

Die Regelungen zur Rasterfahndung und zum Profiling führen zu erheblichen Grundrechtseingriffen (allgemeinen Handlungsfreiheit, Recht auf informationelle Selbstbestimmung und Datenschutz). Allerdings stellen die Abwehr einer erheblichen konkreten Gefahr oder die Verhütung oder vorbeugende Bekämpfung von Straftaten von erheblicher Bedeutung oder von schwerwiegenden Kriminalitätsphänomenen einen legitimen Zweck dar, der diese Grundrechtseingriffe rechtfertigt, weil die Reichweite dieser Regelungen hinreichend eingegrenzt und durch Schutzvorschriften flankiert ist. Ebenso wenig verstoßen diese Regelungen gegen das spezielle Gleichbehandlungsgebot aus Artikel 3 Absatz 3 Satz 1 des Grundgesetzes, denn es gibt ein ausdrückliches Diskriminierungsverbot.

Der neue § 66 BbgPolG regelt projektbezogene gemeinsame Dateien der Polizei mit dem Verfassungsschutz Brandenburg. Diese dienen der Unterstützung einer befristeten projektbezogenen Zusammenarbeit zwischen dem Landeskriminalamt, weiteren Polizeidienststellen des Landes und dem Verfassungsschutz des Landes Brandenburg. Bereits heute arbeiten Polizei und Verfassungsschutz in Analyseprojekten und Arbeitsgruppen zum Informationsaustausch, die zur Durchführung einzelner Projekte zu bestimmten kriminalpolizeilich und nachrichtendienstlich relevanten Bereichen eingerichtet wurden, zusammen, vgl. Gemeinsames Terrorismusabwehrzentrum (GTAZ), die zentrale Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern einschließlich der Rechtsprechung des Bundesverfassungsgerichtes und § 48a PolGBW. Analyseprojekte und Arbeitsgruppen dienen dazu, phänomenbezogene Erkenntnisse auszutauschen, zu analysieren und Bekämpfungsansätze zu entwickeln.

Gemeinsame Projektdaten führen in diesem Zusammenhang zu einer erheblichen Arbeitserleichterung. Durch ihren jeweiligen Zuschnitt auf die konkrete Projektarbeit können in diesen umfassende Informationen zu konkreten Themenkomplexen gezielt verdichtet werden. Die im Polizeigesetz geschaffenen Regelungen für gemeinsame Dateien gehen insoweit als speziellere Regelungen den anderen Vorschriften des Polizeigesetzes oder des Landesverfassungsschutzgesetzes vor.

Der durch die Projektdaten ermöglichte Informationsaustausch ist von erheblichem Gewicht. Für betroffene Personen kann die Aufnahme in eine solche Datei erheblich belastende Wirkungen haben. Das Eingriffsgewicht wird dadurch erhöht, dass die Datei auch den Informationsaustausch zwischen dem Verfassungsschutz und der Polizei ermöglicht.

Die Rechtsordnung unterscheidet zwischen einer grundsätzlich offen arbeitenden Polizei, die auf eine operative Aufgabenwahrnehmung ausgerichtet und von detaillierten Rechtsgrundlagen angeleitet ist, und den grundsätzlich verdeckt arbeitenden Verfassungsschutz, der auf die Beobachtung und Aufklärung im Vorfeld zur politischen Information und Beratung beschränkt ist und sich deswegen auf weniger ausdifferenzierte Rechtsgrundlagen stützen kann. Aus dem Grundrecht auf informationelle Selbstbestimmung folgt für den Datenaustausch zwischen diesen ein informationelles Trennungsprinzip. Soweit Daten zwischen den Nachrichtendiensten und Polizeibehörden für ein operatives Tätigwerden ausgetauscht werden, handelt es sich um einen besonders schweren Eingriff. Dieser ist nur ausnahmsweise zulässig und muss einem herausragenden öffentlichen Interesse dienen. Hierbei dürfen die jeweiligen Eingriffsschwellen für die Erlangung der Daten nicht unterlaufen werden.

Das Eingriffsgewicht wird jedoch dadurch gemindert, dass die Datei als Projektdaten gestaltet ist, die sich in ihrem Kern auf die Informationsanbahnung durch bereits erhobene Daten beschränkt. Für die Übermittlung der Daten zur operativen Aufgabenwahrnehmung ist das einschlägige Fachrecht maßgeblich, das seinerseits den verfassungsrechtlichen Anforderungen und dem informationellen Trennungsprinzip genügen muss.

Straftaten mit dem Gepräge geheimdienstlicher Agententätigkeit und der Bildung terroristischer Vereinigungen, wie sie diese Vorschrift zum Bezugspunkt hat, richten sich gegen die Grundpfeiler der verfassungsrechtlichen Ordnung und das Gemeinwesen als Ganzes. Es ist notwendig diese Straftaten mit den Mitteln des

Rechtsstaats zu bekämpfen. Diesen ist daher im Rahmen der Verhältnismäßigkeitsabwägung ein erhebliches Gewicht beizumessen.

Angesichts der sich gegenüberstehenden Interessen bestehen gegen die Grundstrukturen der Projektdatenbank keine verfassungsrechtlichen Bedenken. Dem Verhältnismäßigkeitsgrundsatz im engeren Sinne ist dadurch genüge getan, dass die Datenbank hinsichtlich der zu erfassenden Daten sowie deren Nutzungsmöglichkeiten normenklar und in der Sache hinreichend begrenzt ausgestaltet ist sowie hierbei qualifizierte Anforderungen an die Kontrolle gestellt und beachtet werden.

Voraussetzung der Errichtung einer gemeinsamen Projektdatenbank ist nach Absatz 1, dass das Projekt auf den Austausch und die gemeinsame Auswertung von polizeilichen oder nachrichtendienstlichen Erkenntnissen zu Straftaten der geheimdienstlichen Agententätigkeit (§ 99 StGB) oder der Bildung terroristischer Vereinigungen (§§ 129a und 129b StGB) sowie damit in einem unmittelbaren Zusammenhang stehenden Straftaten. Der Straftatenkatalog ist vor dem Hintergrund einer effektiven Aufklärung und Bekämpfung des internationalen Terrorismus und der geheimdienstlichen Agententätigkeit zu sehen, deren Gefahrenlagen vor dem Hintergrund der weltpolitischen Entwicklungen seit einigen Jahren erheblich angestiegen sind.

Mit dem Begriff der polizeilichen und nachrichtendienstlichen Erkenntnisse sind alle Erkenntnisse gemeint, die im Rahmen geltender Übermittlungsvorschriften zwischen den beteiligten Stellen ausgetauscht werden können. Der Begriff umfasst insoweit auch sogenannte Vorfelderkenntnisse.

Die Möglichkeiten zur Errichtung einer Projektdatenbank werden durch den Projektbezug begrenzt. Eine gemeinsame Projektdatenbank kommt nur bei einem klar definierten Projektauftrag in Betracht. Projektauftrag, Projektziele sowie die Verfahrensweise der beteiligten Stellen müssen zu Beginn des Projekts zwischen den beteiligten Stellen konkret vereinbart werden. Die Zusammenarbeit muss dem Austausch von Erkenntnissen im Hinblick auf die genannten Straftaten dienen.

Die beteiligten Stellen sind beim Austausch und der gemeinsamen Auswertung von Erkenntnissen an ihre jeweiligen gesetzlichen Aufgaben und Befugnisse gebunden.

Absatz 2 grenzt den Kreis der Personen und der Sachgegenstände der gemeinsamen Datenbank auf ein verfassungsrechtlich unbedenkliches Maß ein. Erfasst werden Personen, die eine geheimdienstliche Agententätigkeit nach § 99 des Strafgesetzbuchs ausüben, einer terroristischen Vereinigung nach § 129a des Strafgesetzbuchs, auch in Verbindung mit § 129b Absatz 1 des Strafgesetzbuchs angehören oder solche Personen oder Vereinigungen willentlich unterstützen. Weiterhin sind Kontakt- oder Begleitpersonen, Vereinigungen, Gruppierungen, Stiftungen, Unternehmen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüsse, Telekommunikationsendgeräte, Internetseiten oder Adressen für elektronische Post betroffen, bei denen tatsächliche Anhaltspunkte die Annahme begründen, dass sie im Zusammenhang mit einer dieser Personen stehen und durch sie Hinweise für die Verhütung, vorbeugende Bekämpfung oder Unterbindung von Straftaten nach Absatz 1 Satz 2 Nummer 1 bis 3 gewonnen werden können.

Absatz 3 regelt die Eingabe von Daten in die Projektdatei. Danach dürfen die an der Projektarbeit beteiligten Stellen die Daten nur dann in der gemeinsamen Datei speichern, wenn sie diese Daten allen an dem Projekt beteiligten Stellen nach den geltenden Übermittlungsvorschriften übermitteln dürfen. Eine Eingabe ist darüber hinaus nur zulässig, wenn die eingebende Stelle die Daten auch in eigenen Dateien speichern darf. Hiermit wird klargestellt, dass durch die Projektdatei nicht die für die jeweilige Stelle geltenden Speicherbefugnisse ausgedehnt werden. Die Grunddaten und die erforderlichenfalls erweiterten Grunddaten der Datei werden aufgeführt. Darüber hinaus werden auch Angaben zur Identifizierung der in Absatz 2 Nummer 2 genannten Kontakt- und Begleitpersonen, Vereinigungen, Gruppierungen, Stiftungen, Unternehmen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüsse, Telekommunikationsendgeräte, Internetseiten und Adressen für elektronische Post erfasst.

Absatz 4 enthält Regelungen zur datenschutzrechtlichen Verantwortung der eingebenden Stelle für die gemeinsame Projektdatei. Die eingebende Stelle muss im Hinblick auf die datenschutzrechtliche Verantwortung feststellbar sein. Die datenschutzrechtliche Verantwortung orientiert sich am sogenannten Besitzerprinzip und legt fest, dass sich die Änderung, Berichtigung, Sperrung und Löschung personenbezogener Daten nach den jeweils für die eingebende Stelle geltenden Vorschriften richtet.

Die Behördenleitung hat nach Absatz 5 für eine gemeinsame Datei ein Verzeichnis von Verarbeitungstätigkeiten nach § 37 Absatz 1 BbgPolG zu führen sowie im Einvernehmen mit dem Verfassungsschutz die jeweiligen Organisationseinheiten zu bestimmen, die zur Speicherung und zum Abruf befugt sind. Das Verzeichnis von Verarbeitungstätigkeiten bedarf der Zustimmung des für Inneres zuständigen Ministeriums.

Nach Absatz 6 haben das für Inneres zuständige Ministerium und die oder der Landesbeauftragte die Einhaltung der Regelungen zur Zusammenarbeit, zur Führung und zum Datenschutz der gemeinsamen Dateien zu überwachen. Sie überprüfen in regelmäßigen Abständen das Verzeichnis von Verarbeitungstätigkeiten einschließlich der Angaben, die die Feststellung der abgerufenen Datensätze sowie der verantwortlichen Stelle ermöglicht.

Nach Absatz 7 gilt zum Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung § 34 BbgPolG und für die Benachrichtigung der betroffenen Person § 35 BbgPolG.

Nach Absatz 8 ist eine Projektdatei auf höchstens zwei Jahre zu befristen. Da es sich um Dateien handelt, die der Unterstützung konkreter Projekte dienen, orientiert sich ihre Befristung an der voraussichtlichen Projektdauer und damit an der Erreichung des mit dem Projekt verfolgten Ziels. Auch hier besteht die Möglichkeit einer Verlängerung um jeweils bis zu einem Jahr mit einer Höchstfrist von 10 Jahren, wenn dies weiterhin für die Erreichung des Ziels erforderlich ist. Die Gründe für die Verlängerung sind entsprechend zu dokumentieren. Die 10-Jahresfrist trägt den sich längerfristig abspielenden Entwicklungstendenzen im Bereich der geheimdienstlichen Agententätigkeit und des Terrorismus Rechnung.

Zu § 67 (Berichtigung, Löschung und Sperrung von Daten)

Der neue § 67 BbgPolG übernimmt die Regelung des alten § 47 BbgPolG zur Berichtigung, Löschung und Sperrung von Daten. Es erfolgen einige grammatikalische und paragrafenverweisliche Anpassungen.

Zu Nummern 33 bis 35 (Vollzugshilfe)

Die neuen §§ 68 bis 70 BbgPolG in Kapitel 3 übernehmen die Vorschriften der alten §§ 50 bis 52 zur Vollzugshilfe.

In § 68 BbgPolG wird ein neuer Absatz 2 eingefügt. Soweit Dienstkräfte der Justizverwaltung nicht oder nicht ausreichend zur Verfügung stehen, führt die Polizei nunmehr Personen dem Gericht oder der Staatsanwaltschaft vor und unterstützt die Gerichtsvorsitzenden erforderlichenfalls bei der Aufrechterhaltung der Ordnung in der Sitzung. In § 69 Absatz 3 BbgPolG erfolgt eine Folgeanpassung.

Im Übrigen werden grammatikalische und paragrafenverweisliche Anpassungen vorgenommen.

Zu Nummern 36 bis 42 (Erzwingung von Handlungen, Duldungen und Unterlassungen)

Die neuen §§ 71 bis 77 BbgPolG in Kapitel 4 übernehmen die Vorschriften der alten §§ 53 bis 59 BbgPolG. Es erfolgen einige grammatikalische und paragrafenverweisliche Anpassungen.

Zu Nummern 43 bis 52 (Anwendung unmittelbaren Zwanges)

Die neuen §§ 78 bis 87 BbgPolG in Kapitel 4 übernehmen die Vorschriften der alten §§ 60 bis 69 BbgPolG. Es werden grammatikalische und paragrafenverweisliche Anpassungen vorgenommen.

In § 79 Absatz 2 BbgPolG wird klargestellt, dass neben Dienstfahrzeugen auch bemannte oder unbemannte Luftfahrzeuge Hilfsmittel der körperlichen Gewalt sein können. Absatz 3 wird um Sprengmittel, die vor Umsetzung von einem festen Mantel umgeben sind, erweitert. Dieses Zwangsmittel ist bereits im Bayerischen Polizeiaufgabengesetz geregelt. Im Polizeigesetz des Landes Nordrhein-Westfalen sind in den Fällen des Artikel 35 Absatz 2 Satz 1 oder des Artikel 91 Absatz 1 des Grundgesetzes für die Bundespolizei auch Handgranaten zugelassen. Auch das am 15. November 2017 beschlossene Gesetz zur Änderung des Polizeigesetzes in Baden-Württemberg sieht in einem neuen § 54a PolGBW eine ausdrückliche Regelung für den Gebrauch von Explosivmitteln vor. Die GSG 9 darf Schusswaffen, aus denen Sprenggeschosse verschossen werden können, und Explosivmittel einsetzen. § 2 Absatz 4 UZwG bestimmt, dass ausschließlich dienstlich zugelassene Schusswaffen zur Anwendung des unmittelbaren Zwangs eingesetzt und gebraucht werden dürfen. Die Berechtigung zum Gebrauch von Waffen für die Polizeivollzugsbeamten des Bundes ist in § 9 UZwG geregelt. Das Bundesministerium des Innern hat die Bewaffnung und die Ausbildung an Waffen in Abschnitt VI der Allgemeinen Verwaltungsvorschrift nach § 18 UZwG festgelegt. Im Land Brandenburg sind Sprengmittel nach § 61 Absatz 2 BbgPolG bislang nicht als Hilfsmittel der körperlichen Gewalt gegen Personen – insbesondere in Fällen des Terrorismus oder sonstiger Schwerstkriminalität – zugelassen.

Auf Grund neuer Bekämpfungsszenarien bei der Terrorismusabwehr, denen sich etwa bereits die Polizei in Frankreich und Belgien bei der Aushebung sogenannter

Terrorzellen konfrontiert sah, bedarf es für diese Waffen eine Regelung, die deren Einsatz im Ausnahmefall ermöglicht. Die Einsatzlagen in Verviers am 15. Januar 2015 und in Paris am 18. November 2015, bei denen gezielte Festnahmen von dringend Tatverdächtigen aus der islamistischen Terrorszene durch Spezialkräfte der Polizei erfolgen sollten, haben gezeigt, dass bei mit Schusswaffen und Sprengmittel schwer bewaffneten Personen Situationen entstehen können, in denen die Polizei beispielsweise Sprengmittel einsetzen muss. Damit ist es gelungen, die Personen zu binden und letztlich die Gefahren für die Einsatzkräfte der Polizei erheblich zu verringern. Ein hergebrachtes polizeitaktisches Vorgehen gegen entschlossene terroristische Gewalttäter hat keine hinreichende oder nur eine mit hohen Kosten verbundene Erfolgswahrscheinlichkeit. Es ist mit erheblichen Gefahren und Risiken für die Einsatzkräfte und Dritte verbunden und kann deren sicheren Tod oder schwerste Verletzungen mit sich bringen. Für solche Ausnahmefälle ist eine stärkere Bewaffnung der Polizei notwendig. Waffen können auf Anordnung des für Inneres zuständigen Ministeriums zeitlich befristet als Einsatzmittel erprobt werden.

Für die Anwendung von Sprengmitteln gegen Personen wird die Regelung des alten § 69 BbgPolG durch § 87 BbgPolG ersetzt. Zur unverzüglichen Abwehr einer Lebensgefahr für die Einsatzkräfte oder Dritte ist die Anwendung von Sprengmitteln gegen Personen das letzte Mittel. Durch den Einsatz dieser Waffen werden Personen erkennbar in ihrem Grundrecht auf Leib oder Leben gefährdet. Sprengmittel haben eine gewisse Streubreite, die sich durch den spezifischen Einsatz reduzieren lässt. Daraus ergeben sich gegenüber dem herkömmlichen Schusswaffengebrauch nochmals höhere Anforderungen, die sich in den Tatbestandsvoraussetzungen des § 87 BbgPolG widerspiegeln. Die engen Tatbestandsvoraussetzungen begrenzen die Verwendung dieser Waffen auf Ausnahmefälle.

§ Absatz 1 regelt die zielgerichtete Anwendung von Sprengmitteln gegen Personen unter engsten Voraussetzungen. So dürfen Sprengmittel nur durch Spezialeinheiten gegen Personen angewendet werden, wenn

- diese Personen Schusswaffen oder Sprengmittel mit sich führen,
- andere Waffen erfolglos angewendet wurden oder deren Gebrauch offensichtlich keinen Erfolg verspricht,
- eine Gefährdung unbeteiligter Personen mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden kann und
- der Einsatz von Sprengmitteln unerlässlich ist, um eine von den Personen ausgehende gegenwärtige konkrete Gefahr für das Leben der eingesetzten Polizeivollzugsbediensteten oder unbeteiligter Dritter abzuwehren.

Darüber hinaus gilt § 84 BbgPolG mit Ausnahme von Absatz 4 entsprechend. Damit sind die weiteren allgemeinen Vorschriften für den Schusswaffengebrauch auch auf den Gebrauch von Sprengmitteln gegen Personen anzuwenden. Die Voraussetzungen eines solchen Gebrauchs werden damit nochmals deutlich erhöht. Die Anwendung von Sprengmitteln ist spätestens unmittelbar nach dem Einsatz umfassend zu dokumentieren, damit dieser durch die Polizei oder im verwaltungsgerichtlichen Verfahren angemessen beurteilt werden kann.

Absatz 2 erklärt den Gebrauch von Sprengmitteln gegen Personen auf der Flucht oder in einer Menschenmenge ausnahmslos für unzulässig, weil deren Anwendung aufgrund ihrer radialen Wirkung erheblich schwieriger zu kalkulieren und zu kontrollieren ist als der herkömmliche Schusswaffeneinsatz. Darüber hinaus wird festgelegt, dass andere Sprengmittel als nach § 79 Absatz 3 BbgPolG nicht gegen Personen angewendet werden dürfen.

Die Anwendung von Sprengmitteln gegen Personen bedarf nach Absatz 3 der Anordnung der Behördenleitung und der Zustimmung des für Inneres zuständigen Ministeriums.

Zu Nummer 53 (Entschädigungsansprüche)

Der neue § 88 BbgPolG in Kapitel 5 zu den Entschädigungsansprüchen übernimmt die Regelung des alten § 70 BbgPolG.

Zu Nummer 54 (Auskunftsrecht, Akteneinsicht)

Das Kapitel 6 mit dem alten § 71 BbgPolG wird aufgehoben, weil diese Vorschrift in das Kapitel 2 Abschnitt 2 Unterabschnitt 1 überführt wurde.

Zu Nummern 55 bis 60 (Organisation und Zuständigkeit der Polizei, Polizeibeiräte)

Das bisherige Kapitel 7 wird Kapitel 6. Die neuen §§ 89 bis 95 BbgPolG regeln wie bisher die alten §§ 72 bis 86 BbgPolG die Organisation und Zuständigkeit der Polizei sowie die Polizeibeiräte. Es werden grammatikalische und paragrafenverweisliche Anpassungen vorgenommen.

Der neue § 92 BbgPolG übernimmt die Regelung des alten § 78 BbgPolG mit der Modifizierung, dass neben dem Polizeipräsidium auch der Zentraldienst der Polizei mit seiner Zentralen Bußgeldstelle für die Überwachung des Straßenverkehrs originär zuständig ist. Die Änderung ist notwendig, weil die Verkehrsunfallentwicklung in Brandenburg weiterhin nicht zufriedenstellend ist. Hauptursache bei schweren Verkehrsunfällen ist die überhöhte oder nicht angepasste Geschwindigkeit. Aufgrund des Personalmangels müssen zusätzliche Kräfte für die Kontrollen bereitgestellt werden. Das Polizeipräsidium ist zudem weiterhin zuständig für die Überwachung des Verkehrs auf schiffbaren Wasserstraßen. Die Überschrift der Vorschrift wird entsprechend angepasst.

Zu Nummern 61 bis 63 (Schlussvorschriften)

Das bisherige Kapitel 8 wird Kapitel 7. Die alten §§ 87 und 88 BbgPolG werden die neuen §§ 96 und 97 BbgPolG.

Der alte § 89 BbgPolG regelt in Bezug auf die Polizeistrukturereform aus dem Jahr 2011 als Übergangsvorschrift die weitere Tätigkeitsausübung und die Zuständigkeiten der zuvor bestehenden Polizeibeiräte bis zur Neubildung von Polizeibeiräten. Diese Übergangsphase ist durch die zwischenzeitlich erfolgte Neubildung von Polizeibeiräten abgeschlossen, so dass die Regelung nunmehr durch den neuen § 98 BbgPolG zum Opfer- und Zeugenschutz ersetzt wird.

Absatz 1 ermöglicht der Polizei zur Abwehr einer erheblichen konkreten Gefahr für

- gegenwärtige und mögliche zukünftige Opfer einer Straftat oder
- Zeugen, bei denen Maßnahmen nach dem Zeugenschutz-Harmonisierungsgesetz beendet wurden oder bei der erst nach rechtskräftigem Verfahrensabschluss Schutzmaßnahmen erforderlich werden,

auf Anordnung der Behördenleitung Urkunden und sonstige Dokumente zum Aufbau und zur Aufrechterhaltung einer vorübergehend geänderten Identität herzustellen, vorübergehend zu verändern und die entsprechend geänderten Daten zu verarbeiten. Dies kann beispielsweise für die Aufnahme eines Arbeitsverhältnisses oder für die Ein- oder Umschulung von Kindern notwendig sein. Personalausweise und Pässe dürfen dabei gemäß den bundesrechtlichen Vorschriften nicht für Personen ausgestellt werden, die nicht Deutsche im Sinne des Artikels 116 des Grundgesetzes sind. Die Tarnidentität kann sich ggf. auch auf Dateien und Register auswirken. Das Personenstandsregister muss aber richtig bleiben.

Die Personen nach Absatz 1 müssen für diese Schutzmaßnahmen geeignet sein. An der Eignung kann es etwa fehlen, wenn diese falsche Angaben machen, Zusagen nicht einhalten, zur Geheimhaltung nicht bereit sind, Straftaten begehen oder sich selbst wissentlich in Gefahr bringen oder nicht mit einer solchen Maßnahme nicht einverstanden ist. Die Geeignetheitsprüfung erfordert eine strukturierte Beurteilung der Gefährdungslage.

Der Aufbau einer vorübergehenden Tarnidentität im Bereich des operativen Opfer- und Zeugenschutzes in herausragenden Gefährdungslagen ist insbesondere bei der Bekämpfung der Organisierten und Politisch motivierten Kriminalität sehr wichtig. Entsprechende Vorschriften finden sich in § 5 des Zeugenschutz-Harmonisierungsgesetzes und in einigen Polizeigesetzen der Länder. Die Zusammenführung dieser Regelungen ermöglicht einen umfassenden Opfer- und Zeugeschutz.

Absatz 3 regelt, dass die zu schützenden Personen unter der vorübergehend geänderten Identität am Rechtsverkehr teilnehmen dürfen. Soweit erforderlich, können Maßnahmen nach Absatz 1 auch auf Angehörige dieser Personen oder ihr sonst nahestehende Personen erstreckt werden. Das kann etwa bei der Wohnsitzverlagerung einer ganzen Familie der Fall sein.

Absatz 4 ermöglicht durch Verweis auf § 52 Absatz 2 BbgPolG die Legendierung auch der zum Schutz der Person eingesetzten Polizeivollzugsbediensteten, soweit dies zur Vorbereitung, Durchführung, Lenkung oder Absicherung der Schutzmaßnahmen erforderlich ist. Offenes Auftreten der Polizeivollzugsbediensteten könnte die Aufmerksamkeit von Dritten wecken und zu einem Risiko für die zu schützenden Personen oder die Polizeivollzugsbediensteten werden.

Zu Artikel 2 (Änderung des Ordnungsbehördengesetzes)

In Nummer 1 wird im Inhaltsverzeichnis die Angabe zu § 2 OBG durch die Angabe „§ 2 Verhältnis zu anderen Behörden“ ersetzt. Dementsprechend wird in Nummer 2 die Paragrafenüberschrift des § 2 OBG angepasst. In Satz 1 wird die Angabe „§§ 50 bis 52“ durch die Angabe „§§ 68 bis 70“ ersetzt. Dem Satz 1 wird ein dem Artikel 1 Nummer 3 Buchstabe b entsprechender Satz zur vernetzten Zusammenarbeitspflicht der Ordnungsbehörden mit anderen Sicherheitsbehörden (Polizei, Verfassungsschutz, Staatsanwaltschaften und Ordnungsbehörden) angefügt.

Aufgrund der umfassenden Änderung im Brandenburgischen Polizeigesetz wird in der Nummer 3 der § 23 OBG zur Geltung des Brandenburgischen Polizeigesetzes neu gefasst und die Paragrafenverweise angepasst. Folgende Maßnahmen und Datenverarbeitungen können die Ordnungsbehörden entsprechend der Vorschriften des Brandenburgischen Polizeigesetzes durchführen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist:

- Befragung und Auskunftspflicht,
- Identitätsfeststellung,
- Prüfung von Berechtigungsscheinen und sonstigen Urkunden,
- Vorladung,
- Platzverweisung und Aufenthaltsverbot,
- Gewahrsam,
- Durchsuchung von Personen, Sachen und Wohnungen,
- Sicherstellung,
- Allgemeine Vorschriften zur Datenverarbeitung und zum Datenschutz,
- Allgemeine Befugnis zur Datenerhebung,
- Offene Bild- und Tonaufnahmen oder -aufzeichnungen,
- Allgemeine Regeln über die Dauer der Datenspeicherung,
- Zweckbindung bei der Datenspeicherung, Datenveränderung und Datennutzung,
- Speicherung, Veränderung und Nutzung von Daten,
- Datenübermittlung und
- Berichtigung, Löschung und Sperrung von Daten.

Es erfolgen zum Teil Einschränkungen für die Ordnungsbehörden bei den Befugnissen und den Maßnahmen der Datenverarbeitung, insbesondere bei der Identitätsfeststellung, dem Gewahrsam (z.B. vier Tagesfrist), der Durchsuchung von Wohnungen, bei den offenen Bild- und Tonaufnahmen oder -aufzeichnungen, den Vorschriften zur Speicherung, Veränderung und Nutzung von Daten sowie der Datenübermittlung.

Der reguläre Einsatz von Bodycams durch Ordnungsamtsbedienstete in den Städten, Gemeinden, Ämtern und Landkreisen hängt von der Zustimmung des für Inneres zuständigen Ministeriums und von einer zwei jährigen Pilotphase mit einer abschließenden Erforderlichkeitsanalyse unter dessen Aufsicht ab. Ist der Einsatz von Bodycams in einer Stadt, einer Gemeinde, einem Amt oder einem Landkreis erforderlich, so kann der regelmäßige Einsatz beginnen.

In Nummer 4 wird der § 43 OBG zur Einschränkung der Grundrechte neu gefasst. Hinzugefügt werden die Grundrechte auf

- Freizügigkeit (Artikel 11 des Grundgesetzes, Artikel 17 der Verfassung des Landes Brandenburg),
- Datenschutz (Artikel 11 der Verfassung des Landes Brandenburg) und
- Eigentum (Artikel 14 des Grundgesetzes, Artikel 41 Absatz 1 Satz 1 der Verfassung des Landes Brandenburg).

Zu Artikel 3 (Inkrafttreten)

Artikel 3 regelt den Zeitpunkt des Inkrafttretens des Gesetzes.