**LANDTAG DES SAARLANDES**
**16. Wahlperiode** **Drucksache 16/1180**
05.02.2020

# GESETZENTWURF

der Regierung des Saarlandes

betr.: Gesetz zur Neuregelung der polizeilichen Datenverarbeitung im Saarland

## A. Problem und Ziel

Die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 04.05.2016, S. 89) war bis zum 6. Mai 2018 in nationales Recht umzusetzen, eine Frist die nicht nur im Saarland nicht einzuhalten war und daher überschritten ist. Die Richtlinie, welche in quantitativer Hinsicht überwiegend die polizeiliche Verarbeitung personenbezogener Daten regelt, stellt jedoch nur einen Teilaspekt des gesetzgeberischen Handlungsbedarfs dar, welcher die umfassende Neuregelung der polizeilichen Datenverarbeitung bedingt: Die Vereinbarungen des Koalitionsvertrags, die Entscheidung des Bundesverfassungsgerichts zum BKA-Gesetz vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, erkannte Defizite im Hinblick auf polizeiliche Befugnisse, Forderungen aus der Praxis sowie des Unabhängigen Datenschutzzentrums (UDZ) stellen das Spannungsfeld dar, innerhalb dessen die polizeiliche Datenverarbeitung neu zu regeln ist. Auch die Umsetzung des Programms „Polizei 2020“ erfordert eine verfassungsgemäße und richtlinienkonforme Anpassung der Datenverarbeitungsnormen.
Mit dem vorliegenden Gesetzentwurf verfolgt die Landesregierung das Ziel, diese zum Teil konträr anmutenden Anforderungen zu normieren, um eine rechtssichere und zukunftsfähige Basis für die polizeiliche Datenverarbeitung zu schaffen.
Zu diesem Zweck wird in Artikel 1 das Saarländische Polizeigesetz dahingehend geändert, dass darin im Wesentlichen die Vorschriften zur Verarbeitung personenbezogener Daten gestrichen und erforderliche Anpassungen vorgenommen werden.
Artikel 2 sieht als völlig neues Normgefüge das Saarländische Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei vor. Da es sich hierbei um eine Vollregelung handelt, ist die gesamte von § 1 Absatz 1 umfasste polizeiliche Datenverarbeitung umfasst, anders als bisher stellt das Saarländische Datenschutzgesetz mithin keine Auffangregelung mehr dar.

Ausgegeben: 05.02.2020

Artikel 3 hebt die durch Artikel 2 obsolet gewordene Verordnung über die Zulassung der Übermittlung personenbezogener Daten von der Polizei an ausländische Polizeibehörden auf.
Artikel 4 setzt das Zitiergebot um und führt die durch dieses Gesetz eingeschränkten Grundrechte auf.

Artikel 5 enthält Übergangsregelungen, die im Wesentlichen dem Ziel dienen, die polizeiliche Datenverarbeitung sicherzustellen. Damit wird der Erfordernis Rechnung getragen, dass die Informationstechnik der Vollzugspolizei nur sukzessive weiterentwickelt bzw. ersetzt werden kann.

Artikel 6 regelt das Inkrafttreten.

## B. Lösung

Verabschiedung des Gesetzes zur Neuregelung der polizeilichen Datenverarbeitung im Saarland.

## C. Alternativen

Einstellung der Gesetzesinitiative und Entscheidung für den Beibehalt einer zum Teil europarechts- und verfassungswidrigen Rechtsgrundlage.

## D. Finanzielle Auswirkungen

### 1. Haushaltsausgaben ohne Vollzugsaufwand

Keine.

### 2. Vollzugsaufwand

Die Gesetzesänderung bewirkt infolge der zusätzlichen Dokumentationspflichten bei Verwaltungs- und Vollzugspolizei einen erhöhten initialen administrativen Aufwand, der zum Teil durch die Umsetzung der erforderlichen neuen Geschäftsprozesse kompensiert werden wird. Zusätzliche Verwaltungs- und Arbeitsanforderungen führen nicht zu einem zusätzlichen bezifferbaren Vollzugsaufwand und werden daher nicht haushaltswirksam.
Durch die Gesetzesänderung entstehen ferner keine direkten Kosten. Mittelbare Kosten, die infolge des Gesetzesvollzugs entstehen, etwa für Kennzeichenlesesysteme, Systeme zur elektronischen Aufenthaltsüberwachung, Jammer zur Unterdrückung von Mobilfunksignalen o. ä. können aktuell nicht identifiziert werden.
Auch die Höhe der auf Seiten der Justiz entstehenden Kosten durch die Stärkung des Richtervorbehalts kann zurzeit nicht seriös prognostiziert werden. Diesbezüglich kann sich finanzieller Nachsteuerungsbedarf ergeben, ebenso wie infolge der vorgesehenen Kennzeichnungs-, Dokumentations-, Protokollierungs-, Prüf- und Benachrichtigungspflichten sowie durch die Berichtigungs-, Hinweis- und Berichtspflichten gegenüber Betroffenen.
Weiterer – mittelbarer – finanzieller Bedarf wird entstehen durch die Ertüchtigung der IT-Infrastruktur des Bundeskriminalamtes und die in Folge notwendige Anpassung der IT des Landespolizeipräsidiums. Für die investiven Kosten ist bereits Haushaltsvorsorge getroffen, wenngleich sich die Höhe des entsprechenden Aufwandes zurzeit nicht verlässlich prognostizieren lässt. Hinzu tritt das ohnehin volatile Preisgefüge

## E. Sonstige Kosten

Nicht ersichtlich.

## F. Auswirkungen von frauenpolitischer Bedeutung

## G. Federführende Zuständigkeit

Die Federführung liegt beim Ministerium für Inneres, Bauen und Sport.

# G e s e t z

## zur Neuregelung der polizeilichen Datenverarbeitung im Saarland[1]

**Vom**

Der Landtag wolle beschließen:

### Artikel 1
### Änderung des Saarländischen Polizeigesetzes

Das Saarländische Polizeigesetz in der Fassung der Bekanntmachung vom 26. März 2001 (Amtsbl. S. 1074), zuletzt geändert durch das Gesetz vom 22. August 2018 (Amtsbl. I S. 674, 681), wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

   a) Die Angabe zu § 12 wird wie folgt gefasst:
   „§ 12 Platzverweisung, Wohnungsverweisung, Aufenthaltsverbot, Kontaktverbot, Aufenthaltsgebot“

   b) Die Angaben zu den Paragrafen 26 bis 40 werden gestrichen.

2. In § 7 werden die Wörter „Fernmeldegeheimnis (Art. 10 des Grundgesetzes)“ gestrichen.

3. In § 8 Absatz 1 wird die Angabe „40“ durch die Angabe „25“ ersetzt.

4. In § 9a Absatz 3 wird die Angabe „gilt § 30“ durch die Wörter „gelten § 21 und § 23 des Saarländischen Gesetzes über die Verarbeitung personenbezogener Daten durch die Polizei“ [**einsetzen: Datum des Gesetzes**] ersetzt.

5. In § 11 Absatz 2 Nummer 2 und Absatz 4 Nummer 2 wird hinter dem Wort „Maßnahmen“ jeweils „oder einer elektronischen Aufenthaltsüberwachung“ ergänzt.

6. § 12 wird wie folgt geändert:

   a) Die Überschrift wird wie folgt gefasst:
   „§ 12 Platzverweisung, Wohnungsverweisung, Aufenthaltsverbot, Kontaktverbot, Aufenthaltsgebot“

   b) Nach Absatz 3 wird folgender Absatz 4 angefügt:

   „(4) [1]Zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person kann die Vollzugspolizei einer Person verbieten,
   1. zu einer bestimmten Person oder zu Angehörigen einer bestimmten Gruppe den Kontakt zu suchen oder aufzunehmen (Kontaktverbot) oder
   2. ein bestimmtes Gebiet zu verlassen (Aufenthaltsgebot).

[1] Dieses Gesetz dient der Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 04.05.2016, S. 89).

[2]Eine Maßnahme nach Satz 1 ist auch zulässig, wenn

1. bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat nach § 100a Absatz 1 Nummer 1 in Verbindung mit § 100a Absatz 2 der Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S 1074, 1319), zuletzt geändert durch Artikel 1 des Gesetzes vom 20. November 2019 (BGBl. I S. 1724), in der jeweils geltenden Fassung begehen wird, oder
2. das individuelle Verhalten dieser Person die konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb eines übersehbaren Zeitraums eine in § 129a Absatz 1 und 2 des Strafgesetzbuchs in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 1 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618), in der jeweils geltenden Fassung bezeichnete Straftat begehen wird.

[3]Eine Maßnahme nach Satz 1 oder 2 darf nur durch die Richterin oder den Richter angeordnet werden; § 20 Absatz 1 Satz 2 und 3 gilt entsprechend. [4]Die Anordnung ist auf höchstens drei Monate zu befristen. [5]Soweit die Voraussetzungen der Anordnung fortbestehen, sind auf Antrag jeweils Verlängerungen bis zu drei Monaten zulässig. [6]Bei Gefahr im Verzug kann die Anordnung durch die Behördenleiterin oder den Behördenleiter oder eine von ihr oder ihm beauftragte Beamtin oder einen beauftragten Beamten getroffen werden. [7]Die Anordnung nach Satz 6 tritt außer Kraft, wenn sie nicht binnen drei Tagen von der Richterin oder dem Richter bestätigt wird. [8]Wird ein Kontaktverbot nach Satz 1 Nummer 1 im Rahmen einer Wohnungsverweisung nach Absatz 2 Satz 1 ausgesprochen, kann die Anordnung auch durch eine Beamtin oder Beamten der Vollzugspolizei erfolgen; Absatz 2 Satz 4 bis 6 gelten entsprechend.“

7. In § 25 werden die Absätze 1 bis 5 aufgehoben und durch folgende Regelung ersetzt:

   „Die Polizei darf, soweit gesetzlich nichts anderes geregelt ist, personenbezogene Daten nur nach Maßgabe des Saarländischen Gesetzes über die Verarbeitung personenbezogener Daten durch die Polizei vom [**einsetzen: Datum des Gesetzes**] in der jeweils geltenden Fassung verarbeiten.“

8. Die §§ 26 bis 40 werden aufgehoben.

## Artikel 2
## Saarländisches Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG)

### Erster Teil
### Allgemeine Bestimmungen

#### 1. Abschnitt
#### Anwendungsbereich, Begriffsbestimmungen und Allgemeine Grundsätze



#### 2. Abschnitt
#### Datenschutzkontrolle



#### 3. Abschnitt
#### Rechte der betroffenen Person



### Zweiter Teil
### Rechtsgrundlagen der Verarbeitung personenbezogener Daten

**Dritter Teil**
**Besondere Befugnisse zur Verarbeitung personenbezogener Daten**



**Vierter Teil**
**Übermittlung personenbezogener Daten**

**1. Abschnitt**
**Allgemeine Regelungen**



**2. Abschnitt**
**Grenzüberschreitender Datenverkehr innerhalb der Europäischen Union**



**3. Abschnitt**
**Datenübermittlungen an Drittstaaten und an internationale Organisationen**

## Fünfter Teil
## Besondere Regelungen für die Verarbeitung personenbezogener Daten und die Auftragsverarbeitung

### 1. Abschnitt
### Allgemeine Vorschriften



### 2. Abschnitt
### Auftragsverarbeitung



### 3. Abschnitt
### Sicherheit und Schutz personenbezogener Daten



## Sechster Teil
## Schlussvorschriften

# Erster Teil
# Allgemeine Bestimmungen

## 1. Abschnitt
## Anwendungsbereich, Begriffsbestimmungen und Allgemeine Grundsätze

### § 1 Anwendungsbereich

(1) Die Vorschriften dieses Gesetzes gelten für die Verarbeitung personenbezogener Daten durch die Polizei im Sinne des § 1 Absatz 1 des Saarländischen Polizeigesetzes in der Fassung der Bekanntmachung vom 26. März 2001 (Amtsbl. S. 1074), zuletzt geändert durch Artikel 1 des Gesetzes vom 15. März 2017 (Amtsbl. I S. 486), in der jeweils geltenden Fassung zum Zweck der Verhütung, Aufdeckung, Ermittlung Verfolgung und Ahndung von Straftaten oder Ordnungswidrigkeiten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung.
(2) Die Bestimmungen der §§ 9, 9a, 10, 10a, 11, 17a des Saarländischen Polizeigesetzes und anderer spezieller Rechtsvorschriften bleiben davon unberührt.
(3) Für die Verarbeitung personenbezogener Daten durch die Polizei, die weder in den Anwendungsbereich des Absatzes 1 fällt, noch durch spezielle Rechtsvorschriften im Sinne des Absatzes 2 geregelt ist, gelten die Vorschriften der Verordnung (EU) 2016/679 (Datenschutzgrundverordnung) sowie das zu deren Umsetzung erlassene Saarländische Datenschutzgesetz vom 16. Mai 2018 (Amtsbl. I S. 254) in der jeweils geltenden Fassung.

### § 2 Begriffsbestimmungen

(1) [1]Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen. [2]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 Person sind, identifiziert werden kann.
(2) [1]Verarbeitung stellt jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten dar. [2]Die Verarbeitung personenbezogener Daten umfasst insbesondere das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
(3) Einschränkung der Verarbeitung ist die Kennzeichnung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.
(4) Profiling umfasst jede Art der automatisierten Verarbeitung personenbezogener Daten, bei der diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte der Arbeitsleistung, der wirtschaftlichen Lage, der Gesundheit, der persönlichen Vorlieben, der Interessen, der Zuverlässigkeit, des Verhaltens, der Aufenthaltsorte oder der Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.
(5) Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, in der die 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 Daten keiner betroffenen Person zugewiesen werden können.
(6) Anonymisierung ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
(7) Ein Dateisystem ist 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.
(8) Verantwortlicher im Sinne des Artikels 3 Nummer 8 und des Artikels 19 der Richtlinie (EU) 2016/680 ist die zuständige Polizeibehörde, die Aufgaben nach § 1 Absatz 1 dieses Gesetzes wahrnimmt, soweit sie allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
(9) Auftragsverarbeiter ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag der oder des Verantwortlichen verarbeitet.
(10) Empfängerin oder Empfänger ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um eine Dritte oder einen Dritten handelt oder nicht; Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder anderen Rechtsvorschriften personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.
(11) Verletzung des Schutzes personenbezogener Daten ist jede Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten geführt hat, die verarbeitet wurden.
(12) Genetische Daten sind personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser Person liefern, insbesondere solche, die aus der Analyse einer biologischen Probe der Person gewonnen wurden.
(13) Biometrische Daten sind mittels spezieller technischer Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, insbesondere Gesichtsbilder oder daktyloskopische Daten.
(14) Gesundheitsdaten sind 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.
(15) Besondere Kategorien personenbezogener Daten umfassen

1. Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,
2. genetische Daten,
3. biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
4. Gesundheitsdaten und
5. Daten zum Sexualleben oder zur sexuellen Orientierung.

(16) Aufsichtsbehörde ist die von einem Mitgliedstaat gemäß Artikel 41 der Richtlinie (EU) 2016/680 eingerichtete unabhängige staatliche Stelle.
(17) Internationale Organisation ist jede völkerrechtliche Organisation und ihre nachgeordneten Stellen sowie jede sonstige Einrichtung, die durch eine von zwei oder mehr Staaten geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

(18) Die Einwilligung stellt eine freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung dar in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.
(19) Grunddaten einer Person im Sinne dieses Gesetzes sind insbesondere:

1. Familienname,
2. Vornamen,
3. Geburtsnamen,
4. Familienstand,
5. erlernter Beruf,
6. ausgeübte Tätigkeit
7. Geburtsdatum,
8. Geburtsort einschließlich Kreis,
9. aktuelle Staatsangehörigkeit und frühere Staatsangehörigkeiten,
10. gegenwärtiger Aufenthaltsort und frühere Aufenthaltsorte,
11. Wohnanschrift sowie
12. der Kontaktaufnahme dienende Daten und Telefon- und Telefaxnummern.

## § 3 Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

(1) Die Polizei darf personenbezogene Daten nur zu den in § 1 Absatz 1 dieses Gesetzes genannten Zwecken verarbeiten.
(2) [1]Personenbezogene Daten müssen

1. auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,
2. für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,
3. dem Verarbeitungszweck entsprechen, für das Erreichen des Verarbeitungszwecks erforderlich sein und ihre Verarbeitung nicht außer Verhältnis zu diesem Zweck stehen,
4. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden,
5. nicht länger als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, und
6. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet; hierzu gehört auch ein durch geeignete technische und organisatorische Maßnahmen zu gewährleistender Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

[2]Die Polizei ist für die Einhaltung dieser Grundsätze verantwortlich und muss deren Einhaltung nachweisen können.
(3) [1]Personenbezogene Daten sind grundsätzlich bei der betroffenen Person zu erheben. [2]Sie können bei anderen Behörden, öffentlichen Stellen oder bei Dritten erhoben werden, wenn sonst die Erfüllung polizeilicher Aufgaben erheblich erschwert oder gefährdet würde.
(4) [1]Personenbezogene Daten sind offen zu erheben. [2]Eine Erhebung personenbezogener Daten, die nicht als polizeiliche Maßnahme erkennbar sein soll, ist nur soweit zulässig, als auf andere Weise die Erfüllung polizeilicher Aufgaben erheblich gefährdet würde, wenn anzunehmen ist, dass dies überwiegenden Interessen der betroffenen Person entspricht oder auf Grundlage eines Gesetzes.

(5) [1]Werden personenbezogene Daten bei der betroffenen Person oder bei Dritten erhoben, sind diese auf Verlangen auf die Rechtsgrundlage für die Erhebung personenbezogener Daten oder auf die Freiwilligkeit ihrer Auskunft hinzuweisen. [2]§ 136a der Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Artikel 1 des Gesetzes vom 20. November 2019 (BGBl. I S. 1724), in der jeweils geltenden Fassung gilt entsprechend. [3]Die betroffene Person kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihr oder ihm selbst oder einem der in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen die Gefahr zuziehen würde, wegen einer Straftat oder einer Ordnungswidrigkeit verfolgt zu werden. [4]Zur Verweigerung der Auskunft sind ferner die in §§ 53 und 53a der Strafprozessordnung genannten Personen nach Maßgabe dieser Vorschriften berechtigt. [5]Die betroffene Person ist über ihr Recht zur Verweigerung der Auskunft zu belehren.

## 2. Abschnitt
## Datenschutzkontrolle

### § 4 Aufsichtsbehörde

Die oder der Landesbeauftragte für Datenschutz ist Aufsichtsbehörde gemäß Artikel 41 der Richtlinie (EU) 2016/680 bei der Verarbeitung personenbezogener Daten nach diesem Gesetz. Sie oder er überwacht die Anwendung dieses Gesetzes und sonstiger Rechtsvorschriften zum Schutz personenbezogener Daten durch die Polizei sowie deren Auftragsverarbeiter.

### § 5 Aufgaben der Aufsichtsbehörde

(1) Der oder dem Landesbeauftragten für Datenschutz obliegen nach Artikel 46 der Richtlinie (EU) 2016/680 die Aufgaben,

1. die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der sonstigen zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, auf ihre Rechtmäßigkeit hin zu überprüfen, zu überwachen und durchzusetzen,
2. die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und sie darüber aufzuklären, wobei spezifische Maßnahmen für Kinder besondere Beachtung finden,
3. den Landtag des Saarlandes und die Landesregierung sowie weitere andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten,
4. die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus diesem Gesetz und sonstigen Rechtsvorschriften zur Umsetzung der Richtlinie (EU) 2016/680 entstehenden Pflichten zu sensibilisieren,
5. auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieses Gesetzes und sonstiger Rechtsvorschriften zur Umsetzung der Richtlinie (EU) 2016/680 zur Verfügung zu stellen und gegebenenfalls zu diesem Zweck mit anderen Aufsichtsbehörden der Bundesrepublik Deutschland und der anderen Mitgliedstaaten der Europäischen Union zusammenzuarbeiten,

6. sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes nach Artikel 55 der Richtlinie (EU) 2016/680 oder § 13 dieses Gesetzes zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist,
7. mit anderen Aufsichtsbehörden der Bundesrepublik Deutschland und der anderen Mitgliedstaaten der Europäischen Union zusammenzuarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe zu leisten, um die einheitliche Anwendung und Durchsetzung dieses Gesetzes und sonstiger Rechtsvorschriften zur Umsetzung der Richtlinie (EU) 2016/680 zu gewährleisten,
8. Untersuchungen über die Anwendung dieses Gesetzes und sonstiger Rechtsvorschriften zur Umsetzung der Richtlinie (EU) 2016/680 durchzuführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde,
9. maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken und
10. Beratung in Bezug auf die in § 59 genannten Verarbeitungsvorgänge zu leisten.

(2) Die oder der Landesbeauftragte für Datenschutz führt Kontrollen bezüglich der Datenverarbeitung bei den in § 42 Absatz 1 und 2 genannten Maßnahmen mindestens alle zwei Jahre durch.

(3) [1]Die oder der Landesbeauftragte für Datenschutz legt dem Landtag des Saarlandes und der Landesregierung jährlich einen Bericht über ihre oder seine Tätigkeit vor. [2]Die Landesregierung legt hierzu dem Landtag des Saarlandes innerhalb von drei Monaten eine Stellungnahme vor. [3]Dieser macht sowohl den Tätigkeitsbericht als auch die Stellungnahme der Landesregierung öffentlich zugänglich.

## § 6 Befugnisse der Aufsichtsbehörde

(1) Die oder dem Landesbeauftragten für Datenschutz ist berechtigt, von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten, die verarbeitet werden, und auf alle Informationen, die zur Erfüllung ihrer oder seiner Aufgaben notwendig sind, zu erhalten.

(2) [1]Sofern die oder der Landesbeauftragte für Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Schutz personenbezogener Daten oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten festgestellt und beanstandet hat, kann sie oder er geeignete Maßnahmen anordnen, wenn dies zur Beseitigung eines Verstoßes gegen datenschutzrechtliche Vorschriften erforderlich ist. [2]Dabei kann sie oder er insbesondere

1. einen Verantwortlichen oder einen Auftragsverarbeiter warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen datenschutzrechtliche Vorschriften verstoßen,
2. den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums, mit den datenschutzrechtlichen Vorschriften in Einklang zu bringen, insbesondere durch die Anordnung der Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung,
3. im Einvernehmen mit den nach Satz 3 Nummer 1 bis 3 jeweils zuständigen Stellen eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, verhängen.

[3]Die Beanstandung richtet sich an den Verantwortlichen und kann mit der Aufforderung verbunden werden, innerhalb einer bestimmten Frist Stellung zu nehmen. Gleichzeitig sind bei Verstößen

1. der Vollzugspolizei das Ministerium für Inneres, Bauen und Sport,
2. der allgemeinen Polizeiverwaltungsbehörden die in § 77 Absatz 2 des Saarländischen Polizeigesetzes genannten zuständigen Ministerien als Fachaufsichtsbehörden,
3. einer Sonderpolizeibehörde im Sinne des § 75 Absatz 3 des Saarländischen Polizeigesetzes die jeweils zuständige Landespolizeibehörde nach § 76 Absatz 1 des Saarländischen Polizeigesetzes

zu unterrichten.

(3) Für den Rechtsschutz gegen Maßnahmen oder verbindliche Entscheidungen der oder des Landesbeauftragten für Datenschutz gilt § 14 entsprechend.

## § 7 Gegenseitige Amtshilfe

(1) *[1]*Die oder der Landesbeauftragte für Datenschutz hat den Datenschutzaufsichtsbehörden der Bundesrepublik Deutschland und der anderen Mitgliedstaaten der Europäischen Union Informationen zu übermitteln und Amtshilfe zu leisten, soweit dies für eine einheitliche Umsetzung und Anwendung der Richtlinie (EU) 2016/680 erforderlich ist. *[2]*Die Amtshilfe betrifft insbesondere Auskunftsersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um Konsultation oder um Vornahme von Nachprüfungen und Untersuchungen.

(2) Die oder der Landesbeauftragte für Datenschutz hat alle geeigneten Maßnahmen zu ergreifen, um Amtshilfeersuchen unverzüglich und spätestens innerhalb eines Monats nach deren Eingang nachzukommen.

(3) Die oder der Landesbeauftragte für Datenschutz darf Amtshilfeersuchen nur ablehnen, wenn

1. sie oder er für den Gegenstand des Ersuchens oder für die Maßnahmen, die sie oder er durchführen soll, nicht zuständig ist oder
2. ein Eingehen auf das Ersuchen gegen Rechtsvorschriften verstoßen würde.

(4) [1]Die oder der Landesbeauftragte für Datenschutz hat die ersuchende Aufsichtsbehörde über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen zu informieren, die getroffen wurden, um dem Amtshilfeersuchen nachzukommen. *[2]*Sie oder er hat im Fall des Absatzes 3 die Gründe für die Ablehnung des Ersuchens zu erläutern.

(5) Die oder der Landesbeauftragte für Datenschutz hat die Informationen, um die sie oder er von der Aufsichtsbehörde ersucht wurde, in der Regel elektronisch und in einem standardisierten Format zu übermitteln.

(6) Die oder der Landesbeauftragte für Datenschutz hat Amtshilfeersuchen kostenfrei zu erledigen, soweit sie oder er nicht im Einzelfall mit der ersuchenden Aufsichtsbehörde die Erstattung entstandener Ausgaben vereinbart hat.

(7) *[1]*Ein Amtshilfeersuchen der oder des Landesbeauftragte für Datenschutz hat alle erforderlichen Informationen zu enthalten; hierzu gehören insbesondere der Zweck und die Begründung des Ersuchens. *[2]*Die auf das Ersuchen übermittelten Informationen dürfen ausschließlich zu dem Zweck verwendet werden, zu dem sie angefordert wurden.

## § 8 Datenschutzbeauftragte

(1) [1]Jede Polizeibehörde hat eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten schriftlich zu benennen. [2]Diese müssen für ihre Tätigkeit geeignet sein, insbesondere über die erforderliche Zuverlässigkeit und Sachkunde verfügen. [3]Hierzu können auch Datenschutzbeauftragte benannt werden, die nach der Verordnung (EU) 2016/679 benannt sind. [4]Die oder der Datenschutzbeauftragte ist im Rahmen ihrer oder seiner Aufgabenerfüllung unmittelbar der Behördenleitung unterstellt. [5]In ihrer oder seiner Funktion ist die oder der Datenschutzbeauftragte weisungsfrei. [6]Sie oder er kann sich unmittelbar an die Landesbeauftragte oder den Landesbeauftragten für Datenschutz wenden. [7]Die oder der Datenschutzbeauftragte darf wegen der Erfüllung ihrer oder seiner Aufgaben nicht benachteiligt werden. [8]Soweit erforderlich, ist sie oder er von anderen Tätigkeiten frei zu stellen und mit räumlichen, sachlichen und personellen Mitteln auszustatten. [9]Zum Erwerb und zum Erhalt der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde sind die Teilnahme an Fort- und Weiterbildungsmaßnahmen zu ermöglichen und deren Kosten zu übernehmen.

(2) [1]Die oder der Datenschutzbeauftragte hat den Verantwortlichen bei der Ausführung datenschutzrechtlicher Vorschriften zu unterstützen und auf deren Einhaltung hinzuwirken, dabei ist er oder sie ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubeziehen. [2]Zu den Aufgaben der oder des Datenschutzbeauftragten zählen insbesondere:

1. Unterrichtung und Beratung der jeweiligen Polizeibehörde und der Beschäftigten, die personenbezogene Daten verarbeiten, hinsichtlich ihrer Pflichten nach diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften,
2. Überwachung der Einhaltung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, sowie der Strategie der jeweiligen Polizeibehörde für den Schutz personenbezogener Daten, einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und der Schulung der Beschäftigten und der diesbezüglichen Überprüfungen,
3. Zusammenarbeit mit der Aufsichtsbehörde und Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in Fragen der Verarbeitung personenbezogener Daten, einschließlich der vorherigen Konsultation gemäß § 59 Absatz 1 dieses Gesetzes,
4. Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß § 55 dieses Gesetzes,
5. Unterstützung der verantwortlichen Stelle bei dem Erarbeiten technischer und organisatorischer Maßnahmen nach § 53 und § 58 dieses Gesetzes.

[3]Sie oder er kann zu ihrer oder seiner Aufgabenerfüllung jederzeit Einsicht in die Verarbeitung personenbezogener Daten der verantwortlichen Stelle nehmen, soweit dem nicht gesetzliche Regelungen entgegenstehen.

(3) [1]Bedienstete der Polizei und von der Verarbeitung ihrer personenbezogenen Daten durch die Polizei betroffene Personen können sich in datenschutzrechtlichen Fragen jederzeit an die Datenschutzbeauftragte oder den Datenschutzbeauftragten wenden. [2]Diese oder dieser ist verpflichtet, über die ihr oder ihm bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. [3]Satz 2 gilt nicht für Mitteilungen im dienstlichen Verkehr oder von Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. [4]Die oder der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf die betroffene Person zulassen, verpflichtet, soweit sie oder er nicht durch die betroffene Person hiervon befreit wird.

## 3. Abschnitt Rechte der betroffenen Person

### § 9 Allgemeine Informationen zu Datenverarbeitungen

Die Polizei hat in allgemeiner Form und für jedermann zugänglich Informationen zur Verfügung zu stellen über

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

### § 10 Benachrichtigung der betroffenen Person

(1) Ist die Benachrichtigung der betroffenen Person über die Verarbeitung sie betreffender personenbezogener Daten in speziellen Rechtsvorschriften, insbesondere bei verdeckten Maßnahmen, vorgesehen oder angeordnet, so hat diese Benachrichtigung zumindest die folgenden Angaben zu enthalten:

1. die in § 9 genannten Angaben,
2. die Rechtsgrundlage der Verarbeitung,
3. die für die personenbezogenen Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
4. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten sowie
5. erforderlichenfalls weitere Informationen, insbesondere, wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden.

(2) In den Fällen des Absatzes 1 kann die Polizei die Benachrichtigung insoweit und solange aufschieben, einschränken oder unterlassen, wenn die Erfüllung der in § 1 Absatz 1 genannten Aufgaben ansonsten gefährdet wäre und das Interesse an der Vermeidung dieser Gefahren das Informationsinteresse der betroffenen Person überwiegt.

(3) Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an die Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst oder ist die Sicherheit eines Landes oder des Bundes berührt, ist sie nur mit Zustimmung der jeweils zuständigen Stellen zulässig.

(4) Im Fall der Einschränkung nach Absatz 2 gilt § 11 Absatz 7 und 8 entsprechend.

(5) [1]Personen, gegen die sich eine verdeckte Datenerhebung nach Maßgabe der § 31, §§ 34 bis 36 und § 40 richtet, sind nach Abschluss der Maßnahme hierüber zu benachrichtigen. [2]Dabei ist die betroffene Person auch über die Tatsache der Erhebung, Speicherung und Löschung von personenbezogenen Daten aus dem Kernbereich der privaten Lebensgestaltung nach § 41 Absatz 3 zu unterrichten. [3]Auf die Möglichkeit nachträglichen Rechtsschutzes ist hinzuweisen. [4]Sonstige betroffene Personen sind nach Maßgabe der Sätze 1 bis 3 zu unterrichten, soweit eine Datenerhebung nach § 34 erfolgt ist oder andere besonders schutzwürdige Interessen dies erfordern. [5]Die Unterrichtung nach den Sätzen 1 oder 4 kann zurückgestellt werden, soweit Leib, Leben oder Freiheit einer Person, besondere Vermögenswerte oder der Zweck der Maßnahme gefährdet werden. [6]Wird die Unterrichtung nach Satz 5 zurückgestellt, sind die Gründe aktenkundig zu machen. [7]Erfolgt die Benachrichtigung nicht binnen zwölf Monate nach Beendigung der Maßnahme, bedürfen jegliche weiteren Zurückstellungen der gerichtlichen Zustimmung; zuständig ist das Gericht, welches die Maßnahme angeordnet hat.

[8]Bedurfte die Maßnahme nicht der richterlichen Anordnung, ist für die Zustimmung das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat, zuständig. [9]Das Gericht bestimmt die Dauer weiterer Zurückstellungen. [10]Es kann dem endgültigen Absehen von der Benachrichtigung zustimmen, wenn die Voraussetzungen für eine Zurückstellung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft weiter vorliegen werden. [10]Sind mehrere Maßnahmen in einem engen zeitlichen Zusammenhang durchgeführt worden, so beginnt die in Satz 7 genannte Frist mit der Beendigung der letzten Maßnahme.

(6) Eine Unterrichtung nach Absatz 5 unterbleibt, soweit

1. sich an den die Maßnahme auslösenden Sachverhalt ein strafrechtliches Ermittlungsverfahren gegen den Betroffenen anschließt,
2. zu ihrer Durchführung in unverhältnismäßiger Weise weitere Daten über die betroffene Person erhoben werden müssten und dies im Interesse der betroffenen Person nicht geboten erscheint oder
3. schutzwürdige Belange anderer Personen entgegenstehen.

## § 11 Auskunftsrecht der betroffenen Person

(1) [1]Die Polizei hat der betroffenen Person auf Antrag Auskunft darüber zu erteilen, ob sie Daten der betroffenen Person verarbeitet. [2]Die betroffene Person hat darüber hinaus das Recht, Informationen zu erhalten über

1. die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, und die Kategorie, zu der sie gehören,
2. die verfügbaren Informationen über die Herkunft der Daten,
3. die Zwecke der Verarbeitung und deren Rechtsgrundlage,
4. die Empfänger oder die Kategorien von Empfängern, gegenüber denen die Daten offengelegt worden sind, insbesondere bei Empfängern in Nicht-Mitgliedstaaten der Europäischen Union (Drittstaaten) oder bei internationalen Organisationen,
5. die für die personenbezogenen Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
6. das Bestehen eines Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung der Daten durch den Verantwortlichen, sowie
7. das Recht, die oder den Landesbeauftragten für Datenschutz anzurufen, sowie
8. Angaben zur Erreichbarkeit der oder des Landesbeauftragten für Datenschutz.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb verarbeitet werden, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder die ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(3) Von der Auskunftserteilung kann abgesehen werden, wenn die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen, und deshalb der für die Erteilung der Auskunft erforderliche Aufwand außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

(4) Die Polizei kann unter den Voraussetzungen des § 10 Absatz 2, 5 oder 6 von der Auskunft nach Absatz 1 Satz 1 absehen oder die Auskunftserteilung nach Absatz 1 Satz 2 teilweise oder vollständig einschränken.

(5) § 10 Absatz 3 gilt entsprechend.

(6) [1]Die Polizei hat die betroffene Person über das Absehen von oder die Einschränkung einer Auskunft unverzüglich schriftlich zu unterrichten. [2]Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 10 Absatz 2, 5 oder 6 mit sich bringen würde. [3]Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von oder der Einschränkung der Auskunft verfolgten Zweck gefährden würde.

(7) [1]Wird die betroffene Person nach Absatz 6 über das Absehen von oder die Einschränkung der Auskunft unterrichtet, kann sie ihr Auskunftsrecht auch über die Landesbeauftragte oder den Landesbeauftragten für Datenschutz ausüben. [2]Die Polizei hat die betroffene Person über diese Möglichkeit sowie darüber zu unterrichten, dass sie die oder den Landesbeauftragten für Datenschutz anrufen oder gerichtlichen Rechtsschutz suchen kann. [3]Macht die betroffene Person von ihrem Recht nach Satz 1 Gebrauch, ist die Auskunft auf ihr Verlangen der oder dem Landesbeauftragten für Datenschutz zu erteilen, soweit nicht das Ministerium für Inneres, Bauen und Sport im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. [4]Die oder der Landesbeauftragte für Datenschutz hat die betroffene Person zumindest darüber zu unterrichten, dass alle erforderlichen Prüfungen erfolgt sind oder eine Überprüfung durch sie stattgefunden hat. [5]Diese Mitteilung kann die Information enthalten, ob datenschutzrechtliche Verstöße festgestellt wurden. [6]Die Mitteilung der oder des Landesbeauftragten für Datenschutz an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand der Polizei zulassen, sofern diese keiner weitergehenden Auskunft zustimmt. [7]Die Polizei darf die Zustimmung nur insoweit und solange verweigern, wie sie nach Absatz 4 von einer Auskunft absehen oder sie einschränken könnte. [8]Die oder der Landesbeauftragte für Datenschutz hat zudem die betroffene Person über ihr Recht auf gerichtlichen Rechtsschutz zu unterrichten.
(8) Die Polizei hat die sachlichen oder rechtlichen Gründe für die Entscheidung zu dokumentieren.

## § 12 Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

(1) [1]Die betroffene Person ist berechtigt, von der Polizei unverzüglich die Berichtigung sie betreffender unrichtiger Daten zu verlangen. [2]Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder Beurteilung. [3]Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. [4]In diesem Fall hat die Polizei die betroffene Person zu unterrichten, bevor die Einschränkung aufgehoben wird. [5] Die betroffene Person kann darüber hinaus die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist.
(2) Die betroffene Person ist berechtigt, von der Polizei unverzüglich die Löschung sie betreffender Daten zu verlangen, wenn deren Verarbeitung unzulässig ist, deren Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist oder diese zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen.
(3) Bei automatisierten Dateisystemen ist technisch sicherzustellen, dass eine Einschränkung der Verarbeitung eindeutig erkennbar ist und eine Verarbeitung für andere Zwecke nicht ohne weitere Prüfung möglich ist.
(4) [1]Die Polizei hat die betroffene Person über ein Absehen von der Berichtigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung schriftlich zu unterrichten. [2]Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 10 Absatz 2, 5 oder 6 mit sich bringen würde. [3]Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von der Unterrichtung verfolgten Zweck gefährden würde.
(5) § 11 Absatz 7 und 8 sowie § 26 gelten entsprechend.

## § 13 Anrufung der oder des Landesbeauftragten für Datenschutz

(1) [1]Jede betroffene Person kann sich unbeschadet anderweitiger Rechtsbehelfe mit einer Beschwerde an die oder den Landesbeauftragten für Datenschutz wenden, wenn sie der Auffassung ist, bei der Verarbeitung ihrer personenbezogenen Daten in ihren Rechten verletzt worden zu sein. [2]Die oder der Landesbeauftragte für Datenschutz hat die betroffene Person über den Stand und das Ergebnis der Beschwerde zu unterrichten und sie hierbei auf die Möglichkeit gerichtlichen Rechtsschutzes hinzuweisen.
(2) [1]Die oder der Landesbeauftragte für Datenschutz hat eine bei ihr oder ihm eingelegte Beschwerde über eine Verarbeitung, die in die Zuständigkeit einer anderen Aufsichtsbehörde fällt, unverzüglich an die zuständige Aufsichtsbehörde weiterzuleiten, auch wenn diese in einem anderen Mitgliedstaat der Europäischen Union gelegen ist. [2]Sie oder er hat in diesem Fall die betroffene Person über die Weiterleitung zu unterrichten und ihr auf deren Ersuchen weitere Unterstützung zu leisten.

## § 14 Rechtsschutz gegen Entscheidungen der oder des Landesbeauftragten für Datenschutz oder bei deren oder dessen Untätigkeit

(1) Jede natürliche oder juristische Person kann unbeschadet anderer Rechtsbehelfe gerichtlich gegen Maßnahmen oder verbindliche Entscheidungen der oder des Landesbeauftragten für Datenschutz vorgehen; § 26 des Saarländischen Datenschutzgesetzes gilt entsprechend.
(2) Absatz 1 gilt entsprechend zugunsten betroffener Personen, wenn sich die oder der Landesbeauftragte für Datenschutz mit einer Beschwerde nach § 13 nicht befasst oder die betroffene Person nicht innerhalb von drei Monaten nach Einlegung der Beschwerde über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt hat.

## § 15 Verfahren für die Ausübung der Rechte der betroffenen Person

(1) [1]Die Polizei hat mit der betroffenen Person unter Verwendung einer klaren und einfachen Sprache in präziser, verständlicher und leicht zugänglicher Form zu kommunizieren. [2]Unbeschadet besonderer Formvorschriften soll bei der Beantwortung von Anträgen grundsätzlich die für den Antrag gewählte Form verwendet werden.
(2) Bei Anträgen hat die Polizei die betroffene Person unbeschadet des § 11 Absatz 6 und des § 12 Absatz 4 unverzüglich schriftlich darüber in Kenntnis zu setzen, wie verfahren wurde.
(3) [1]Die Erteilung von Informationen nach § 9, die Benachrichtigung nach § 10 und die Bearbeitung von Anträgen nach den §§ 11 und 12 erfolgen unentgeltlich. [2]Bei offenkundig unbegründeten oder exzessiven Anträgen nach den §§ 11 und 12 kann die Polizei entweder eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. [3]In diesem Fall muss die Polizei den offenkundig unbegründeten oder exzessiven Charakter des Antrags belegen können.
(4) Hat die Polizei begründete Zweifel an der Identität einer betroffenen Person, die einen Antrag nach den §§ 11 oder 12 gestellt hat, sind Nachweise zur Bestätigung der Identität anzufordern.

## § 16 Schadensersatz

(1) [1]Hat die Polizei einer betroffenen Person durch eine rechtswidrige Verarbeitung personenbezogener Daten einen Schaden zugefügt, ist sie zum Schadensersatz verpflichtet. [2]Die Ersatzpflicht entfällt, soweit bei einer nicht-automatisierten Verarbeitung der Schaden nicht auf ein Verschulden des Verantwortlichen zurückzuführen ist.
(2) Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

(3) Lässt sich bei einer automatisierten Verarbeitung personenbezogener Daten nicht ermitteln, welche von mehreren beteiligten Verantwortlichen den Schaden verursacht hat, so haftet jeder Verantwortliche beziehungsweise ihr Rechtsträger.
(4) Hat bei der Entstehung des Schadens ein Verschulden der Beschädigten mitgewirkt, ist § 254 des Bürgerlichen Gesetzbuches in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Artikel 1 des Gesetzes vom 31. Januar 2019 (BGBl. I S. 54), in der jeweils geltenden Fassung entsprechend anzuwenden.
(5) Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuches entsprechende Anwendung.

## Zweiter Teil
## Rechtsgrundlagen der Verarbeitung personenbezogener Daten

### § 17 Kategorien betroffener Personen

(1) Nach Maßgabe der §§ 18 bis 29 und §§ 31 bis 52 darf die Polizei personenbezogene Daten über
1. die in den §§ 4 und 5 des Saarländischen Polizeigesetzes und unter den Voraussetzungen des § 6 des Saarländischen Polizeigesetzes über die dort genannten Personen,
2. geschädigte, hilflose oder vermisste Personen sowie deren Angehörige, gesetzliche Vertreterinnen oder Vertreter oder Vertrauenspersonen,
3. gefährdete Personen,
4. Zeuginnen oder Zeugen, Hinweisgeberinnen oder Hinweisgeber oder sonstige Auskunftspersonen,
5. Personen, deren besondere Kenntnisse oder Fähigkeiten zur Gefahrenabwehr benötigt werden,
6. Verantwortliche für Anlagen oder Einrichtungen, von denen eine erhebliche Gefahr ausgehen kann,
7. Verantwortliche für gefährdete Anlagen oder Einrichtungen,
8. Verantwortliche für Veranstaltungen in der Öffentlichkeit

verarbeiten.
(2) Nach Maßgabe der §§ 18 bis 29 und §§ 31 bis 52 darf die Vollzugspolizei personenbezogene Daten über
1. Personen, bei denen Anhaltspunkte bestehen, dass sie künftig Straftaten begehen,
2. Personen, die mit einer der in Nummer 1 genannten Personen nicht nur flüchtig oder in zufälligem Kontakt und in einer Weise in Verbindung stehen, die erwarten lässt, dass Hinweise für die Verfolgung oder vorbeugende Bekämpfung von Straftaten gewonnen werden,
   a) weil Tatsachen die Annahme rechtfertigen, dass die Personen von der Planung oder der Vorbereitung der Straftaten oder der Verwertung der Tatvorteile Kenntnis haben oder daran mitwirken oder sie
   b) aus der Verwertung der Tat Vorteile ziehen könnten.
3. Personen, bei denen Anhaltspunkte bestehen, dass sie Opfer von Straftaten werden,
4. Zeuginnen oder Zeugen, Hinweisgeberinnen oder Hinweisgeber oder sonstige Auskunftspersonen,
5. Verurteilte,
6. Beschuldigte,
7. Personen, die verdächtig sind, eine mit Strafe bedrohte Tat begangen zu haben,

verarbeiten.

## § 18 Erhebung personenbezogener Daten

(1) Die Polizei darf personenbezogene Daten über die in § 17 Absatz 1 Nummer 1 bis Nummer 4 genannten Personen erheben, soweit das zur Abwehr einer Gefahr erforderlich ist und die §§ 28 bis 42 die Erhebungsbefugnisse nicht besonders regeln.
(2) Die Vollzugspolizei darf personenbezogene Daten über die in § 17 Absatz 2 Nummer 1 bis Nummer 4 genannten Personen erheben, soweit dies erfahrungsgemäß zur vorbeugenden Bekämpfung von Straftaten erforderlich ist und die Erhebungsbefugnisse in diesem Gesetz nicht besonders geregelt sind.
(3) [1]Die Polizei darf Namen, Vornamen, akademische Grade, Anschriften, Telefonnummern und andere Daten über die Erreichbarkeit sowie nähere Angaben über die Zugehörigkeit zu einer der genannten Personengruppen aus allgemein zugänglichen Quellen, bei Behörden oder auf Grund freiwilliger Angaben über die in § 17 Absatz 1 Nummer 5 bis Nummer 8 genannten Personen erheben, soweit das zur Vorbereitung auf die Hilfeleistung in Gefahrenabwehrfällen erforderlich ist. [2]Eine verdeckte Erhebung personenbezogener Daten ist in diesen Fällen nicht zulässig. [3]Die nach Satz 1 bei Personen nach § 17 Absatz 1 Nummer 8 erhobenen personenbezogenen Daten sind spätestens einen Monat nach Beendigung des Anlasses zu löschen. [4]§ 23 Absatz 5 und 6 bleibt unberührt.

## § 19 Einwilligung

(1) [1]Soweit in diesem Gesetz eine Einwilligung der betroffenen Person in die Verarbeitung ihrer personenbezogenen Daten vorgesehen ist, ist der Zweck, zu dem sie verarbeitet werden sollen, vorher zu bestimmen und der betroffenen Person mitzuteilen. [2]Die Einwilligung erfolgt schriftlich, soweit nicht ausnahmsweise hiervon abgesehen werden kann. [3]Die betroffene Person ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, bei einer beabsichtigten Übermittlung an Dritte über diese aufzuklären; sie ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass sie die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann. [4]Eine Verarbeitung zu einem anderen Zweck ist nicht zulässig. [5]Die Polizei muss die Einwilligung der betroffenen Person nachweisen können.
(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.
(3) [1]Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. [2]Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. [3]Die betroffene Person ist vor der Einwilligung hiervon in Kenntnis zu setzen.
(4) [1]Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. [2]Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden.
(5) Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

## § 20 Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des § 2 Absatz 15 ist nur zulässig, wenn dies zur Aufgabenerfüllung unbedingt erforderlich ist und

1. aufgrund gesetzlicher Vorschriften ausdrücklich vorgesehen ist,
2. der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dient,
3. sich auf personenbezogene Daten bezieht, welche die betroffene Person offensichtlich öffentlich gemacht hat oder
4. die betroffene Person eingewilligt hat.

(2) [1]Werden besondere Kategorien personenbezogener Daten verarbeitet, sind geeignete Garantien für die Rechtsgüter der betroffenen Person vorzusehen. [2]Geeignete Garantien können insbesondere sein

1. spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle,
2. die Festlegung von besonderen Aussonderungsprüffristen,
3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der jeweiligen Polizeibehörde,
5. die von anderen Daten getrennte Verarbeitung,
6. die Pseudonymisierung personenbezogener Daten,
7. die Anonymisierung personenbezogener Daten,
8. die Verschlüsselung personenbezogener Daten oder
9. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Rechtmäßigkeit der Verarbeitung sicherstellen.

## § 21 Speicherung, Veränderung und Verwendung personenbezogener Daten

(1) [1]Die Polizei kann personenbezogene Daten speichern, verändern sowie verwenden, soweit das zur Erfüllung ihrer Aufgaben, zur Vorgangsverwaltung oder zur Dokumentation erforderlich ist. [2]Die Speicherung, Veränderung oder sonstige Verwendung darf nur zu dem Zweck erfolgen, zu dem die personenbezogenen Daten erlangt worden sind. [3]Die Verwendung einschließlich ihrer erneuten Speicherung und einer Veränderung zu einem anderen polizeilichen Zweck durch die Polizeiverwaltungsbehörden ist jedoch zulässig, soweit die Polizeiverwaltungsbehörden die personenbezogenen Daten zu diesem Zweck erheben dürften. [4]Die Vollzugspolizei kann personenbezogene Daten nur unter den Voraussetzungen des § 23 zu anderen Zwecken verarbeiten.

(2) Soweit bereits Daten zu einer Person gespeichert sind, dürfen zu der betreffenden Person auch

1. personengebundene Hinweise, die zum Schutz dieser Person oder zur Eigensicherung von Beamten erforderlich sind, oder
2. weitere standardisierte Hinweise, die geeignet sind, dem Schutz Dritter oder der Gewinnung von Ermittlungsansätzen zu dienen,

gespeichert und verwendet werden.

(3) [1]Bei der Verarbeitung ist so weit wie möglich danach zu unterscheiden, ob personenbezogene Daten auf Tatsachen oder auf persönlichen Einschätzungen beruhen. [2]Beurteilungen, die auf persönlichen Einschätzungen beruhen sind als solche kenntlich machen, soweit dies im Rahmen der jeweiligen Verarbeitung möglich und angemessen ist. [3]Werden Hinweise nach Absatz 2 oder Bewertungen, die auf persönlichen Einschätzungen beruhen, gespeichert, muss feststellbar sein, bei welcher Stelle die Unterlagen geführt werden, die der Bewertung zu Grunde liegen.

(4) [1]Werden personenbezogene Daten von Kindern, die ohne Kenntnis der Sorgeberechtigten erhoben worden sind, gespeichert, sind die Sorgeberechtigten zu unterrichten, sobald die Aufgabenerfüllung dadurch nicht mehr gefährdet wird. [2]Von der Unterrichtung kann abgesehen werden, solange zu besorgen ist, dass die Unterrichtung zu erheblichen Nachteilen für das Kind führt.

## § 22 Kennzeichnung

(1)[1]Bei der Speicherung durch die Vollzugspolizei zum Zweck der Verarbeitung mittels automatisierter Verfahren sind personenbezogene Daten wie folgt zu kennzeichnen:

1. Angabe des Mittels der Erhebung der Daten einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden,
2. Angabe der Kategorie nach § 17 bei Personen, zu denen Grunddaten angelegt wurden,
3. Angabe der
   a) Rechtsgüter, deren Schutz die Erhebung dient oder
   b) Straftaten, deren Verhütung oder Verfolgung die Erhebung dient,
4. Angabe der Stelle, die sie erhoben hat.

[2]Die Kennzeichnung nach Satz 1 Nummer 1 kann auch durch Angabe der Rechtsgrundlage der jeweiligen Mittel der Datenerhebung ergänzt werden. [3]Personenbezogene Daten, denen keine Erhebung vorausgegangen ist, sind, soweit möglich, nach Satz 1 zu kennzeichnen; darüber hinaus sind die erste Daten verarbeitende Stelle sowie**,** soweit möglich, derjenige, von dem die Daten erlangt wurden, anzugeben.

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

(3) Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung nach Absatz 1 durch diese Stelle aufrechtzuerhalten.

## § 23 Zweckbindung, Grundsatz der hypothetischen Datenneuerhebung, Datenverarbeitung zu anderen Zwecken

(1) [1]Die Vollzugspolizei kann personenbezogene Daten, die sie selbst erhoben hat, unter Berücksichtigung der jeweiligen Datenerhebungsvorschrift verarbeiten

1. zur Erfüllung derselben Aufgabe und
2. zum Schutz derselben Rechtsgüter oder zur Verhütung oder Verfolgung derselben Straftaten oder Ordnungswidrigkeiten.

[2]Satz 1 gilt entsprechend für personenbezogene Daten, denen keine Erhebung vorausgegangen ist, mit der Maßgabe, dass für die Verarbeitung der Zweck der Speicherung zu berücksichtigen ist. [3]Für die Verarbeitung von personenbezogenen Daten, die durch den Einsatz technischer Mittel in oder aus Wohnungen nach § 32 Absatz 3 Satz 2 oder § 34 erlangt wurden, muss im Einzelfall eine Gefahr oder Gefahrenlage im Sinne des § 34 Absatz 1 vorliegen. [4]§ 34 Absatz 3 Satz 2 gilt entsprechend.

(2) [1]Die Vollzugspolizei kann zur Erfüllung ihrer Aufgaben personenbezogene Daten zu anderen Zwecken, als denjenigen, zu denen sie erhoben worden sind, verarbeiten, wenn

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

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

[2]Abweichend von Satz 1 können die vorhandenen Grunddaten einer Person (§ 2 Absatz 19) auch verarbeitet werden, um diese Person zu identifizieren. [3]Die Absätze 4 bis 10 sowie besondere Vorschriften zur Verarbeitung bleiben unberührt. [4] Satz 1 bis 3 gilt entsprechend für personenbezogene Daten, denen keine Erhebung vorausgegangen

ist, mit der Maßgabe, dass für die Verarbeitung der Zweck der Speicherung zu berücksichtigen ist.
(3) [1]Für die Verarbeitung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel nach § 31 Absatz 2 Nummer 2 in oder aus Wohnungen erhoben wurden, gilt Absatz 2 Satz 1 Nummer 2 Buchstabe b mit der Maßgabe entsprechend, dass eine Gefahr oder eine Gefahrenlage im Sinne des § 34 Absatz 1 vorliegen muss. [2]Personenbezogene Daten, die im Wege der verdeckten akustischen Wohnraumüberwachung dürfen nur unter den Voraussetzungen des § 100b der Strafprozessordnung zu Strafverfolgungszwecken verarbeitet werden. [3]Personenbezogene Daten, die durch Herstellung von Lichtbildern oder Bildaufzeichnungen über eine Person im Wege eines verdeckten Einsatzes technischer Mittel in oder aus Wohnungen erlangt wurden, dürfen nicht zu Strafverfolgungszwecken verarbeitet werden.
(4) [1]Die Vollzugspolizei kann personenbezogene Daten

1. die sie im Rahmen von Strafermittlungsverfahren über Personen gewonnen hat, die verdächtig sind, eine mit Strafe bedrohte Tat begangen zu haben oder
2. von Personen, die wegen einer solchen verurteilt wurden,

speichern und nach Maßgabe der Absätze 1 und 2 verändern sowie verwenden, soweit dies zur Abwehr von Gefahren oder zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. [2]Die suchfähig gespeicherten personenbezogenen Daten sind zu löschen

1. nach Ablauf einer Speicherungsfrist von zwei Jahren,
2. wenn die betroffene Person im Strafverfahren rechtskräftig freigesprochen wurde,
3. die Eröffnung des Hauptverfahrens unanfechtbar abgelehnt wurde oder
4. das Strafverfahren nicht nur vorläufig eingestellt wurde und sich aus den Entscheidungsgründen ergibt, das die betroffene Person die Straftat nicht oder nicht rechtswidrig begangen hat.

[3]Eine Speicherung über die in Satz 2 Nummer 1 genannte Frist hinaus ist nur zulässig, wenn wegen der wegen der Art, Ausführung oder Schwere der Tat oder der Persönlichkeit der betroffenen Person die Gefahr der Wiederholung besteht.
(5) [1]Die Vollzugspolizei kann im Rahmen der vorbeugenden Bekämpfung von Straftaten personenbezogene Daten über die in § 17 Absatz 2 Nummer 1 bis 4 genannten Personen, auch wenn sie in Strafermittlungsverfahren erhoben wurden, speichern und nach Maßgabe der Absätze 1 und 2 verändern oder verwenden, soweit dies zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten, erforderlich ist. [2]Die Speicherungsdauer darf bei den in § 17 Absatz 2 Nummer 2 bis 4 genannten Personen drei Jahre nicht überschreiten. [3]Nach jeweils einem Jahr, gerechnet vom Zeitpunkt der letzten Speicherung, ist zu prüfen, ob die Voraussetzungen nach Satz 1 noch vorliegen; die Entscheidung trifft die Behördenleiterin oder der Behördenleiter oder eine von ihr oder ihm beauftragte Beamtin oder ein von ihr oder ihm beauftragter Beamter.
(6) [1]Die Vollzugspolizei kann zu Zwecken der Planung von Maßnahmen der vorbeugenden Kriminalitätsbekämpfung oder der Verkehrsüberwachung personenbezogene Daten zur Erstellung von Lagebildern verwenden. [2]Die Verwendung personenbezogener Daten der in § 17 Absatz 1 Nummer 2 bis 4 genannten Personen ist nur zulässig, soweit dies zur Erstellung der jeweiligen Lagebilder erforderlich ist. [3]Die in Satz 2 genannten personenbezogenen Daten sind spätestens am Ende des der Speicherung folgenden Kalenderjahres automatisiert zu löschen.
(7) [1]Die Verarbeitung personenbezogener Daten zu Aus-, Fort-, Weiterbildungs- und Prüfungszwecken ist nur zulässig, soweit eine Verarbeitung anonymisierter Daten zu diesem Zweck nicht möglich ist. [2]Die personenbezogenen Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren. [3]Die Verarbeitung personenbezogener Daten, die mittels Einsatz technischer Mittel in oder aus Wohnungen nach § 32 Absatz 3 Satz 2 oder § 34 erhoben worden sind, ist nur in anonymisierter Form zulässig.

(8) [1]Die Verarbeitung personenbezogener Daten zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung, zur Durchführung von Organisationsuntersuchungen und zur Prüfung und Wartung von automatisierten Verfahren der Datenverarbeitung sowie zu statistischen Zwecken ist nur zulässig, soweit eine Verarbeitung anonymisierter Daten zu diesem Zweck nicht möglich ist. [2]Die personenbezogenen Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren.
(9) Die Verarbeitung personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken ist nach Maßgabe der §§ 23 und 24 des Saarländischen Datenschutzgesetzes zulässig.
(10) Bei der Verarbeitung von personenbezogenen Daten stellt die Vollzugspolizei durch organisatorische und technische Vorkehrungen sicher, dass die Absätze 1 bis 9 beachtet werden.

## § 24 Verarbeitung auf Weisung des Verantwortlichen

Jede einer Polizeibehörde oder einem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach einer Rechtsvorschrift zur Verarbeitung verpflichtet ist.

## § 25 Automatisierte Einzelentscheidung

(1) Eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt, ist nur zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.
(2) Entscheidungen nach Absatz 1 dürfen nicht auf besonderen Kategorien personenbezogener Daten beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechtsgüter sowie der berechtigten Interessen der betroffenen Person getroffen wurden.
(3) Profiling, das zur Folge hat, dass die betroffene Person auf der Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert wird, ist verboten.

## § 26 Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten

(1) [1]Gespeicherte personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. [2]Wird festgestellt, dass in Akten gespeicherte personenbezogene Daten unrichtig sind, ist das in der Akte zu vermerken oder auf sonstige Weise festzuhalten.
(2) [1]Gespeicherte personenbezogene Daten sind zu löschen und die dazugehörigen Unterlagen sind zu vernichten, wenn

1. ihre Speicherung unzulässig war,
2. bei der nach bestimmten Fristen vorzunehmenden Überprüfung oder aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist, oder
3. der Verdacht, welcher der Speicherung zugrunde liegt, entfällt.

[2]Die Prüffristen dürfen

1. bei Erwachsenen zehn Jahre, nach Vollendung des 70. Lebensjahres fünf Jahre,
2. bei Jugendlichen fünf Jahre und
3. bei Kindern zwei Jahre

nicht überschreiten, wobei nach Zweck der Speicherung, den Kategorien betroffener Personen sowie Art und Schwere des Sachverhalts zu unterscheiden ist.

[3]Die Frist beginnt regelmäßig mit dem letzten Anlass, der zur Speicherung personenbezogener Daten geführt hat, jedoch nicht vor Entlassung der betroffenen Person aus einer Justizvollzugsanstalt oder Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung. [4]Werden innerhalb dieser gesetzlichen Fristen weitere personenbezogene Daten über die jeweils betroffene Person gespeichert, in deren Zusammenhang sie als Straftäterin oder -täter oder Teilnehmerin oder Teilnehmer an einer Straftat geführt wird, gilt für den gesamten Datensatz die Frist, die als letzte endet.
(3) [1]Löschung und Vernichtung unterbleiben, wenn

1. Grund zu der Annahme besteht, dass schutzwürdige Belange der betroffenen Person beeinträchtigt würden,
2. die personenbezogenen Daten zur Behebung einer bestehenden Beweisnot unerlässlich sind,
3. die Verwendung der personenbezogenen Daten zu wissenschaftlichen Zwecken erforderlich ist, oder
4. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist

[2]In diesen Fällen ist die Verarbeitung der personenbezogenen Daten einzuschränken (§ 2 Absatz 3). [3]Sie dürfen nur zu den in Satz 1 genannten Zwecken oder mit Einwilligung der betroffenen Person verwendet werden.
(4) An Stelle der Löschung und Vernichtung nach Absatz 2 Satz 1 Nummer 2 können die Datenträger an ein Staatsarchiv abgegeben werden, soweit archivrechtliche Regelungen das vorsehen.
(5) § 12 bleibt unberührt.

### § 27 Protokolldaten

(1) [1]Soweit personenbezogene Daten in automatisierten Dateisystemen verarbeitet werden, sind mindestens die Verarbeitungsvorgänge Erhebung, Speicherung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung zu protokollieren. [2]Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identifizierung der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität der Empfängerin oder des Empfängers solcher personenbezogenen Daten festzustellen.
(2) [1]Die Polizei und gegebenenfalls der Auftragsverarbeiter haben die Protokolle der oder dem Landesbeauftragten für Datenschutz auf Anforderung zum Zweck der Überprüfung der Rechtmäßigkeit der Datenverarbeitung soweit möglich in elektronisch auswertbarer Form zur Verfügung zu stellen; der oder dem Landesbeauftragten für Datenschutz darf auch ein lesender Zugriff eingeräumt werden. [2]Darüber hinaus dürfen die protokollierten Daten nur für die Überprüfung der Rechtmäßigkeit der Verarbeitung, der Eigenüberwachung, für die Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten sowie für die Verfolgung von Straftaten verwendet werden.
(3) Die nach Absatz 2 Satz 1 erstellten Protokolle sind, soweit personenbezogene Daten verarbeitet werden, am Ende des auf deren Generierung folgenden Jahres zu löschen zu löschen, sofern sie nicht zur Verfolgung von Straftaten erforderlich sind.

## Dritter Teil
## Besondere Befugnisse zur Verarbeitung personenbezogener Daten

### § 28 Abgleich personenbezogener Daten, Zuverlässigkeitsüberprüfung

(1) [1]Die Vollzugspolizei kann personenbezogene Daten der in den §§ 4, 5 des Saarländischen Polizeigesetzes sowie in § 17 Absatz 2 Nummer 1 und 2 dieses Gesetzes genannten Personen mit Dateisystemen, die sie selbst führt, oder für die sie eine Berechtigung zum Abruf hat, abgleichen. [2]Personenbezogene Daten anderer Personen kann die Vollzugspolizei abgleichen, wenn das auf Grund tatsächlicher Anhaltspunkte zur Erfüllung polizeilicher Aufgaben erforderlich erscheint. [3]Die Vollzugspolizei kann ferner im Rahmen ihrer Aufgabenerfüllung erlangte personenbezogene Daten mit dem Fahndungsbestand abgleichen. [4]Ein Abgleich der gemäß § 17 Absatz 1 Nummer 5 bis 8 erlangten personenbezogenen Daten ist nur mit Einwilligung der betroffenen Person zulässig.
(2) Rechtsvorschriften über den Abgleich personenbezogener Daten in anderen Fällen bleiben unberührt.
(3) [1]Der Abgleich nach Absatz 1 darf auch im Rahmen von Zuverlässigkeitsüberprüfungen durchgeführt werden. [2]Hierzu darf die Vollzugspolizei solche betroffenen Personen mit deren Einwilligung überprüfen, die

1. eine Tätigkeit als Bedienstete anstreben
   a) in einer Behörde mit Vollzugsaufgaben,
   b) in einer anderen öffentlichen Stelle, bei der sie regelmäßig Zugriff auf Personalaktendaten von Bediensteten haben, die bei einer Behörde mit Vollzugsaufgaben verwendet werden, oder
   c) in besonders gefährdeten Liegenschaften öffentlicher Stellen,
2. selbstständige Dienstleistungen zur Unterstützung von Vollzugsaufgaben erbringen wollen,
3. unbegleiteten Zutritt zu Liegenschaften von Behörden mit Vollzugsaufgaben oder Liegenschaften öffentlicher Stellen, die besonders gefährdet sind, erhalten sollen, ohne den in Nummer 1 und 2 genannten Personengruppen anzugehören,
4. Zugang zu Vergabe- und Vertragsunterlagen haben, aus denen sich sicherheitsrelevante Funktionszusammenhänge, insbesondere aus baulichen und betrieblichen Anforderungen für Liegenschaften der Polizei oder der Justiz ergeben,
5. die Zulassung zum Besuch von Gefangenen oder Untergebrachten in einer Justizvollzugseinrichtung begehren oder
6. beratend oder unterstützend für eine Behörde tätig werden.

[3]Eine Zuverlässigkeitsüberprüfung darf ferner durchgeführt werden bei Personen, für die ein privilegierter Zutritt zu einer Veranstaltung einer Behörde, einer sonstigen öffentlichen oder einer nicht-öffentlichen Stelle beantragt wird. [4]Bei Veranstaltungen in nicht-öffentlicher Trägerschaft ist eine Zuverlässigkeitsüberprüfung ungeachtet der Einwilligung betroffener Personen nur zulässig, wenn

1. es sich um eine besonders gefährdete Veranstaltung handelt oder
2. eine Zuverlässigkeitsüberprüfung im Einzelfall zum Schutz der Veranstaltung erforderlich ist.

(4) [1]Die Vollzugspolizei hat die Identität der betroffenen Person, deren Zuverlässigkeit überprüft werden soll, festzustellen. [2]Zu diesem Zweck darf sie vorgelegte Ausweisdokumente kopieren oder Kopien von Ausweisdokumenten anfordern. [3]Die Überprüfung kann durch den Abgleich von Datenbeständen

1. der Vollzugspolizeibehörden des Bundes und der Länder,
2. im Fall von Erkenntnissen über Strafverfahren auch der Justizbehörden und Gerichte sowie,
3. soweit im Einzelfall erforderlich, der Verfassungsschutzbehörde und
4. unter den Voraussetzungen der §§ 31, 41 des Bundeszentralregistergesetzes in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 I S. 195), zuletzt geändert durch Artikel 1 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2732), auch des Bundeszentralregisters

erfolgen.

(5) [1]Entscheidet die Vollzugspolizei nicht selbst auch über die Zuverlässigkeit, unterrichtet sie die ersuchende Stelle darüber, ob sicherheitsrelevante Erkenntnisse vorliegen, gegebenenfalls durch Angabe von

1. Deliktsbezeichnung,
2. Tatort,
3. Tatzeit,
4. Ausgang des Verfahrens, soweit feststellbar, sowie
5. Name und Aktenzeichen der sachbearbeitenden Justiz- oder Vollzugspolizeibehörde.

[2]Erkenntnisse der Verfassungsschutzbehörde dürfen nur als allgemeiner Hinweis in die Mitteilung aufgenommen werden. [3]Gegenüber anderen ersuchenden Stellen als Gefahrenabwehr- und Justizbehörden, insbesondere gegenüber nicht-öffentlichen Stellen, beschränkt sich die Rückmeldung auf die Auskunft, ob Sicherheitsbedenken vorliegen.

(6) [1]Wiederholungsüberprüfungen sind zulässig, wenn seit der letzten Überprüfung mindestens ein Jahr vergangen ist und die Voraussetzungen des Absatzes 3 noch vorliegen. [2]Wiederholungsüberprüfungen dürfen in den Fällen des Absatzes 3 Satz 3 auch in Bezug auf gleichartige Veranstaltungen durchgeführt werden. [3]Werden Wiederholungsüberprüfungen auf Ersuchen durchgeführt, unterrichtet die ersuchende Behörde die Vollzugspolizei zugleich über das Vorliegen der Voraussetzungen des Absatzes 3.

(7) Die im Rahmen der Zuverlässigkeitsüberprüfungen nach Absatz 3, 6 erhobenen personenbezogen Daten sind am Ende des Kalenderjahres, das dem Jahr der Überprüfung folgt, zu löschen.

## § 29 Besondere Formen des Abgleichs personenbezogener Daten

(1) [1]Die Vollzugspolizei kann von öffentlichen oder nichtöffentlichen Stellen zur Abwehr von Gefahren für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zweck des Abgleichs mit anderen Datenbeständen verlangen, soweit dies erforderlich ist. [2]Vorschriften über ein Berufs- oder besonderes Amtsgeheimnis bleiben unberührt.

(2) [1]Das Übermittlungsersuchen ist auf Namen, Anschrift, Tag und Ort der Geburt sowie auf im einzelnen Falle festzulegende Merkmale zu beschränken. [2]Werden wegen technischer Schwierigkeiten, die mit angemessenem Zeit- oder Kostenaufwand nicht beseitigt werden können, weitere personenbezogene Daten übermittelt, dürfen diese nicht verwertet werden.

(3) [1]Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen personenbezogenen Daten auf dem Datenträger zu löschen und die Unterlagen, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind, zurückzugeben oder zu vernichten.

[2]Über die getroffene Maßnahme ist eine Niederschrift anzufertigen. [3]Diese Niederschrift ist gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Vernichtung der Unterlagen nach Satz 1 folgt, zu vernichten.
(4) [1]Die Anordnung der Maßnahme darf nur durch die Richterin oder den Richter erfolgen; für das Verfahren gilt das das erste Buch des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit vom 17. Dezember 2008 (BGBl. I S. 2586, 2587), zuletzt geändert durch Artikel 7 des Gesetzes vom 20. Juli 2017 (BGBl. I S. 2780), in der jeweils geltenden Fassung entsprechend mit Ausnahme des § 34. [2]Die oder der Landesbeauftragte für Datenschutz ist zu unterrichten.

## § 30 Verarbeitung von DNA-Identifizierungsmustern zur Erkennung von DNA-Trugspuren

(1) [1]Die Vollzugspolizei kann von ihren Mitarbeiterinnen und Mitarbeitern, die Umgang mit Spurenmaterial haben oder die Bereiche in den Liegenschaften und Einrichtungen betreten müssen, in denen mit Spurenmaterial umgegangen oder dieses gelagert wird,

1. mittels eines Mundschleimhautabstrichs oder einer hinsichtlich ihrer Eingriffsintensität vergleichbaren Methode Körperzellen entnehmen,
2. diese zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersuchen und
3. die festgestellten DNA-Identifizierungsmuster mit den an Spurenmaterial festgestellten DNA-Identifizierungsmuster abgleichen,

um zur Erkennung von DNA-Trugspuren festzustellen, ob an Spurenmaterial festgestellte DNA-Identifizierungsmuster von diesen Personen stammen. [2]Die Entnahme der Körperzellen darf nicht erzwungen werden. Die entnommenen Körperzellen dürfen nur für die in Satz 1 genannte molekulargenetische Untersuchung verwendet werden; sie sind unverzüglich zu vernichten, sobald sie hierfür nicht mehr erforderlich sind. Bei der Untersuchung dürfen andere Feststellungen als diejenigen, die zur Ermittlung des DNA-Identifizierungsmusters erforderlich sind, nicht getroffen werden; hierauf gerichtete Untersuchungen sind unzulässig.
(2) Untersuchungen und Abgleiche nach Absatz 1 bei Personen, die nicht Mitarbeiterinnen und Mitarbeiter der Vollzugspolizei sind, dürfen nur mit deren schriftlicher Einwilligung erfolgen.
(3) [1]Die nach den Absätzen 1 und 2 erhobenen Daten sind zu pseudonymisieren und darüber hinaus in einem gesonderten Dateisystem zu speichern. [2]Eine Verwendung dieser Daten zu anderen Zwecken als den in den Absätzen 1 und 2 genannten Zwecken ist unzulässig. [3]Die DNA-Identifizierungsmuster sind zu löschen, wenn sie für die genannten Zwecke nicht mehr erforderlich sind. Die Löschung hat spätestens drei Jahre nach dem letzten Umgang der betreffenden Person mit Spurenmaterial oder dem letzten Zutritt zu einem in Absatz 1 Satz 1 genannten Bereich zu erfolgen. [4]Betroffene Personen sind schriftlich über den Zweck und die Verarbeitung sowie die Löschung der erhobenen Daten zu informieren.

## § 31 Besondere Formen der Erhebung personenbezogener Daten

(1) [1]Die Vollzugspolizei kann personenbezogene Daten über die in § 17 Absatz 2 Nummer 1 und 2 genannten Personen mit Mitteln nach Absatz 2 nur erheben, soweit das zur vorbeugenden Bekämpfung

1. von Verbrechen, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine solche Straftat begangen werden soll, oder

2. anderer Straftaten, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine solche Straftat gewerbsmäßig, gewohnheitsmäßig, von Banden oder von Organisationen begangen werden soll,

erforderlich ist.

[2]Ferner kann die Vollzugpolizei personenbezogene Daten über die in § 17 Absatz 2 Nummer 1 und 2 genannten Personen mit Mitteln nach Absatz 2 erheben, wenn das individuelle Verhalten einer solchen Person die konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb eines übersehbaren Zeitraums eine in § 129a Absatz 1 und 2 des Strafgesetzbuchs in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 1 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618), in der jeweils geltenden Fassung bezeichnete Straftat begehen wird und die dazu bestimmt ist,

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

[3]Die Erforschung des Sachverhaltes muss ohne Gefährdung der Aufgabenerfüllung auf andere Weise aussichtslos sein; die Maßnahme darf nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhaltes stehen. [4]Brief-, Post- und Fernmeldegeheimnis bleiben unberührt. [5]Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen sind.

(2) Mittel des Absatzes 1 sind

1. die planmäßig angelegte offene oder verdeckte Beobachtung einer Person (Observation),
2. der verdeckte Einsatz technischer Mittel, insbesondere zur Anfertigung von Bildaufnahmen oder -aufzeichnungen sowie zum Abhören oder Aufzeichnen des gesprochenen Wortes auf Tonträger,
3. der Einsatz von Vertrauenspersonen und Informantinnen und Informanten,
4. der Einsatz von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten unter einer Legende (Verdeckte Ermittlerinnen oder Verdeckte Ermittler),
5. sonstige besondere für Observationszwecke bestimmte technische Mittel zur Erforschung des Sachverhalts oder zur Bestimmung des Aufenthaltsortes einer in § 17 Absatz 2 Nummer 1 oder 2 genannten Person.

(3) [1]Eine Maßnahme nach Absatz 2

1. Nummer 1 oder 5, die durchgehend länger als 24 Stunden dauern oder an mehr als zwei Tagen stattfinden soll (längerfristige Observation),
2. Nummer 2
   a) bei der durchgehend länger als 24 Stunden oder an mehr als zwei Tagen Bildaufzeichnungen bestimmter Personen angefertigt werden sollen oder
   b) beim Einsatz technischer Mittel zum Abhören und Aufzeichnen des gesprochenen Wortes
3. Nummer 3 oder 4, bei denen sich der Einsatz gegen eine bestimmte Person richtet oder bei denen eine Wohnung betreten wird, die nicht allgemein zugänglich ist,

darf nur durch die Richterin oder den Richter angeordnet werden.

[2]Die Anordnung der längerfristigen Observation oder des Einsatzes technischer Mittel zur Standortfeststellung ist auf höchstens sechs Monate, diejenige der übrigen Maßnahmen auf höchstens drei Monate zu befristen. [3]Soweit die Voraussetzungen der Anordnung fortbestehen, sind im Falle der Anordnung einer längerfristigen Observation oder des Einsatzes technischer Mittel zur Standortfeststellung auf Antrag jeweils Verlängerungen bis zu sechs Monaten, für den Einsatz der übrigen Maßnahmen jeweils bis zu drei Monaten zulässig. [4]Bei Gefahr im Verzug kann die Anordnung auch von der Behördenleiterin oder dem Behördenleiter getroffen werden. [5]Die Anordnung der

Behördenleiterin oder des Behördenleiters tritt außer Kraft, wenn sie nicht binnen drei Tagen von der Richterin oder dem Richter bestätigt wird. [6]Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeivollzugsbehörde ihren Sitz hat. [7]Für das Verfahren gilt § 29 Absatz 4 Satz 1 entsprechend. [8]Die Anordnung der nicht unter Satz 1 fallenden Maßnahmen erfolgt außer bei Gefahr im Verzug durch die Behördenleiterin oder den Behördenleiter oder eine von ihr beauftragte Beamtin oder einen von ihr beauftragten Beamten.
(4) Wird bei der Observation ein selbsttätiges Aufzeichnungsgerät eingesetzt, sind die Aufzeichnungen über andere als die in Absatz 1 genannten Personen unverzüglich zu vernichten.

## § 32 Offene Bild- und Tonaufzeichnungen

(1) [1]Die Vollzugspolizei kann bei oder im Zusammenhang mit öffentlichen Veranstaltungen und Ansammlungen, die ein besonderes Gefährdungsrisiko aufweisen, personenbezogene Daten durch die offene Anfertigung von Bild- und Tonaufzeichnungen zur Erkennung und Abwehr von Gefahren erheben. [2]Veranstaltungen und Ansammlungen weisen ein besonderes Gefährdungsrisiko auf, wenn

1. auf Grund einer aktuellen Gefährdungsanalyse anzunehmen ist, dass Veranstaltungen und Ansammlungen vergleichbarer Art und Größe von terroristischen Anschlägen bedroht sind,
2. auf Grund der Art und Größe der Veranstaltungen und Ansammlungen erfahrungsgemäß erhebliche Gefahren für die öffentliche Sicherheit entstehen können oder
3. ungeachtet von Art und Größe der Veranstaltungen und Ansammlungen tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten begangen werden.

[3]Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. [4]Die §§ 12a, 19a des Versammlungsgesetzes in der Fassung der Bekanntmachung vom 15. November 1978 (BGBl. I S. 1789), zuletzt geändert durch Artikel 2 des Gesetzes vom 8. Dezember 2008 (BGBl. I S. 2366), bleiben unberührt.
(2) [1]Die Vollzugspolizei kann offen Bildaufzeichnungen von Personen anfertigen

1. zur vorbeugenden Bekämpfung von Straftaten an öffentlich zugänglichen Orten, soweit an diesen Orten wiederholt Straftaten der Straßenkriminalität begangen worden sind und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung derartiger Straftaten zu rechnen ist, oder zur Abwehr einer Gefahr für die öffentliche Sicherheit,
2. in den in § 9 Absatz 1 Nummer 3 des Saarländischen Polizeigesetzes genannten Objekten oder in deren unmittelbarer Nähe, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dort oder an oder in Objekten dieser Art Straftaten begangen werden sollen, durch die Personen oder diese Objekte gefährdet werden.

[2]Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.
(3) [1]Die Vollzugspolizei kann in öffentlich zugänglichen Räumen personenbezogene Daten kurzzeitig speichern (Vorabaufnahme) und durch die offene Anfertigung von Bild- und Tonaufzeichnungen erheben, soweit dies zum Schutz von Polizeivollzugsbeamtinnen oder Polizeivollzugsbeamten oder Dritten zur Abwehr einer konkreten Gefahr erforderlich ist. [2]Zum Schutz der eingesetzten Polizeivollzugsbeamtinnen oder Polizeivollzugsbeamten ist auch die offene Anfertigung von Bild- und Tonaufzeichnungen in Wohnungen zulässig, sofern dies zur Abwehr einer dringenden Gefahr für Leib oder Leben erforderlich ist; die Maßnahme darf durch die einsatzleitende Polizeivollzugsbeamtin oder den einsatzleitenden Polizeivollzugsbeamten vor Ort angeordnet werden.

[3]Eine anderweitige Verwendung der hierbei erlangten Ergebnisse ist nur zum Zwecke der Strafverfolgung oder einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person und auch dann nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt ist; bei Gefahr im Verzuge ist die richterliche Entscheidung unverzüglich nachzuholen. [4]Für das Verfahren gilt § 29 Absatz 4 Satz 1 entsprechend. [5]Maßnahmen nach Satz 1 bis 3 dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.
(4) Die Vollzugspolizei kann in polizeilich genutzten Räumen durch den offenen Einsatz von technischen Mitteln zur Anfertigung von Bild- und Tonaufzeichnungen personenbezogene Daten erheben, soweit diese Maßnahme zum Schutz der festgehaltenen Person, der Polizeivollzugsbeamtinnen oder der Polizeivollzugsbeamten erforderlich ist.
(5) [1]Auf Maßnahmen nach den Absätzen 1 bis 4 ist durch Schilder oder in sonstiger geeigneter Form hinzuweisen. [2]Dabei ist in den Fällen der Absätze 1, 2 und 4 neben dem Umstand der Beobachtung auf Name und Kontaktdaten des Verantwortlichen hinzuweisen sowie die Möglichkeit zu eröffnen, die Informationen nach § 9 zu erhalten.
(6) Die Aufzeichnungen sind, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten erforderlich sind,

1. bei Maßnahmen nach Absatz 4 unverzüglich,
2. ansonsten spätestens nach einem Monat

zu löschen.

### § 33 Erhebung und Speicherung von Anrufen und des Sprechfunks

(1) [1]Die Vollzugspolizei zeichnet eingehende Notrufe zur Dokumentation des Notfallgeschehens auf. [2]Die Aufzeichnung anderer Anrufe ist nur zulässig, soweit dies zur Gefahrenabwehr erforderlich ist. [3]In den Fällen des Satzes 2 sind die Anruferin oder der Anrufer in geeigneter Weise auf die Tatsache der Aufzeichnung hinzuweisen, soweit dadurch nicht der Zweck der Aufzeichnung gefährdet wird.
(2) Die Aufzeichnungen sind, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten erforderlich sind, spätestens nach einem Monat zu löschen.
(3) Die Absätze 1 und 2 gelten entsprechend für die Aufzeichnung des polizeilichen Sprechfunks.

### § 34 Erhebung personenbezogener Daten in oder aus Wohnungen

(1) [1]In oder aus Wohnungen im Sinne des § 19 Absatz 1 Satz 2 des Saarländischen Polizeigesetzes kann die Vollzugspolizei personenbezogene Daten mit den in § 31 Absatz 2 Nummer 2 genannten technischen Mitteln erheben, wenn dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, unerlässlich ist. [2]Bei der Durchführung der Maßnahmen ist sicher zu stellen, dass der Einsatz technischer Mittel jederzeit unter- oder abgebrochen werden kann. [3]Die Maßnahme darf sich nur gegen den in den §§ 4 und 5 des Saarländischen Polizeigesetzes genannten Personenkreis richten und nur in deren Wohnung oder deren Wohnungen durchgeführt werden. [4]In Wohnungen anderer Personen ist die Maßnahme nur zulässig, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass

1. sich eine in Satz 3 genannte Person dort aufhält und
2. diese Person in den zu überwachenden Räumlichkeiten im Überwachungszeitraum verfahrensrelevante und im weiteren Verfahren verwertbare Gespräche führen wird.

[5]Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(2) [1]Die Erhebung personenbezogener Daten mit Mitteln nach § 31 Absatz 2 Nummer 2 in oder aus Wohnungen dürfen nur durch die Richterin oder den Richter angeordnet werden; für den Inhalt des hierfür erforderlichen Antrags gilt § 46 Absatz 4 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten vom 1. Juni 2017 (BGBl. I S. 1354) entsprechend. [2]Die Maßnahme ist auf höchstens einen Monat zu befristen. [3]Soweit die Voraussetzungen der Anordnung fortbestehen, sind auf Antrag Verlängerungen um jeweils einen weiteren Monat zulässig. [4]Für das Verfahren gilt § 29 Absatz 4 Satz 1 entsprechend. [5]Bei Gefahr im Verzug erfolgt die Anordnung durch die Behördenleitung oder eine von ihr beauftragte Beamtin oder einen von ihr beauftragten Beamten des höheren Polizeivollzugsdienstes; eine richterliche Entscheidung ist unverzüglich nachzuholen. [6]Soweit die Anordnung nach Satz 5 nicht binnen drei Tagen durch eine Richterin oder einen Richter bestätigt wurde, tritt sie außer Kraft.
(3) [1]Werden Mittel nach § 31 Absatz 2 Nummer 2 ausschließlich zur Abwehr einer Gefahr für Leib oder Leben der bei einem polizeilichen Einsatz in der Wohnung tätigen Personen eingesetzt, darf die Maßnahme durch die Behördenleitung oder eine von ihr beauftragte Beamtin oder einen von ihr beauftragten Beamten angeordnet werden. [2]Eine anderweitige Verwendung der hierbei erlangten Ergebnisse ist nur zum Zwecke der Strafverfolgung oder unter den Voraussetzungen des Absatzes 1 und auch dann nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt ist; bei Gefahr im Verzuge ist die richterliche Entscheidung unverzüglich nachzuholen. [3]Für das Verfahren gilt § 29 Absatz 4 Satz 1 entsprechend.
(4) [1]Personenbezogene Daten, die durch Maßnahmen nach Absatz 1 erhoben und gespeichert wurden, sind einzuschränken, wenn ihre Verwendung nicht erforderlich ist oder ein Verwendungsverbot besteht, sofern sie nicht zur Information der betroffenen Person benötigt werden. [2]Im Fall der Benachrichtigung nach § 10 Absatz 5 sind eingeschränkte personenbezogene Daten zu löschen, wenn die betroffene Person nicht innerhalb eines Monats nach Benachrichtigung um Rechtsschutz nachgesucht hat. [3]Nach Abschluss des Rechtsschutzverfahrens sind die eingeschränkten personenbezogenen Daten zu löschen.

## § 35 Überwachung und Aufzeichnung der Telekommunikation

(1) [1]Die Vollzugspolizei kann durch Überwachung und Aufzeichnung der Telekommunikation personenbezogene Daten erheben

1. zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person über die in den §§ 4 und 5 des Saarländischen Polizeigesetzes genannten und unter den Voraussetzungen des § 6 des Saarländischen Polizeigesetzes über die dort genannten Personen
2. zur vorbeugenden Bekämpfung der in § 100b der Strafprozessordnung genannten Straftaten über Personen, wenn konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass sie diese Straftaten begehen werden,
3. sowie über solche Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen,
   a) dass sie für eine der in Nummer 1 oder 2 genannten Personen bestimmte oder von ihnen herrührende Mitteilungen entgegennehmen oder weitergeben oder,
   b) dass ihr Telekommunikationsanschluss von einer der in Nummer 1 oder 2 genannten Personen genutzt wird,

soweit die Erforschung des Sachverhalts ohne Gefährdung der Aufgabenerfüllung auf andere Weise aussichtslos oder wesentlich erschwert wäre. [2]Die Erhebung personenbezogener Daten ist nur zulässig bei Telekommunikationsanschlüssen, die von den in den Nummern 1 und 2 genannten Personen mit hoher Wahrscheinlichkeit genutzt werden. [3]Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen sind.

(2) [1]Zur Durchführung von Maßnahmen nach Absatz 1 darf mit technischen Mitteln in informationstechnische Systeme, die von den in Absatz 1 Satz 1 Nummer 1 und 2 genannten Personen genutzt werden, eingegriffen werden, wenn

1. durch technische Maßnahmen sichergestellt ist, dass
   a) ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, oder
   b) die erhobenen Daten nur Inhalte und Umstände der Kommunikation enthalten, die auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können, und
2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

[2]Dabei ist technisch sicherzustellen, dass

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

**[3]**Die eingesetzten technischen Mittel sind nach dem Stand der Technik gegen unbefugte Verwendung zu schützen.

(3) [1]Zur Vorbereitung von Maßnahmen nach Absatz 1 oder 2 darf die Vollzugspolizei durch den Einsatz technischer Mittel die Geräte- und Kartennummer eines mobilen Telekommunikationsendgeräts ermitteln, wenn die Durchführung der Maßnahme nicht möglich oder wesentlich erschwert wäre. [2]Die Vollzugspolizei darf unter den Voraussetzungen des Absatzes 1 Satz 1 durch den Einsatz technischer Mittel auch den Standort eines mobilen Telekommunikationsendgeräts feststellen. [3]Personenbezogene Daten Dritter dürfen anlässlich solcher Maßnahmen nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist. [4]Diese personenbezogenen Daten dürfen über den Datenabgleich zur Ermittlung der Geräte- und Kartennummer oder der Feststellung des Standortes hinaus nicht verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen. [5]Die Maßnahme ist unverzüglich zu beenden, sobald die gesuchten Nummern oder der Standort des jeweiligen Telekommunikationsendgerätes ermittelt sind.

(4) [1]Maßnahmen nach den Absätzen 1 bis 3 dürfen nur durch die Richterin oder den Richter angeordnet werden. [2]Sie sind auf höchstens einen Monat zu befristen. [3]Soweit die Voraussetzungen der Anordnung fortbestehen, sind auf Antrag Verlängerungen um jeweils einen weiteren Monat zulässig. [4]Bei Gefahr im Verzug erfolgt die Anordnung durch die Behördenleitung oder eine von ihr beauftragte Beamtin oder einen von ihr beauftragten Beamten des höheren Polizeivollzugsdienstes; eine richterliche Entscheidung ist unverzüglich nachzuholen. [5]In der schriftlich zu erlassenden Anordnung sind soweit wie möglich Name und Anschrift der Person, gegen die sich die Maßnahme richtet, die Rufnummer oder eine andere Kennung des Telekommunikationsanschlusses oder des Endgerätes, die Art der Maßnahme sowie die tragenden Erkenntnisse für das Vorliegen der Gefahr nach Absatz 1 und die Begründung der Verhältnismäßigkeit der Maßnahme zu bezeichnen. [6]Für das Verfahren gilt § 29 Absatz 4 Satz 1 entsprechend. [7]Soweit eine Maßnahme nach Absatz 3 ausschließlich dazu dient, mittels Feststellung des Standortes eines Telekommunikationsendgerätes den Aufenthaltsort einer vermissten, suizidgefährdeten oder sonstigen hilflosen oder an Leib und Leben gefährdeten Person zu ermitteln, darf sie durch die Behördenleitung angeordnet werden. [8]Diese kann die Anordnungsbefugnis auf besonders beauftragte Polizeivollzugsbeamtinnen oder -beamte übertragen.

(5) Für die Entschädigung der Diensteanbieter ist § 23 des Justizvergütungs- und -entschädigungsgesetzes vom 5. Mai 2004 (BGBl. I S. 718, 776), zuletzt geändert durch Artikel 5 Absatz 2 des Gesetzes vom 11. Oktober 2016 (BGBl. I S. 2222), entsprechend anzuwenden.

(6) Die Beendigung der Maßnahme ist den nach Absatz 5 Verpflichteten mitzuteilen.

(7) § 34 Absatz 4 gilt entsprechend.

### § 36 Erhebung von Telekommunikationsdaten und Nutzungsdaten von Telemedien bei Diensteanbietern

(1) [1]Die Vollzugspolizei kann unter den Voraussetzungen des § 35 Absatz 1 von denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken (Diensteanbieter), verlangen, unverzüglich Auskunft über Verkehrsdaten nach § 96 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 10 Absatz 12 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618) in der jeweils geltenden Fassung zu erteilen. [2]Soweit die Auskunft nach Satz 1 ausschließlich dazu dient, den Aufenthaltsort von Personen zu ermitteln, darf lediglich Auskunft über Verkehrsdaten im jeweils erforderlichen Umfang verlangt werden.
(2) [1]Die Vollzugspolizei kann zur Abwehr einer im Einzelfall bestehenden Gefahr für die öffentliche Sicherheit von dem Diensteanbieter unverzügliche Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen personenbezogenen Daten (Bestandsdaten) verlangen (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). [2]Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Verwendung der Daten vorliegen.
(3) [1]Unter den Voraussetzungen des Absatzes 2 Satz 1 kann die Vollzugspolizei von denjenigen, die geschäftsmäßig eigene oder fremde Telemedien bereithalten oder den Zugang zur Nutzung vermitteln, Auskunft über Bestandsdaten nach § 14 des Telemediengesetzes vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Artikel 1 des Gesetzes vom 28. September 2017 (BGBl. I S. 3530), in der jeweils geltenden Fassung, verlangen. [2]Unter den Voraussetzungen des § 35 Absatz 1 kann die Vollzugspolizei von denjenigen, die geschäftsmäßig eigene oder fremde Telemedien bereithalten oder den Zugang zur Nutzung vermitteln, Auskunft über Nutzungsdaten nach § 15 Absatz 1 des Telemediengesetzes verlangen. [3]Die Auskunft nach den Sätzen 1 und 2 kann auch über zukünftige Bestands- oder Nutzungsdaten angeordnet werden. [4]Der Diensteanbieter hat die Daten auf dem durch die Vollzugspolizei bestimmten Weg zu übermitteln.
(4) Die Auskunft nach Absatz 2 oder 3 darf zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder einer gemeinen Gefahr auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse sowie weiteren zur Individualisierung erforderlicher technischer Daten verlangt werden.
(5) [1]Auskunftsverlangen nach Absatz 1 Satz 2, Absatz 2 Satz 1 und Absatz 3 Satz 1 dürfen durch die Behördenleitung angeordnet werden. [2]Diese kann die Anordnungsbefugnis auf besonders beauftragte Polizeivollzugsbeamtinnen oder -beamte übertragen. [3]Auskunftsverlangen nach Absatz 1 Satz 1, Absatz 2 Satz 2, Absatz 3 Satz 2 und 3 und Absatz 4 dürfen nur durch die Richterin oder den Richter angeordnet werden; zuständig ist das Amtsgericht, in dessen Bezirk die Behörde der Vollzugspolizei ihren Sitz hat. [4]Für das Verfahren gilt § 29 Absatz 4 Satz 1 entsprechend. [5]Bei Gefahr im Verzug erfolgt die Anordnung durch die Behördenleitung oder eine von ihr beauftragte Beamtin oder einen von ihr beauftragten Beamten des höheren Polizeivollzugsdienstes; eine richterliche Entscheidung ist unverzüglich nachzuholen.
(6) Für die Entschädigung der Diensteanbieter gilt § 35 Absatz 5 entsprechend.

### § 37 Unterbrechung von Telekommunikationsverbindungen

(1) [1]Die Vollzugspolizei kann von jedem Diensteanbieter im Sinne von § 3 Nummer 6 des Telekommunikationsgesetzes verlangen, Kommunikationsverbindungen zu unterbrechen oder zu verhindern, wenn dies zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist. [2]Kommunikationsverbindungen Dritter dürfen unter den Voraussetzungen des Satzes 1 nur unterbrochen oder verhindert werden, wenn dies nach den Umständen unvermeidbar ist. [3]Die Unterbrechung oder Verhinderung der Kommunikation ist unverzüglich herbeizuführen und für die Dauer der Anordnung aufrechtzuerhalten.
(2) Unter den Voraussetzungen des Absatzes 1 kann die Vollzugspolizei technische Mittel einsetzen, um Kommunikationsverbindungen zu unterbrechen oder zu verhindern.
(3) [1]Die Anordnung der Maßnahme erfolgt durch die Behördenleitung oder eine von ihr beauftragte Beamtin oder einen von ihr beauftragten Beamten des höheren Polizeivollzugsdienstes unter Festlegung des örtlichen Bereichs, Zeit und Dauer sowie Umfang der Maßnahmen. [2]Eine richterliche Bestätigung über die Fortdauer der Kommunikationsverbindungsunterbrechung oder –verhinderung ist unverzüglich einzuholen. [3]Die Anordnung tritt außer Kraft, wenn nicht binnen drei Tagen vom Richter die Fortdauer der Maßnahme bestätigt wird. [4]Für das Verfahren gilt § 29 Absatz 4 Satz 1 entsprechend.
(4) Für die Entschädigung der Diensteanbieter gilt § 35 Absatz 5 entsprechend.

### § 38 Elektronische Aufenthaltsüberwachung

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

1. bestimmte Tatsachen die Annahme rechtfertigen, dass diese Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat nach § 100a Absatz 1 Nummer 1 in Verbindung mit § 100a Absatz 2 der Strafprozessordnung begehen wird, oder
2. das individuelle Verhalten dieser Person die konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb eines übersehbaren Zeitraums eine in § 129a Absatz 1 und 2 des Strafgesetzbuchs bezeichnete Straftat begehen wird und die dazu bestimmt ist,
   a) die Bevölkerung auf erhebliche Weise einzuschüchtern,
   b) eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder
   c) die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen,

um diese Person durch die Überwachung und die Verarbeitung ihrer personenbezogenen Daten von der Begehung dieser Straftaten abzuhalten. [2]Die Anordnung eines technischen Mittels zur Aufenthaltsüberwachung ist auch zulässig, soweit gegen eine der in Satz 1 genannten Personen ein Aufenthaltsverbot nach § 12 Absatz 3 des Saarländischen Polizeigesetzes verhängt wurde, soweit bestimmte Tatsachen die Annahme rechtfertigen, dass die Personen dort Straftaten nach Satz 1 begehen werden.

(2) [1]Die Vollzugspolizei erhebt und speichert mit Hilfe der betroffenen Person mitgeführten technischen Mittel automatisiert personenbezogene Daten über deren Aufenthaltsort sowie Daten über etwaige Beeinträchtigungen der Datenerhebung. [2]Die erhobenen personenbezogenen Daten dürfen ohne Einwilligung der betroffenen Person nur verarbeitet werden, soweit dies erforderlich ist

1. zur Verhütung oder zur Verfolgung einer der in Absatz 1 bezeichneten Straftaten,
2. zur Feststellung von Verstößen gegen
   a) Aufenthaltsverbote nach § 12 Absatz 3 Satz 1,
   b) Kontaktverbote nach § 12 Absatz 4 Satz 1 Nummer 1 oder
   c) Aufenthaltsgebote nach § 12 Absatz 4 Satz 1 Nummer 2
   des Saarländischen Polizeigesetzes,
3. zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer dritten Person,
4. zur Verfolgung einer Straftat nach Absatz 5 oder
5. zur Aufrechterhaltung der Funktionsfähigkeit der technischen Mittel.

[3]Soweit es technisch möglich ist, ist sicherzustellen, dass innerhalb der Wohnung der betroffenen Person keine über den Umstand ihrer Anwesenheit hinausgehenden personenbezogenen Daten erhoben werden. [4]Zur Einhaltung der Zweckbindung nach Satz 2 hat die Verarbeitung der Daten automatisiert zu erfolgen. [5]Zudem sind die Daten gegen unbefugte Kenntnisnahme und Verarbeitung besonders zu sichern.

(3) [1]Eine Maßnahme nach Absatz 1 darf nur durch die Richterin oder den Richter angeordnet werden. [2]Für das Verfahren gilt das erste Buch des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. [3]Bei Gefahr im Verzug kann die Maßnahme auch durch die Behördenleitung angeordnet werden; in diesem Fall ist unverzüglich eine richterliche Bestätigung der Maßnahme einzuholen. [4]In dem Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, mit Name und Anschrift,
2. Art, Umfang und Dauer der Maßnahme, die Angabe, ob gegenüber der Person, gegen die sich die Maßnahme richtet, ein Aufenthaltsverbot oder Kontaktverbot besteht,
3. der Sachverhalt sowie
4. eine Begründung.

[5]Die Anordnung ergeht schriftlich. [6]In ihr sind anzugeben:

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

[7]Die Anordnung ist sofort vollziehbar und auf höchstens drei Monate zu befristen. [8]Eine Verlängerung um jeweils nicht mehr als drei Monate ist möglich, soweit die Anordnungsvoraussetzungen fortbestehen. [9]Liegen die Voraussetzungen der Anordnung nicht mehr vor, ist die Maßnahme unverzüglich zu beenden. [10]Für das Verfahren gilt § 29 Absatz 4 Satz 1 entsprechend.

(4) [1]Die nach Absatz 2 Satz 1 erhobenen und gespeicherten Daten sind spätestens zwei Monate nach Erhebung zu löschen, soweit sie nicht für die in Absatz 2 Satz 2 genannten Zwecke verwendet werden. [2]Jeder Abruf der Daten ist zu protokollieren. [3]§ 27 Absatz 1 bis 3 gilt entsprechend mit der Maßgabe, dass die Protokolldaten nach zwölf Monaten zu löschen sind. [4]Werden innerhalb der Wohnung der betroffenen Person über den Umstand ihrer Anwesenheit hinausgehende Aufenthaltsdaten erhoben, dürfen diese nicht verarbeitet werden und sind unverzüglich nach Kenntnisnahme zu löschen. [5]Die Tatsache ihrer Kenntnisnahme und Löschung ist zu dokumentieren. [6]Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. [7]Sie ist nach Abschluss der Datenschutzkontrolle zu löschen.

(5) [1]Wer einer gerichtlichen Anordnung nach Absatz 3 Satz 1 zuwiderhandelt und dadurch die kontinuierliche Feststellung ihres oder seines Aufenthaltsortes durch die Vollzugspolizei verhindert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. [2]Die Tat wird nur auf Antrag der Behördenleitung verfolgt; § 82 Absatz 4 des Saarländischen Polizeigesetzes bleibt unberührt.

## § 39 Anlassbezogene automatische Kennzeichenfahndung

(1) [1]Die Vollzugspolizei kann die Kennzeichen von Fahrzeugen ohne Wissen der Person durch den Einsatz technischer Mittel automatisiert erheben, wenn

1. dies zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person erforderlich ist,
2. dies zur Abwehr einer gegenwärtigen Gefahr erforderlich ist und die Voraussetzungen für eine Identitätsfeststellung nach § 9 Absatz 1 Nummer 2 oder 3 des Saarländischen Polizeigesetzes vorliegen oder
3. eine Person oder ein Fahrzeug nach § 40 Absatz 1 ausgeschrieben wurde und Tatsachen die Annahme rechtfertigen, dass die für die Ausschreibung relevante Begehung von Straftaten unmittelbar bevorsteht.

[2]Der Einsatz technischer Mittel nach Satz 1 darf nicht flächendeckend erfolgen.

(2) [1]Die erhobenen Daten können mit zur Abwehr einer Gefahr nach Absatz 1 gespeicherten polizeilichen Daten automatisch abgeglichen werden. [2]Im Trefferfall ist unverzüglich die Datenübereinstimmung zu überprüfen. [3]Bei Datenübereinstimmung können die Daten polizeilich verarbeitet und im Falle des Absatzes 1 Nummer 3 zusammen mit den gewonnenen Erkenntnissen an die ausschreibende Stelle übermittelt werden. [4]Andernfalls sind sie sofort zu löschen.

(3) Die Anordnung und die Durchführung einer Maßnahme nach Absatz 1 sind zu protokollieren. Dabei sind insbesondere festzuhalten

1. Begründung unter Verweis auf Absatz 1 Nummer 1 bis 3,
2. Dauer,
3. Örtlichkeiten, an denen die Maßnahmen durchgeführt werden,
4. die Dateisysteme mit denen der Abgleich erfolgen soll, und
5. die Anzahl der Übereinstimmungen, auch in Relation zur Gesamtzahl erfasster Kennzeichen.

Im Falle der Übermittlung nach Absatz 2 sind zudem die Datenempfänger zu protokollieren. § 27 Absatz 3 gilt entsprechend.

## § 40 Polizeiliche Beobachtung

(1) Die Vollzugspolizei kann zur vorbeugenden Bekämpfung von Straftaten die Personalien einer der in § 17 Absatz 2 Nummer 1 genannten Personen oder das amtliche Kennzeichen der von einer solchen Person benutzten oder eingesetzten Kraftfahrzeuge speichern, damit andere Polizeibehörden das Antreffen der Person oder des Fahrzeuges bei Gelegenheit einer Überprüfung aus anderem Anlass melden (Ausschreibung), soweit

1. tatsächliche Anhaltspunkte dafür vorliegen, dass die Person Straftaten im Sinne des § 31 Absatz 1 begehen wird, oder
2. die Gesamtwürdigung der Person und ihre bisherigen Straftaten erwarten lassen, dass sie auch künftig Straftaten von erheblicher Bedeutung begehen wird.

(2) [1]Die Anordnung der Ausschreibung ist nur zulässig, wenn Tatsachen die Annahme rechtfertigen, dass die gemeldeten Erkenntnisse über das Antreffen der Person oder der Kraftfahrzeuge für die vorbeugende Bekämpfung von Straftaten im Sinne des Absatzes 1 erforderlich sind. [2]Die Maßnahme darf nur durch die Behördenleiterin oder den Behördenleiter angeordnet werden.

(3) [1]Die Anordnung ist auf höchstens ein Jahr zu befristen. Spätestens nach Ablauf von sechs Monaten ist zu prüfen, ob die Voraussetzungen für die Anordnung noch bestehen; das Ergebnis dieser Prüfung ist aktenkundig zu machen. [2]Zur Verlängerung der Laufzeit bedarf es einer neuen Anordnung.

(4) Liegen die Voraussetzungen für die Anordnung nicht mehr vor, ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, ist die Ausschreibung unverzüglich zu löschen.

## § 41 Schutz des Kernbereichs privater Lebensgestaltung und Schutz zeugnisverweigerungsberechtigter Personen

(1) [1]Maßnahmen nach § 34 Absatz 1 dürfen nur angeordnet und durchgeführt werden, soweit auf Grund tatsächlicher Anhaltspunkte, insbesondere zu der Art der zu überwachenden Räumlichkeiten und dem Verhältnis der zu überwachenden Personen zueinander, anzunehmen ist, dass durch die Überwachung Äußerungen, die überhaupt Erkenntnisse aus dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. [2]Die Erhebung personenbezogener Daten ist weiter nicht zulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch

1. Maßnahmen nach § 31 Absatz 2 Nummer 1, 2 oder 4,
2. die offene Anfertigung von Bild- und Tonaufzeichnungen nach § 32 Absatz 3 Satz 2,
3. die Überwachung und Aufzeichnung der Telekommunikation nach § 35 Absatz 1 oder 2 oder
4. die Erhebung von Verkehrs-, Bestands- oder Nutzungsdaten nach § 36 Absatz 1, 2 oder 4

ausschließlich Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden.

(2) [1]Wird bei einer der in Absatz 1 bezeichneten Maßnahmen erkennbar, dass dennoch personenbezogene Daten erhoben werden, die dem Kernbereich privater Lebensgestaltung zuzuordnen sind, ist die Datenerhebung unverzüglich und so lange wie erforderlich zu unterbrechen; im Zweifelsfall dürfen automatisierte Aufzeichnungen fortgesetzt werden. [2]Automatisiert aufgezeichnete personenbezogene Daten, die durch eine Maßnahme nach § 34 Absatz 1 erhoben wurden, sind unverzüglich und vor ihrer Sichtung durch die Vollzugspolizei der zuständigen Richterin oder dem zuständigen Richter zur Entscheidung über die Rechtmäßigkeit der Erhebung oder Löschung der personenbezogenen Daten vorzulegen. [3]Zuständig ist die Richterin oder der Richter, welche oder welcher die ursprüngliche Anordnung getroffen hat. [4]Bei Gefahr im Verzug erfolgt in den Fällen des Satzes 2 eine Prüfung durch zwei Bedienstete der Vollzugspolizei, von denen eine oder einer dem Laufbahnabschnitt des höheren Polizeivollzugsdienstes angehören muss. [5]Die richterliche Entscheidung ist unverzüglich nachzuholen.[6]Personenbezogene Daten, die durch

1. eine Maßnahme nach § 31 Absatz 2 Nummer 1, 2 oder 4,
2. die offene Anfertigung von Bild- und Tonaufzeichnungen in Wohnungen nach § 32 Absatz 3 Satz 2,
3. durch die Überwachung und Aufzeichnung der Telekommunikation nach § 35 Absatz 1 oder 2 oder
4. eine Maßnahme nach § 36 Absatz 1, 2 oder 4

erhoben wurden, sind durch zwei Bedienstete der Vollzugspolizei, von denen eine oder einer dem Laufbahnabschnitt des höheren Polizeidienstes angehören muss, sowie der oder dem Datenschutzbeauftragten der Polizeibehörde auf kernbereichsrelevante Inhalte hin zu prüfen. [6]Im Zweifelsfall entscheidet die zuständige Richterin oder der zuständige Richter über die Verwertbarkeit oder Löschung der personenbezogenen Daten. [7]Soweit Maßnahmen nach Absatz 1 ohne richterliche Anordnung durchgeführt wurden, ist das Amtsgericht zuständig, in dessen Bezirk die Behörde der Vollzugspolizei ihren Sitz hat. [8]Für das Verfahren gilt § 29 Absatz 4 Satz 1 entsprechend.

(3) [1]Soweit zweifelsfrei aus dem Kernbereich privater Lebensgestaltung stammende personenbezogene Daten bereits erhoben und gespeichert worden sind, sind diese unverzüglich zu löschen. [3] Personenbezogene Daten, bei denen sich nach Auswertung herausstellt, dass sie dem Kernbereich privater Lebensgestaltung zuzuordnen sind, sind ebenfalls unverzüglich zu löschen. [4]Die Tatsachen der Erhebung, Speicherung und Löschung sind ohne Hinweis auf den tatsächlichen Inhalt der personenbezogenen Daten zu dokumentieren. [5]§ 10 Absatz 5 Satz 2 und § 42 Absatz 4 Satz 2 gelten entsprechend.

(4) [1]Verdeckte Maßnahmen im Sinn der §§ 31, 35 und 36, die sich gegen eine in § 53 Absatz 1 Satz 1 Nummer 1, 2, 3 oder Nummer 4 der Strafprozessordnung genannte Person richten und voraussichtlich Erkenntnisse erbringen würden, über die diese Person das Zeugnis verweigern dürfte, sind unzulässig. [2]Dennoch erlangte Erkenntnisse dürfen nicht verwertet werden. [3]Aufzeichnungen hierüber sind unverzüglich zu löschen. [4]Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. [5]Die Sätze 3 bis 5 gelten entsprechend, wenn durch eine Maßnahme, die sich nicht gegen eine in § 53 Absatz 1 Satz 1 Nummer 1, 2, 3 oder Nummer 4 der Strafprozessordnung genannte Person richtet, von einer dort genannten Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte. [6]Für Personen nach § 53 Absatz 1 Satz 1 Nummer 3 der Strafprozessordnung gelten die Sätze 1 bis 5 nur, soweit es sich um Rechtsanwälte oder Kammerrechtsbeistände handelt.
(5) [1]Soweit durch eine Maßnahme eine in § 53 Absatz 1 Satz 1 Nummer 3, 3a und 3b oder Nummer 5 der Strafprozessordnung genannte Person betroffen wäre und dadurch voraussichtlich Erkenntnisse erlangt würden, über die diese Person das Zeugnis verweigern dürfte, ist dies im Rahmen der Prüfung der Verhältnismäßigkeit unter Würdigung des öffentlichen Interesses an den von dieser Person wahrgenommenen Aufgaben und des Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. [2]Soweit hiernach geboten, ist die Maßnahme zu unterlassen oder, soweit dies nach der Art der Maßnahme möglich ist, zu beschränken. [3]Für Personen nach § 53 Absatz 1 Satz 1 Nummer 3 der Strafprozessordnung gelten die Sätze 1 und 2 nur, soweit es sich nicht um Rechtsanwälte oder Kammerrechtsbeistände handelt.
(6) Die Absätze 4 und 5 gelten entsprechend, soweit die in § 53a der Strafprozessordnung genannten Personen das Zeugnis verweigern dürften.
(7) Die Absätze 4 bis 6 gelten nicht, sofern Tatsachen die Annahme rechtfertigen, dass die zeugnisverweigerungsberechtigte Person für die Gefahr verantwortlich ist.

### § 42 Protokollierung verdeckter oder eingriffsintensiver Maßnahmen

(1) Bei der Erhebung personenbezogener Daten nach § 29, § 31 Absatz 2, § 32 Absatz 3 Satz 2, § 34 Absatz 1 und 3, § 35 Absatz 1, 2 und 3, § 36 Absatz 1, 3 und 4 Satz 2 und 3, § 40 sind zu protokollieren

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

(2) Zu protokollieren sind je nach Durchführung der konkreten Maßnahme auch bei

1. Maßnahmen nach § 29 die im Übermittlungsersuchen nach § 29 Absatz 2 enthaltenen Merkmale und die betroffenen Personen, gegen die nach Auswertung der Daten weitere Maßnahmen getroffen wurden,
2. Maßnahmen nach § 31 Absatz 2 Nummer 1 bis 5, bei denen Vorgänge außerhalb von Wohnungen erfasst wurden, die Zielperson und die erheblich mitbetroffenen Personen,
3. Maßnahmen nach § 32 Absatz 3 Satz 2 alle betroffenen Personen sowie die Personen, deren Wohnung betreten wurde,
4. Maßnahmen nach § 34 Absatz 1 die Person, gegen die sich die Maßnahme richtete, sonstige überwachte Personen und die Personen, die die überwachte Wohnung zur Zeit der Durchführung der Maßnahme innehatten oder bewohnten,
5. Maßnahmen nach § 34 Absatz 3 und nach § 31 Absatz 2 Nummer 3 und 4, bei denen Vorgänge innerhalb von Wohnungen erfasst wurden, die Zielperson, die erheblich mitbetroffenen Personen und die Personen, deren nicht allgemein zugängliche Wohnung betreten wurde,
5. Maßnahmen nach § 35 Absatz 1 die Beteiligten der überwachten Telekommunikation,

6. Maßnahmen nach § 35 Absatz 2 die Beteiligten der überwachten Telekommunikation und die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
7. Maßnahmen nach § 35 Absatz 3 die Zielperson,
8. Maßnahmen nach § 36 Absatz 1 die Beteiligten der betroffenen Telekommunikation,
9. Maßnahmen nach § 36 Absatz 3 die festgestellte Person,
10. Maßnahmen nach § 36 Absatz 4 Satz 2 und 3 die Nutzerin oder der Nutzer,
11. Maßnahmen nach § 40 die Zielperson und die Personen, deren personenbezogene Daten gemeldet worden sind.

(3) [1]Nachforschungen zur Feststellung der Identität einer in Absatz ~~5~~ 2 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist. [2]Die Zahl der Personen, deren Protokollierung unterblieben ist, ist im Protokoll anzugeben.
(4) [1]Die Daten nach den Absätzen 1 und 2 dürfen nur verwendet werden für die Zwecke der Benachrichtigung nach § 10 und um eine Prüfung zu ermöglichen, ob die Maßnahme rechtmäßig durchgeführt worden ist. [2]Sie sind bis zum Ablauf der Datenschutzkontrolle nach § 5 Absatz 2 aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 1 genannten Zweck noch erforderlich sind.

## Vierter Teil
## Übermittlung personenbezogener Daten

### 1. Abschnitt
### Allgemeine Regelungen

### § 43 Allgemeine Regeln der Übermittlung personenbezogener Daten

(1) [1]Die Polizei darf personenbezogene Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck übermitteln, zu dem sie die personenbezogenen Daten erlangt oder gespeichert hat; § 23 gilt entsprechend. [2]Abweichend hiervon kann die Polizei personenbezogene Daten übermitteln, soweit das zur Abwehr einer Gefahr erforderlich ist und die Empfängerin oder der Empfänger die personenbezogenen Daten auf andere Weise nicht oder nicht rechtzeitig oder nur mit unverhältnismäßig hohem Aufwand erlangen kann. [3]Während eines laufenden Ermittlungsverfahrens bedarf die Übermittlung von personenbezogenen Daten im Sinne des § 23 Absatz 4 und 5 der Zustimmung der für die Ermittlung zuständigen Staatsanwaltschaft.
(2) [1]Die über Personen nach § 17 Absatz 2 Nummer 1 bis 7 gespeicherten personenbezogenen Daten dürfen nur an die Vollzugspolizei übermittelt werden. [2]Bewertungen dürfen nur an Polizeibehörden übermittelt werden.
(3) 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 Übermittlung personenbezogener Daten durch die Polizei nur zulässig, wenn die Empfängerin oder der Empfänger die personenbezogenen Daten zur Erfüllung des gleichen Zwecks benötigt, zu dem sie die Polizei erlangt hat.
(4) [1]Die übermittelnde Polizeibehörde prüft die Zulässigkeit der Übermittlung personenbezogener Daten. [2]Erfolgt die Übermittlung personenbezogener Daten auf Grund eines Ersuchens der Empfängerin oder des Empfängers, hat diese oder dieser der übermittelnden Polizeibehörde die zur Prüfung erforderlichen Angaben zu machen.

[3]Bei Ersuchen von Polizeibehörden sowie anderen Behörden und öffentlichen Stellen prüft die übermittelnde Polizeibehörde nur, ob das Ersuchen im Rahmen der Aufgaben der Empfängerin oder des Empfängers liegt, es sei denn, im Einzelfall besteht Anlass zur Überprüfung der Rechtmäßigkeit des Ersuchens. [4]Die übermittelnde Polizeibehörde protokolliert jede Übermittlung personenbezogener Daten; § 42 gilt entsprechend.
(5) [1]Die übermittelnde Polizeibehörde hat angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig oder nicht mehr aktuell sind, nicht übermittelt oder sonst zur Verfügung gestellt werden. [2]Zu diesem Zweck ist, soweit dies mit angemessenem Aufwand möglich ist, die Qualität der Daten vor ihrer Übermittlung oder Bereitstellung zu überprüfen. [3]Bei jeder Übermittlung personenbezogener Daten sind zudem, soweit dies möglich und angemessen ist, Informationen beizufügen, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der Daten sowie deren Aktualität zu beurteilen.
(6) [1]Gelten für die Verarbeitung von personenbezogenen Daten besondere Rechtsvorschriften, hat die übermittelnde Stelle die Empfängerin oder den Empfänger auf diese Vorschriften und die Pflicht zu ihrer Beachtung hinzuweisen. [2]Die Hinweispflicht kann dadurch erfüllt werden, dass die Daten entsprechend markiert werden.
(7) [1]Die Empfängerin oder der Empfänger darf die übermittelten personenbezogenen Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verwenden, zu dem sie ihr oder ihm übermittelt worden sind. [2]Die Empfängerin oder der Empfänger ist darauf hinzuweisen, dass die übermittelten personenbezogenen Daten nur zu dem Zweck verwendet werden dürfen, zu dessen Erfüllung sie übermittelt wurden. [3]Stellt die Empfängerin oder der Empfänger fest, dass die übermittelten personenbezogenen Daten zu berichtigen sind, ist dies der übermittelnden Polizeibehörde mitzuteilen.
(8) [1]Stellt die übermittelnde Polizeibehörde fest, dass personenbezogene Daten übermittelt wurden, die zu berichtigen, einzuschränken oder zu löschen sind, ist dies der Empfängerin oder dem Empfänger mitzuteilen, es sei denn, dass die Mitteilung für die Beurteilung der betroffenen Person oder des Sachverhalts nicht oder nicht mehr wesentlich ist. [2]Die Empfängerin oder der Empfänger hat die Daten zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken. [3]Der übermittelnden Stelle ist auf deren Ersuchen zu Zwecken der Datenschutzkontrolle Auskunft darüber zu erteilen, wie die übermittelten personenbezogenen Daten verarbeitet worden sind.
(9) Soweit gesetzlich nichts anderes geregelt ist, unterbleibt die Übermittlung personenbezogener Daten, soweit Grund zu der Annahme besteht, dass dadurch gegen den Zweck eines Gesetzes verstoßen würde oder schutzwürdige Belange der betroffenen Person beeinträchtigt würden.
(10) Anderweitige besondere Rechtsvorschriften über die Übermittlung personenbezogener Daten bleiben unberührt.

### § 44 Übermittlung personenbezogener Daten zwischen Polizeibehörden

[1]Zwischen Polizeibehörden können personenbezogene Daten übermittelt werden, soweit das zur Erfüllung polizeilicher Aufgaben erforderlich ist. [2]§ 23 gilt entsprechend. [3]Es können insbesondere übermittelt werden:

1. Lagebilder einschließlich Tagesberichte über aktuelle Geschehnisse,
2. sachbezogene Erkenntnisse sowie personenbezogene Daten, soweit sie für die Abwehr von Gefahren oder Verhütung und Aufklärung künftiger Straftaten von Bedeutung sein können und eine Speicherung gemäß § 23 Absatz 4 oder 5 zulässig ist,
3. Beobachtungs- und Feststellungsberichte über verdächtige Vorkommnisse und Personen,
4. Fahndungsdaten zu polizeilich gesuchten Personen.

### § 45 Übermittlung personenbezogener Daten an Behörden, öffentliche oder sonstige Stellen

[1]Sind andere Behörden oder öffentliche Stellen für die Gefahrenabwehr zuständig, kann die Polizei diesen Behörden oder öffentlichen Stellen die bei ihr vorhandenen personenbezogenen Daten übermitteln, soweit die Kenntnis dieser personenbezogenen Daten zur Erfüllung der Aufgaben der Empfängerin oder des Empfängers erforderlich ist; § 44 gilt entsprechend. [2]Im Übrigen kann die Polizei personenbezogene Daten an Behörden und öffentliche Stellen sowie an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit dies

1. durch Rechtsvorschrift zugelassen,
2. unter Beachtung des § 23 zulässig und zur Erfüllung ihrer Aufgaben nach diesem Gesetz erforderlich ist oder
3. an die Fachhochschule für Verwaltung des Saarlandes zu den in § 23 Absatz 7 genannten Zwecken.

### § 46 Automatisiertes Abrufverfahren und Datenverbund

(1) [1]Bei der Vollzugspolizei ist die Einrichtung eines automatisierten Verfahrens, das die Verarbeitung, insbesondere die Übermittlung, personenbezogener Daten durch Abruf aus einem Dateisystem ermöglicht, zulässig, soweit diese Form der Übermittlung personenbezogener Daten unter Berücksichtigung der schutzwürdigen Belange der betroffenen Person und der Erfüllung der polizeilichen Aufgaben angemessen ist. [2]Datenempfangende Stelle, Verantwortliche, Abrufberechtigte, Datenart und Zweck des Abrufs sind festzulegen. [3]Die Einrichtung des Abrufverfahrens bedarf der Zustimmung des Ministeriums für Inneres, Bauen und Sport. [4]Unbeschadet des § 59 ist die oder der Landesbeauftragte für Datenschutz über die erfolgte Einrichtung eines automatisierten Abrufverfahrens zu unterrichten.
(2) [1]Das Ministerium für Inneres, Bauen und Sport ist berechtigt, zur Erfüllung polizeilicher Aufgaben einen Datenverbund zu vereinbaren, der eine automatisierte Übermittlung personenbezogener Daten zwischen den Polizeibehörden des Landes, der Bundesländer, des Bundes und den in § 48 genannten ausländischen Stellen ermöglicht. [2]Dies gilt auch für über- oder zwischenstaatliche Stellen. [3]Absatz 1 Satz 4 gilt entsprechend.

## 2. Abschnitt
## Grenzüberschreitender Datenverkehr innerhalb der Europäischen Union

### § 47 Verarbeitung personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union übermittelt worden sind

(1) [1]Personenbezogene Daten, die von einem der Mitgliedstaaten der Europäischen Union an die Vollzugspolizei übermittelt worden sind, dürfen ohne Zustimmung der übermittelnden Stelle nur für die Zwecke verarbeitet werden, für die sie übermittelt worden sind. [2]Die Zustimmung kann bereits bei Gelegenheit der Übermittlung erteilt werden. [3]Einer Zustimmung bedarf es nicht, wenn die betroffene Person eingewilligt hat oder die Verarbeitung erforderlich ist

1. zur Verhütung von Straftaten, zur Strafverfolgung oder zur Strafvollstreckung,
2. für andere justizielle oder verwaltungsbehördliche Verfahren, die mit der Verhütung von Straftaten, der Strafverfolgung oder der Strafvollstreckung unmittelbar zusammenhängen oder
3. zur Abwehr einer gegenwärtigen erheblichen Gefahr für die öffentliche Sicherheit.

(2) [1]Die Vollzugspolizei hat von der übermittelnden Stelle mitgeteilte Bedingungen und besondere Verarbeitungsbeschränkungen, insbesondere Fristen, nach deren Ablauf die Daten zu löschen, einzuschränken oder auf die Erforderlichkeit ihrer fortgesetzten Speicherung zu prüfen sind, zu beachten. [2]Hat die übermittelnde Stelle eine nach ihrem innerstaatlichen Recht geltende Einschränk- oder Löschfrist mitgeteilt, dürfen die personenbezogenen Daten nach Ablauf dieser Frist nur noch für laufende Strafverfolgungs- oder Strafvollstreckungsverfahren verarbeitet werden.
(3) Die nach Absatz 1 übermittelten personenbezogenen Daten dürfen an nichtöffentliche Stellen innerhalb der europäischen Union nur mit Zustimmung der übermittelnden Stelle übermittelt werden, soweit dies zur

1. Verhütung von Straftaten,
2. Strafverfolgung,
3. Strafvollstreckung,
4. Abwehr einer gegenwärtigen erheblichen Gefahr für die öffentliche Sicherheit oder
5. Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Einzelner

erforderlich ist und überwiegende schutzwürdige Interessen der betroffenen Person nicht entgegenstehen.
(4) Die Absätze 1 bis 3 gelten entsprechend für Schengen-assoziierte Staaten sowie Behörden und Informationssysteme, die aufgrund des Vertrages über die Europäische Union oder des Vertrages zur Gründung der Europäischen Gemeinschaft errichtet worden sind.
(5) Die nach Absatz 1 übermittelten personenbezogenen Daten dürfen an Stellen außerhalb der Mitgliedstaaten der Europäischen Union und der in Absatz 4 genannten Stellen oder an dort ansässige internationale Organisationen nur unter den Voraussetzungen der §§ 49 bis 52 übermittelt werden.

### § 48 Datenübermittlung an Polizeibehörden und öffentliche Stellen der Europäischen Union, der Mitgliedstaaten und der assoziierten Staaten

(1) Im Rahmen der grenzüberschreitenden Zusammenarbeit ist die Übermittlung personenbezogener Daten nach Maßgabe der §§ 44 bis 46 an Polizeibehörden und sonstige öffentliche Stellen

1. anderer Mitgliedstaaten der Europäischen Union,
2. der Staaten, in denen der Schengen-Besitzstand gemäß Artikel 1 Absatz 2 des Beschlusses 1999/435/EG des Rates vom 20. Mai 1999 (ABl. L 239 vom 22. Dezember 2000, S. 1) angewandt wird, oder
3. der Europäischen Union

unter Beachtung des Dienstweges nach den Absätzen 2 und 3 zulässig.
(2) [1]Die Übermittlung personenbezogener Daten erfolgt grundsätzlich über das Bundeskriminalamt als zentraler Stelle der Bundesrepublik Deutschland an die jeweilige nationale zentrale Stelle. [2]Im Eilfall kann die Übermittlung unmittelbar an die zuständigen nationalen Polizeibehörden des jeweiligen Vertragsstaates erfolgen. [3]Die zentralen Stellen der betroffenen Vertragsstaaten sind jedoch über das Bundeskriminalamt unverzüglich zu unterrichten.
(3) Im Grenzbereich übermittelt das Landespolizeipräsidium im Rahmen seiner Zuständigkeit und auf der Grundlage der bestehenden bilateralen Vereinbarungen sowie unter Beachtung der innerstaatlichen Benachrichtigungspflichten personenbezogene Daten an die zuständigen Polizeibehörden in Frankreich und Luxemburg, insbesondere in Frankreich an die Groupements der Gendarmerie Nationale und die Directions Départementales der Police Nationale in den Départements Niederrhein, Hochrhein und Mosel und in Luxemburg an die Direction Générale der Police Grand Ducal über die dortige zentrale Stelle und an die Nachbardienststellen.

## 3. Abschnitt
## Übermittlung personenbezogener Daten an Drittstaaten und an internationale Organisationen

### § 49 Allgemeine Voraussetzungen

(1) [1]Die Übermittlung personenbezogener Daten durch die Vollzugspolizei an Stellen außerhalb der Mitgliedstaaten und der in § 47 Absatz 4 genannten Stellen (Drittstaaten) oder an dort ansässige internationale Organisationen ist bei Vorliegen der übrigen für Datenübermittlungen geltenden Voraussetzungen zulässig, wenn

1. die Stelle oder internationale Organisation für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten oder die Abwehr von Gefahren zuständig ist und
2. die Europäische Kommission gemäß Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 einen Angemessenheitsbeschluss gefasst hat.

[2]§ 43 Absatz 9 bleibt unberührt.

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

(3) [1]Wenn personenbezogene Daten, die von einem der Mitgliedstaaten der Europäischen Union oder einer in § 47 Absatz 4 genannten Stelle übermittelt oder zur Verfügung gestellt wurden, nach Absatz 1 übermittelt werden sollen, muss diese Übermittlung zuvor von der jeweils ursprünglich zuständigen Stelle genehmigt werden. [2]Übermittlungen ohne vorherige Genehmigung sind nur dann zulässig, wenn die Übermittlung erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Staates oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. [3]Im Fall des Satzes 2 ist die Stelle des anderen Mitgliedstaats, die für die Erteilung der Genehmigung zuständig gewesen wäre, unverzüglich über die Übermittlung zu unterrichten. [4]Für die Übermittlung personenbezogener Daten an nicht öffentliche Stellen gilt § 47 Absatz 3 entsprechend.

(4) [1]Werden personenbezogene Daten nach Absatz 1 übermittelt, ist durch geeignete Maßnahmen sicherzustellen, dass die Empfängerin oder der Empfänger die übermittelten Daten nur dann an andere Drittstaaten oder andere internationale Organisationen weiterübermittelt, wenn die Vollzugspolizei diese Übermittlung zuvor genehmigt hat. [2]Bei der Entscheidung über die Erteilung der Genehmigung hat die Vollzugspolizei alle maßgeblichen Faktoren zu berücksichtigen, insbesondere die Schwere der Straftat, den Zweck der ursprünglichen Übermittlung und das in dem Drittstaat oder der internationalen Organisation, an das oder an die die Daten weiterübermittelt werden sollen, bestehende Schutzniveau für personenbezogene Daten. [3]Die Genehmigung darf nur dann erteilt werden, wenn auch eine direkte Übermittlung an den anderen Drittstaat oder die andere internationale Organisation zulässig wäre. [4]Die Zuständigkeit für die Erteilung der Genehmigung kann auch abweichend geregelt werden.

### § 50 Datenübermittlung bei geeigneten Garantien

(1) Liegt entgegen § 49 Absatz 1 Nummer 2 kein Beschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor, ist die Übermittlung personenbezogener Daten durch die Vollzugspolizei bei Vorliegen der übrigen Voraussetzungen des § 49 auch dann zulässig, wenn

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

§ 43 Absatz 9 bleibt unberührt.

(2) [1]Die Vollzugspolizei hat Übermittlungen nach Absatz 1 Nummer 2 zu dokumentieren. [2]Die Dokumentation hat den Zeitpunkt der Übermittlung, die Identität der Empfängerin oder des Empfängers, den Grund der Übermittlung und die übermittelten personenbezogenen Daten zu enthalten. [3]Die Dokumentation ist der oder dem Landesbeauftragten für Datenschutz auf Anforderung zur Verfügung zu stellen.

(3) [1]Die Vollzugspolizei hat die Landesbeauftragte oder den Landesbeauftragten für Datenschutz zumindest jährlich über Übermittlungen zu unterrichten, die aufgrund einer Beurteilung nach Absatz 1 Nummer 2 erfolgt sind. [2]In der Unterrichtung kann er die Empfängerinnen und Empfänger sowie die Übermittlungszwecke angemessen kategorisieren.

### § 51 Datenübermittlung ohne geeignete Garantien

(1) [1]Liegt entgegen § 49 Absatz 1 Nummer 2 kein Beschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor und liegen auch keine geeigneten Garantien im Sinne des § 50 Absatz 1 vor, ist die Übermittlung personenbezogener Daten durch die Vollzugspolizei bei Vorliegen der übrigen Voraussetzungen des § 49 auch dann zulässig, wenn die Übermittlung erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer natürlichen Person,
2. zur Wahrung berechtigter Interessen der betroffenen Person,
3. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Staates,
4. im Einzelfall für Zwecke der Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten oder der Abwehr von gegenwärtigen und erheblichen Gefahren oder
5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in Nummer 4 aufgeführten genannten Zwecken.

[2]§ 43 Absatz 9 bleibt unberührt.

(2) Für Übermittlungen nach Absatz 1 gilt § 50 Absatz 2 entsprechend.

### § 52 Sonstige Datenübermittlung an Empfänger in Drittstaaten

(1) [1]Die Vollzugspolizei kann bei Vorliegen der übrigen für die Übermittelung personenbezogener Daten in Drittstaaten geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten unmittelbar an nicht in § 49 Absatz 1 Nummer 1 genannte Stellen in Drittstaaten übermitteln, wenn die Übermittlung für die Erfüllung ihrer Aufgaben unbedingt erforderlich ist und

1. im konkreten Fall keine Grundrechte der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen,
2. die Übermittlung an die in § 49 Absatz 1 Nummer 1 genannten Stellen wirkungslos oder ungeeignet wäre, insbesondere, weil sie nicht rechtzeitig durchgeführt werden kann, und

3. die Vollzugspolizei dem Empfänger die Zwecke der Verarbeitung mitteilt und ihn darauf hinweist, dass die übermittelten Daten nur in dem Umfang verarbeitet werden dürfen, in dem ihre Verarbeitung für diese Zwecke erforderlich ist.

[2]§ 43 Absatz 9 und § 46 Absatz 3 bleiben unberührt.

(2) Im Fall des Absatzes 1 hat die Vollzugspolizei die in § 49 Absatz 1 Nummer 1 genannten Stellen unverzüglich über die Übermittlung zu unterrichten, sofern dies nicht wirkungslos oder ungeeignet ist.

(3) Für Übermittlungen nach Absatz 1 gilt § 50 Absatz 2 und 3 entsprechend.

(4) Bei Übermittlungen nach Absatz 1 hat die Vollzugspolizei die Empfängerinnen oder den Empfänger zu verpflichten, die übermittelten personenbezogenen Daten ohne ihre Zustimmung nur für den Zweck zu verarbeiten, für den sie übermittelt worden sind.

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

## Fünfter Teil
## Besondere Regelungen für die Verarbeitung personenbezogener Daten und die Auftragsverarbeitung

### 1. Abschnitt
### Allgemeine Vorschriften

### § 53 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) [1]Die Polizei hat sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst angemessene Vorkehrungen zu treffen, die geeignet sind, die Datenschutzgrundsätze wie etwa die Datensparsamkeit wirksam umzusetzen, und die sicherstellen, dass die gesetzlichen Anforderungen eingehalten und die Rechte der betroffenen Person geschützt werden. [2]Hierbei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Person zu berücksichtigen. [3]Insbesondere sind die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. [4]Personenbezogene Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verarbeitungszweck möglich ist.

(2) [1]Die Polizei hat geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden können, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. [2]Dies betrifft die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. [3]Die Maßnahmen müssen insbesondere gewährleisten, dass die Daten durch Voreinstellungen nicht automatisiert einer unbestimmten Anzahl von Personen zugänglich gemacht werden können.

### § 54 Gemeinsam Verantwortliche

[1]Legen zwei oder mehr Polizeibehörden gemeinsam die Zwecke und die Mittel der Verarbeitung fest, gelten sie als gemeinsame Verantwortliche im Sinne des § 2 Absatz 8. [2]Sie haben ihre jeweiligen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten in transparenter Form in einer Vereinbarung festzulegen, soweit diese nicht bereits in Rechtsvorschriften festgelegt sind.

[3]Aus der Vereinbarung muss insbesondere hervorgehen, wer welchen Informationspflichten nachzukommen hat und wie und gegenüber wem die betroffene Person ihre Rechte wahrnehmen kann. [4]Eine entsprechende Vereinbarung hindert die betroffene Person nicht, ihre Rechte gegenüber jeder der gemeinsam Verantwortlichen geltend zu machen.

### § 55 Durchführung einer Datenschutz-Folgenabschätzung

(1) [1]Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person zur Folge, hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffene Person durchzuführen. [2]Die oder der Datenschutzbeauftragte ist an der Durchführung der Datenschutz-Folgenabschätzung zu beteiligen.
(2) Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohem Gefahrenpotential kann eine gemeinsame Datenschutz-Folgenabschätzung vorgenommen werden.
(3) Die Datenschutz-Folgenabschätzung hat den Rechten der von der Verarbeitung betroffenen Person Rechnung zu tragen und zumindest Folgendes zu enthalten:

1. Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,
2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck,
3. eine Bewertung der Gefahren für die Rechtsgüter der betroffenen Person und
4. die Maßnahmen, mit denen bestehenden Gefahren abgeholfen werden soll, einschließlich der Garantien, der Sicherheitsvorkehrungen und der Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden sollen.

(4) Soweit erforderlich, ist eine Überprüfung durchzuführen, ob die Verarbeitung den Maßgaben folgt, die sich aus der Datenschutz-Folgenabschätzung ergeben haben.

### § 56 Zusammenarbeit mit der oder dem Landesbeauftragten für Datenschutz

Die Polizei hat mit der oder dem Landesbeauftragten für Datenschutz bei der Erfüllung ihrer oder seiner Aufgaben zusammenzuarbeiten.

## 2. Abschnitt
## Auftragsverarbeitung

### § 57 Auftragsverarbeitung

(1) [1]Werden personenbezogene Daten im Auftrag durch andere Personen oder Stellen verarbeitet, hat die jeweilige Polizeibehörde (Auftragsgeberin) für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Schutz personenbezogener Daten zu sorgen. [2]Die Rechte der betroffenen Person auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Schadensersatz sind in diesem Fall gegenüber der Auftragsgeberin geltend zu machen.
(2) Die Auftragsgeberin darf nur solche Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragen, die mit geeigneten technischen und organisatorischen Maßnahmen sicherstellen, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(3) [1]Auftragsverarbeiter dürfen ohne vorherige schriftliche Genehmigung der Auftragsgeberin keine weiteren Auftragsverarbeiter hinzuziehen. [2]Wurde dem Auftragsverarbeiter eine allgemeine Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter erteilt, hat der Auftragsverarbeiter die Auftragsgeberin über jede beabsichtigte Hinzuziehung oder Ersetzung zu informieren. [3]In diesem Fall kann die Hinzuziehung oder Ersetzung untersagt werden.
(4) [1]Zieht ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter hinzu, so hat er diesem dieselben Verpflichtungen aus dem Vertrag oder Rechtsinstrument nach Absatz 5 aufzuerlegen, die auch für ihn gelten, soweit diese Pflichten für den weiteren Auftragsverarbeiter nicht schon aufgrund anderer Vorschriften verbindlich sind. [2]Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.
(5) [1]Die Verarbeitung durch einen Auftragsverarbeiter hat auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments zu erfolgen, der oder das den Auftragsverarbeiter an die Auftragsgeberin bindet und der oder das den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten der Auftragsgeberin festlegt. [2]Der Vertrag oder das andere Rechtsinstrument haben insbesondere vorzusehen, dass der Auftragsverarbeiter

1. nur auf dokumentierte Weisung der Auftragsgeberin handelt; ist der Auftragsverarbeiter der Auffassung, dass eine Weisung rechtswidrig ist, hat er die Auftragsgeberin unverzüglich zu informieren,
2. gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden, soweit sie keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen,
3. die Auftragsgeberin mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten,
4. alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl der Auftragsgeberin zurückgibt oder löscht und bestehende Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht,
5. der Auftragsgeberin alle erforderlichen Informationen, insbesondere die gemäß § 27 Absatz 1 erstellten Protokolldaten, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt,
6. Überprüfungen, die von der Auftragsgeberin oder einer oder einem von dieser oder diesem beauftragten Prüferin oder Prüfer durchgeführt werden, ermöglicht und dazu beiträgt,
7. die in den Absätzen 3 und 4 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält,
8. alle nach § 53 erforderlichen Maßnahmen ergreift und
9. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen die Auftragsgeberin bei der Einhaltung der in den §§ 55, 58 und 61 genannten Pflichten unterstützt.

(6) Der Vertrag nach Absatz 5 ist schriftlich oder elektronisch abzufassen.
(7) Ein Auftragsverarbeiter, der die Zwecke und Mittel der Verarbeitung unter Verstoß gegen diese Vorschrift bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher im Sinne des § 2 Absatz 8.
(8) [1]Sofern die Vorschriften dieses Gesetzes auf den Auftragsverarbeiter keine Anwendung finden, ist vertraglich sicherzustellen, dass er sich der Kontrolle der oder des Landesbeauftragten für Datenschutz unterwirft und die Vorschriften dieses Gesetzes befolgt. [2]Die Auftragsgeberin hat die oder den Landesbeauftragten für Datenschutz über die Beauftragung zu unterrichten. [3]Der Gerichtsstand muss in der Bundesrepublik Deutschland belegen sein. [4]Die Beauftragung eines in einem Drittstaat im Sinne des § 49 Absatz 1 Satz 1 ansässigen Auftragsverarbeiters ist nicht zulässig.

## 3. Abschnitt
## Sicherheit und Schutz personenbezogener Daten

### § 58 Anforderungen an die Sicherheit der Verarbeitung personenbezogener Daten

(1) [1]Sowohl die Polizei selbst als auch ein Auftragsverarbeiter haben unter Berücksichtigung des Standes der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten der betroffenen Person die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. [2]Die Polizei hat hierbei die einschlägigen technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.
(2) [1]Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. [2]Die Maßnahmen nach Absatz 1 sollen dazu führen, dass

1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und
2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

(3) [1]Im Fall einer automatisierten Verarbeitung haben die Polizei und gegebenenfalls der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

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

11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),
12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).

[2]Die in Satz 1 Nummer 2 bis 5 genannten Ziele können insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

### § 59 Anhörung der oder des Landesbeauftragten für Datenschutz

(1) [1]Vor dem erstmaligen Einsatz neuer Dateisysteme oder neuer Verfahren oder der wesentlichen Änderung bestehender Verfahren ist die oder der Landesbeauftragte für Datenschutz anzuhören, wenn

1. aus einer Datenschutz-Folgenabschätzung nach § 55 hervorgeht, dass die Verarbeitung eine ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person zur Folge hätte, wenn der Verantwortliche keine Abhilfemaßnahmen treffen würde, oder
2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, eine erhebliche Gefahr für die Rechtsgüter der betroffenen Person zur Folge hat.

[2]Die oder der Landesbeauftragte für Datenschutz kann eine Liste der Verarbeitungsvorgänge erstellen, die der Pflicht zur Anhörung nach Satz 1 unterliegen. [3]Im Bereich der Landesverwaltung ist die jeweils zuständige oberste Landesbehörde über die Einleitung und den Abschluss des Verfahrens nach Satz 1 zu informieren.

(2) [1]Der oder dem Landesbeauftragten für Datenschutz sind im Fall des Absatzes 1 vorzulegen:

1. die nach § 55 durchgeführte Datenschutz-Folgenabschätzung,
2. gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten aller beteiligten Polizeibehörden und der an der Verarbeitung beteiligten Auftragsverarbeiter,
3. Angaben zu den Zwecken und Mitteln der beabsichtigten Verarbeitung,
4. Angaben zu den zum Schutz der Rechtsgüter der betroffenen Person vorgesehenen Maßnahmen und Garantien und
5. Name und Kontaktdaten der oder des Datenschutzbeauftragten.

[2]Auf Anforderung sind der oder dem Landesbeauftragten für Datenschutz zudem alle sonstigen Informationen zu übermitteln, die sie oder er benötigt, um die Rechtmäßigkeit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Person bestehenden Gefahren und die diesbezüglichen Garantien bewerten zu können.

(3) [1]Falls die oder der Landesbeauftragte für Datenschutz der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstoßen würde, insbesondere, weil das Risiko nicht ausreichend ermittelt oder keine ausreichenden Abhilfemaßnahmen getroffen wurden, kann sie oder er innerhalb eines Zeitraums von sechs Wochen nach Einleitung der Anhörung schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergriffen werden sollten. [2]Die oder der Landesbeauftragte für Datenschutz kann diese Frist um einen Monat verlängern, wenn die geplante Verarbeitung besonders komplex ist. [3]Sie oder er hat in diesem Fall innerhalb eines Monats nach Einleitung der Anhörung den Verantwortlichen und gegebenenfalls den Auftragsverarbeiter über die Fristverlängerung zu informieren.

(4) [1]Hat die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung der Polizei und ist sie daher besonders dringlich, kann mit der Verarbeitung nach Beginn der Anhörung, aber vor Ablauf der in Absatz 3 Satz 1 genannten Frist begonnen werden. [2]In diesem Fall sind die Empfehlungen der oder des Landesbeauftragten für Datenschutz im Nachhinein zu berücksichtigen und sind die Art und Weise der Verarbeitung daraufhin gegebenenfalls anzupassen.

### § 60 Freigabe

(1) Jede mittels automatisierter Verfahren vorgesehene Verarbeitung personenbezogener Daten bedarf vor ihrem Beginn oder vor einer wesentlichen Änderung der schriftlichen Freigabe. In der Freigabeerklärung ist zu bestätigen, dass

1. die Verarbeitung im Einklang mit den § 3 erfolgt,
2. ein aus einer Risikoanalyse und unter Berücksichtigung der Vorgaben des § 58 entwickeltes Sicherheitskonzept ergeben hat, dass geeignete technische und organisatorische Maßnahmen getroffen sind, um ein dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessenes Schutzniveau zu gewährleisten,
3. für die Verfahren, von denen voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen ausgeht, eine Datenschutz-Folgenabschätzung gemäß § 55 erfolgt ist und
4. im Falle des § 55 Absatz 1 die Stellungnahme der oder des Landesbeauftragten für Datenschutz nach § 59 Absatz 3 Satz 1 erfolgt ist.

Die Freigabe erfolgt durch den Verantwortlichen. Bei gemeinsamen Verfahren kann die Zuständigkeit für die Freigabe entsprechend § 54 Satz 2 vereinbart werden. Die Freigabeerklärung ist dem Verzeichnis nach § 61 beizufügen.

(2) Eine Freigabe ist nicht erforderlich für

1. Verfahren, deren einziger Zweck das Führen eines Registers ist, das zur Information der Öffentlichkeit bestimmt ist oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht,
2. Verfahren, soweit mit ihnen Datensammlungen erstellt werden, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden,
3. den Einsatz standardisierter Büro-Software,
4. Verfahren, die ausschließlich der Datensicherung und Datenschutzkontrolle dienen,
5. Verfahren, die ausschließlich dem Auffinden von Vorgängen, Anträgen oder Akten dienen (Registraturverfahren),
6. Verfahren, die ausschließlich zur Überwachung von Terminen und Fristen dienen,
7. Zimmer-, Inventar- und Softwareverzeichnisse,
8. Bibliothekskataloge und Fundstellenverzeichnisse oder
9. Anschriftenverzeichnisse, die ausschließlich für die Versendung von Informationen an betroffene Personen genutzt werden.

### § 61 Verzeichnis von Verarbeitungstätigkeiten

(1) [1]Jeder Verantwortliche hat ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die in ihre Zuständigkeit fallen. [2]Dieses Verzeichnis hat die folgenden Angaben zu enthalten:

1. den Namen und die Kontaktdaten beteiligten Polizeibehörden sowie den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten,
2. die Zwecke der Verarbeitung,
3. die Kategorien von Empfängerinnen und Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen,

4. eine Beschreibung der Kategorien der betroffenen Person und der Kategorien personenbezogener Daten,
5. gegebenenfalls die Verwendung von Profiling,
6. gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,
7. Angaben über die Rechtsgrundlage der Verarbeitung,
8. die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten und
9. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach § 58.

(2) [1]Der Auftragsverarbeiter hat ein Verzeichnis aller Kategorien von Verarbeitungen zu führen, die er im Auftrag eines Verantwortlichen durchführt. [2]Dieses Verzeichnis hat die folgenden Angaben zu enthalten:

1. den Namen und die Kontaktdaten des Auftragsverarbeiters, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls der oder des Datenschutzbeauftragten,
2. gegebenenfalls Übermittlungen von personenbezogenen Daten an Stellen in einem Drittstaat oder an eine internationale Organisation unter Angabe des Staates oder der Organisation und
3. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 58.

(3) Die in den Absätzen 1 und 2 genannten Verzeichnisse sind schriftlich oder elektronisch zu führen. [2]Sie sind der oder dem Landesbeauftragten für Datenschutz auf Anfrage zur Verfügung zu stellen. [3]Soweit die Verzeichnisse elektronisch geführt werden, kann der oder dem Landesbeauftragten für Datenschutz ein lesender Zugriff eingeräumt werden.

(4) [1]Das Verzeichnis nach Absatz 1 einschließlich der Freigabeerklärung nach § 60 kann von jedermann unentgeltlich eingesehen werden. Das Recht auf Einsicht entfällt für Angaben nach Absatz 1 Nummer 9 und Absatz 2 Nummer 3, soweit hierdurch die Sicherheit des Verfahrens beeinträchtigt würde. [2]Satz 1 gilt nicht, soweit die jeweilige Polizeibehörde eine Einsichtnahme im Einzelfall mit der Erfüllung ihrer Aufgaben für unvereinbar erklärt.

### § 62 Meldung von Verletzungen des Schutzes personenbezogener Daten an die oder den Landesbeauftragten für Datenschutz

(1) [1]Die jeweilige Polizeibehörde hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb von 72 Stunden, nachdem sie ihr bekannt geworden ist, der oder dem Landesbeauftragten für Datenschutz zu melden, es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen wird. [2]Erfolgt die Meldung an die Landesbeauftragte oder den Landesbeauftragten für Datenschutz nicht innerhalb von 72 Stunden, so ist die Verzögerung zu begründen.

(2) Ein Auftragsverarbeiter hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich der jeweiligen Polizeibehörde zu melden.

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

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, die, soweit möglich, Angaben zu den Kategorien und der ungefähren Anzahl der betroffenen Personen, zu den betroffenen Kategorien personenbezogener Daten und zu der ungefähren Anzahl der betroffenen personenbezogenen Datensätze zu enthalten hat,
2. den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten oder einer sonstigen Person oder Stelle, die weitere Informationen erteilen kann,
3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung und

4. eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung und der getroffenen Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn die Informationen nach Absatz 3 nicht zusammen mit der Meldung übermittelt werden können, sind diese unverzüglich nachzureichen, sobald sie vorliegen.
(5) [1]Die Polizei hat Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. [2]Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen.
(6) Soweit von einer Verletzung des Schutzes personenbezogener Daten personenbezogene Daten betroffen sind, die von einer öffentlichen Stelle in einem anderen Mitgliedstaat der Europäischen Union übermittelt wurden, sind die in Absatz 3 genannten Informationen dem dortigen Verantwortlichen unverzüglich zu übermitteln.

### § 63 Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten

(1) Hat eine Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die Rechte und Freiheiten betroffener Personen zur Folge, sind diese unverzüglich über den Vorfall zu benachrichtigen.
(2) Die Benachrichtigung nach Absatz 1 hat in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und zumindest die in § 62 Absatz 3 Nummer 2 bis 4 genannten Informationen und Maßnahmen zu enthalten.
(3) Von der Benachrichtigung nach Absatz 1 kann abgesehen werden, wenn

1. geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen sind und diese Vorkehrungen auf die von der Verletzung des Schutzes personenbezogener Daten betroffenen Daten angewandt wurden; dies gilt insbesondere für Vorkehrungen wie Verschlüsselungen, durch die die Daten für unbefugte Personen unzugänglich gemacht wurden;
2. durch im Anschluss an die Verletzung getroffene Maßnahmen sichergestellt ist, dass aller Wahrscheinlichkeit nach kein hohes Risiko im Sinne des Absatzes 1 mehr besteht, oder
3. dies mit einem unverhältnismäßigen Aufwand verbunden wäre; in diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) [1]Soweit die betroffenen Personen über eine Verletzung des Schutzes personenbezogener Daten nicht benachrichtigt wurden, kann die oder der Landesbeauftragte für Datenschutz förmlich feststellen, dass ihrer oder seiner Auffassung nach die in Absatz 3 genannten Voraussetzungen nicht erfüllt sind. [2]Hierbei hat sie oder er die Wahrscheinlichkeit zu berücksichtigen, dass die Verletzung eine erhebliche Gefahr im Sinne des Absatzes 1 zur Folge hat.
(5) Die Benachrichtigung der betroffenen Personen nach Absatz 1 kann unter den in § 10 Absatz 2, 5 oder 6 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden, soweit nicht die Interessen der betroffenen Person aufgrund der von der Verletzung ausgehenden erheblichen Gefahr im Sinne des Absatzes 1 überwiegen.

### § 64 Vertrauliche Meldung von Verstößen

Die Leiterin oder der Leiter einer Polizeibehörde hat es zu ermöglichen, dass ihr oder ihm vertrauliche Meldungen über in ihrem oder seinem Verantwortungsbereich erfolgte oder erfolgende Verstöße gegen Vorschriften zum Schutz personenbezogener Daten zugeleitet werden können.

## Sechster Teil
## Schlussvorschriften

### § 65 Ordnungswidrigkeiten und Straftaten

(1) [1]Ordnungswidrig handelt, wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, verwendet, verändert, übermittelt, zum Abruf bereithält, den Personenbezug herstellt, löscht oder nutzt,
2. abruft, sich oder einem anderen verschafft oder durch unrichtige oder unvollständige Angaben ihre Übermittlung an sich oder andere veranlasst.

[2]§ 27 Absatz 2, 3 des Saarländischen Datenschutzgesetzes gilt entsprechend.

(2) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.

(3) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(4) [1]Die Tat wird nur auf Antrag verfolgt. [2]Antragsberechtigt sind

1. die betroffene Person,
2. die jeweilige Behördenleitung,
3. die oder der Landesbeauftragte für Datenschutz,
4. das Ministerium für Inneres, Bauen und Sport als oberste Dienstbehörde nach § 82 Absatz 4 Satz 1 des Saarländischen Polizeigesetzes und als Dienst- und Fachaufsichtsbehörde über die Vollzugspolizei nach § 83 des Saarländischen Polizeigesetzes und
5. die jeweils zuständigen Ministerien als Fachaufsicht über die nachgeordneten Polizeiverwaltungsbehörden nach § 77 des Saarländischen Polizeigesetzes.

(5) Eine Meldung nach § 62 oder eine Benachrichtigung nach § 63 darf in einem Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

### § 66 Berichtspflichten der Landesregierung

[1]Die Landesregierung berichtet dem Landtag des Saarlandes jährlich über

1. durchgeführte längerfristige Observationen nach § 31 Absatz 2 Nummer 1 in Verbindung mit § 31 Absatz 3 Satz 1 Nummer 1,
2. den verdeckten Einsatz technischer Mittel nach § 31 Absatz 2 Nummer 2 in Verbindung mit § 31 Absatz 3 Satz 1 Nummer 2,
3. den Einsatz von Vertrauenspersonen, Informantinnen und Informanten nach § 31 Absatz 2 Nummer 3 in Verbindung mit § 31 Absatz 3 Satz 1 Nummer 3,
4. den Einsatz verdeckter Ermittlerinnen oder Ermittler nach § 31 Absatz 2 Nummer 4 in Verbindung mit § 31 Absatz 3 Satz 1 Nummer 3,
5. den Einsatz von sonstigen, besonders für Observationszwecke bestimmten technischen Mittel im Rahmen einer längerfristigen Observation nach § 31 Absatz 2 Nummer 5 in Verbindung mit § 31 Absatz 3 Satz 1 Nummer 1,
6. die Erhebung personenbezogener Daten in oder aus Wohnungen nach § 34 Absatz 1 und 3,

7. Maßnahmen zur Überwachung und Aufzeichnung der Telekommunikation nach § 35 Absatz 1 und 2,
8. Maßnahmen zur Lokalisierung und Identifizierung von Telekommunikationsendgeräten nach § 35 Absatz 3,
9. Maßnahmen zur Erhebung von Verkehrsdaten, von bestimmten Zeitpunkten zugewiesenen Internetprotokoll-Adressen und Nutzungsdaten von Telemedien nach § 36 Absatz 1, 3 Satz 2 und 3 und Absatz 4,
10. die Unterbrechung von Telekommunikationsverbindungen nach § 37,
11. Maßnahmen zur elektronischen Aufenthaltsüberwachung nach § 38,
12. Maßnahmen zur anlassbezogenen automatischen Kennzeichenfahndung nach § 39,
13. Ausschreibungen zur polizeilichen Beobachtung nach § 40 sowie
14. Übermittlungen an Drittstaaten und internationale Organisationen nach den §§ 49 bis 52

erstmals bis zum 1. Januar 2021. [2]Der Landtag des Saarlandes macht die Unterrichtung öffentlich zugänglich.

### § 67 Inkrafttreten

Dieses Gesetz tritt am [**einsetzen: Datum des Inkrafttretens**] in Kraft.

## Artikel 3
## Aufhebung der Verordnung über die Zulassung der Übermittlung personenbezogener Daten von der Polizei an ausländische Polizeibehörden

Die Verordnung über die Zulassung der Übermittlung personenbezogener Daten von der Polizei an ausländische Polizeibehörden vom 4. Dezember 1996 (Amtsbl. 1997 S. 30), zuletzt geändert durch das Gesetz vom 12. November 2014 (Amtsbl. I S. 1465), wird aufgehoben.

## Artikel 4
## Einschränkung von Grundrechten

Durch dieses Gesetz werden das allgemeine Persönlichkeitsrecht (Artikel 2 Absatz 1 des Grundgesetzes in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes), das Grundrecht auf informationelle Selbstbestimmung (Artikel 2 Absatz 1 des Grundgesetzes in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes), die Freiheit der Person (Artikel 2 Absatz 2 in Verbindung mit Artikel 104 des Grundgesetzes), das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes), das Grundrecht auf Freizügigkeit (Artikel 11 des Grundgesetzes) und die Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) eingeschränkt.

## Artikel 5
## Übergangsvorschriften

(1) Abweichend von Artikel 2 § 22 Absatz 2 ist die Verarbeitung personenbezogener Daten nur zulässig

1. nach den Bestimmungen der vor Inkrafttreten dieses Gesetzes jeweils geltenden Errichtungsanordnungen nach § 39 Absatz 2 des Saarländischen Polizeigesetzes in der Fassung der Bekanntmachung vom 26. März 2001 (Amtsbl. S. 1074), zuletzt geändert durch Gesetz vom 22. August 2018 (Amtsbl. I S. 674, 681),
2. soweit die Kennzeichnung
   a) tatsächlich oder technisch unmöglich ist oder
   b) einen unverhältnismäßigen Aufwand erfordern würde.

(2) [1]Für Dateisysteme, die vor dem 16. Mai 2016 eingerichtet wurden, kann die Umsetzung des Artikels 2 § 27 Absatz 1 bis 3 und § 43 Absatz 4 Satz 4 bis zum 6. Mai 2023 aufgeschoben werden, wenn die Verarbeitung der Protokolldaten mit einem unverhältnismäßigen Aufwand verbunden wäre. [2]Das Ministerium für Inneres, Bauen und Sport ist hierüber zu informieren. [3]Die oder der Landesbeauftragte für Datenschutz ist zu beteiligen; Artikel 2 § 59 Absatz 3 gilt entsprechend.

(3) Absatz 1 Nummer 2 tritt am 31. Dezember 2025 außer Kraft.

## Artikel 6
## Inkrafttreten

Dieses Gesetz tritt **2020** in Kraft.

**B e g r ü n d u n g :**

## A. Allgemeines

Mit dem Gesetz zur Neuregelung der polizeilichen Datenverarbeitung im Saarland werden mehrere Ziele verfolgt. Zunächst dient die Norm der Umsetzung der 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 (im Folgenden „Richtlinie“.) Somit wird der Schutz personenbezogener Daten bei der polizeilichen Datenverarbeitung durch die Schaffung europaweit materiell gleicher, hoher, Standards gestärkt.
Weiter fließen die Vorgaben des Bundesverfassungsgerichtsurteils vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, zum Bundeskriminalamtgesetz – insbesondere zu eingriffsintensiven verdeckten Maßnahmen - in der mit Normenkontrollklage angegriffenen Fassung ein.
Ein weiterer Schwerpunkt ist die angemessene gesetzgeberische Reaktion auf den insbesondere islamistischen Terrorismus. Hierzu bedarf es auch neuer Instrumente in Bezug auf die Verarbeitung personenbezogener Daten, so etwa

- die elektronische Aufenthaltsüberwachung („Fußfessel“),
- erweiterte Befugnisse zur Videoüberwachung öffentlich zugänglicher Orte,
- die Wiedereinführung der Befugnis, automatische Kennzeichenlesesysteme einzusetzen,
- Einführung der sog. Quellen-TKÜ,
- Datenabfragen nach dem Telemediengesetz und
- Einsatz von sog. Jammern zur situativen temporären Unterbrechung der mobilen Telekommunikation.

Diese eingriffsintensiven Maßnahmen korrelieren mit der ausschließlichen Befugnis der Vollzugspolizei zu ihrem Einsatz; sie stehen regelmäßig unter Richtervorbehalt und sind nur zulässig zur Abwehr von Gefahren für hochwertige Schutzgüter oder zur vorbeugenden Bekämpfung schwerer Straftaten.
Darüber hinaus wird die rechtliche Grundlage zur Einrichtung einer sog. Referenzdatenbank geschaffen. Dadurch sollen sog. DNA-Trugspuren, die im Rahmen der Tatortarbeit und der sich anschließenden Asservierung, Verwendung bzw. Versand der betreffenden Spurenträger entstehen können, frühzeitig erkannt und aussortiert werden.
Primär dem Schutz der eingesetzten Beamtinnen und Beamten dient das neu definierte Einsatzspektrum der Body-Cams. Dieses relativ neue und dennoch bereits bewährte und erfolgreiche Einsatzmittel soll auch in Wohnungen, überwiegend bei Einsätzen im Zusammenhang mit häuslicher Gewalt, eingesetzt werden dürfen. Das Ministerium für Inneres, Bauen und Sport hat hierzu ein eigenes Rechtsgutachten bei den renommierten Polizeirechtlern Prof. Dr. Dr. Markus Thiel und Dr. Knud Dietrich, beide von der Deutschen Hochschule der Polizei in Auftrag gegeben. Dessen Ergebnis ist in den Regelungsvorschlag eingeflossen.
Durch die Umsetzung der Richtlinie wird der Informationsfluss zwischen Polizeibehörden sowohl national als auch mit denen der EU-Partnerstaaten harmonisiert.
Die Umsetzung dieses gesetzgeberischen Regelungswillens erfolgt in Form eines Artikelgesetzes, dessen wesentlicher Schwerpunkt das künftige Saarländische Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG) ist. In diesem Gesetzeswerk werden alle gefahrenabwehrbezogenen Regelungen zur polizeilichen Verarbeitung personenbezogener Daten zusammengefasst.

Dazu werden durch Artikel 1 die §§ 26 bis 40 des Saarländischen Polizeigesetzes (SPolG) aufgehoben; diese werden – zum Teil modifiziert – in das SPolDVG übertragen. § 25 SPolG enthält künftig einen Verweis auf die Anwendung des SPolDVG. Unberührt hiervon bleiben die Datenerhebungsbefugnisse, die weiterhin im Regelungswerk des SPolG vorhanden sind, beispielsweise in § 9 die Befugnis zur Identitätsfeststellung.
Die Verordnung über die Zulassung der Übermittlung personenbezogener Daten von der Polizei an ausländische Polizeibehörden (InfÜVPol) vom 4. Dezember 1996 wird aufgehoben, da jegliche Übermittlung personenbezogener Daten durch Polizeibehörden künftig im SPolDVG geregelt wird.
Inhaltlich orientiert sich die Neuregelung hinsichtlich der polizeilichen Befugnisse weitgehend an den bisherigen Regelungen des SPolG, orientiert an den Vorgaben des Bundesverfassungsgerichts; insoweit greift das SPolDVG ergänzend die Korrespondenzregelungen des ab 25. Mai 2018 in Kraft getretenen Bundeskriminalamtgesetzes (BKAG 2018) auf.

Die Regelungen, welche
- die allgemeinen Rechtsgrundlagen der Verarbeitung personenbezogener Daten,
- die Rechte der betroffenen Personen,
- die Übermittlung an Drittstaaten sowie
- die Sicherheit und die Datenverarbeitung im Auftrag

betreffen, sind überwiegend sowohl an die bisherigen Regelungen im SPolG als auch an das ebenfalls am 25. Mai 2018 in Kraft tretende neue Bundesdatenschutzgesetz (BDSG 2018) angelehnt. Insbesondere die Übernahme von Bundesrecht leistet einen Beitrag zu einer bundesweit möglichst einheitlichen Rechtsanwendung.

## B. Im Einzelnen

### Zu Artikel 1 – Änderung des Saarländischen Polizeigesetzes

Zu 1., Änderung der Inhaltsübersicht:

a) Es handelt sich um eine redaktionelle Anpassung aufgrund der Änderung des § 12.

b) Hier liegt ebenfalls eine redaktionelle Änderung vor. Durch die Neuregelung der gesamten polizeilichen Datenverarbeitung werden die Paragrafen 26 bis 40 überflüssig und sind daher aufzuheben. Dies gilt auch für die jeweiligen Angaben in der Inhaltsübersicht des SPolG.

Zu 2., Änderung des § 7:

Es handelt sich hier um eine Folgeänderung aus Artikel 2 § 35 und § 36, da die polizeiliche Telekommunikationsüberwachung und verwandte Maßnahmen, die in Artikel 10 Grundgesetz eingreifen, künftig im Saarländischen Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei geregelt sein werden.

Zu 3., Änderung des § 8:

Es handelt sich hier um eine Folgeänderung aus Nummer 7 und 8, Änderung des § 25 bzw. Streichung der §§ 26 – 40.

Zu 4., Änderung des § 9a:

Es handelt sich hier um eine Folgeänderung, da die Befugnis zur Speicherung, Veränderung und Nutzung personenbezogener Daten künftig im Saarländischen Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei geregelt sein wird.

Zu 5., Änderung des § 11:

Die Vollzugspolizei erhält in § 38 des Saarländischen Gesetzes über die Verarbeitung personenbezogener Daten durch die Polizei (s. Artikel 2) die Befugnis zur Anordnung bzw. Durchführung einer elektronischen Aufenthaltsüberwachung. Insbesondere zur technischen Durchführung dieser Maßnahme kann es erforderlich werden, die betroffene Person zur Polizeidienststelle vorzuladen sowie ggf. bei Nichtbefolgen der Vorladung diese zwangsweise durchzusetzen. Aus diesem Grund werden die bisherigen Vorladungszwecke in den Absätzen 2 und 4 entsprechend ergänzt. Da die Vorladung zu einer solchen Maßnahme voraussetzt, dass die tatbestandlichen Voraussetzungen des § 38 des Saarländischen Gesetzes über die Verarbeitung personenbezogener Daten durch die Polizei vorliegen bzw. eine entsprechende Anordnung erfolgt ist, kann eine solche Vorladung – analog der Vorladung zur Erkennungsdienstlichen Behandlung – auch nur durch die Vollzugspolizei erfolgen. Liegen die Voraussetzungen des § 19 Absatz 1 Nummer 1 SPolG vor, kann zur zwangsweisen Durchsetzung der Vorladung die Wohnung des Vorgeladenen betreten und durchsucht werden.

Zu 6., Änderung des § 12:

Im Zusammenhang mit der Einführung der elektronischen Aufenthaltsüberwachung in § 38 des Saarländischen Gesetzes über die Verarbeitung personenbezogener Daten durch die Polizei (s. Artikel 2) wird auch die Möglichkeit von deren Anordnung zur Überwachung eines Aufenthaltsgebots beziehungsweise eines Kontaktverbots geregelt, siehe § 38 Absatz 2. Dementsprechend ist auch § 12 SPolG anzupassen, da dort aktuell lediglich Platzverweisung, Wohnungsverweisung und Aufenthaltsverbot geregelt sind.
Da insbesondere das sog. Aufenthaltsgebot wesentlich stärker in die Grundrechte der Betroffenen eingreift, wird sowohl diese Maßnahme als auch das Kontaktverbot analog zu anderen Länderregelungen und auch der Regelung in § 55 Absatz 3 BKAG 2018 grundsätzlich unter Richtervorbehalt gestellt. Auch bleiben die Maßnahmen der Vollzugspolizei vorbehalten. Eine Ausnahme hiervon stellt die Anordnung eines Kontaktverbots im Rahmen einer Wohnungsverweisung nach § 12 Absatz 2 SPolG dar. Um hier einen Gleichklang zwischen dem Rückkehrverbot zur Wohnung des Opfers und dem Kontaktverbot zum Opfer außerhalb der Wohnung zu erreichen – beide Maßnahmen werden oftmals gleichzeitig angeordnet -, wird die Anordnungskompetenz analog den Regelungen des § 12 Absatz 2 SPolG auf Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte übertragen. Die Fristen richten sich ebenfalls nach den Vorgaben des § 12 Absatz 2 SPolG. Da es sich bei der Wohnungsverweisung nach § 12 Absatz 2 SPolG lediglich um eine vorläufige Maßnahme handelt, bis eine entsprechende richterliche Entscheidung nach dem Gewaltschutzgesetz getroffen wurde (Frist maximal 20 Tage, vgl. § 12 Absatz 2 Satz 4 und 5 SPolG), ist in solchen Fällen ein Abweichen von dem generellen Richtervorbehalt rechtlich zu vertreten.
Das bislang der Anordnungsbefugnis der von Verwaltungs- und Vollzugspolizei unterfallende Aufenthaltsverbot mit seinen vergleichsweise geringen örtlichen Beschränkungen, Absatz 3, bleibt unverändert.

Zu 7., Änderung des § 25:

§ 25 enthält nunmehr einen deklaratorischen Hinweis auf den neuen Regelungsstandort der polizeilichen Verarbeitung personenbezogener Daten.

Zu 8., Aufhebung der §§ 26 bis 40:

Es handelt sich um eine Folgeänderung aus Artikel 2.

**Zu Artikel 2 – Saarländisches Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG)**

## Erster Teil
## Allgemeine Bestimmungen

### 1. Abschnitt
### Anwendungsbereich, Begriffsbestimmungen und Allgemeine Grundsätze

Zu § 1, Anwendungsbereich:

Absatz 1 übernimmt zunächst den Begriff der Polizei aus der Legaldefinition in § 1 Absatz 1 SPolG (Polizeiverwaltungsbehörden und Vollzugspolizei).
Der sachliche Anwendungsbereich ist in Absatz 1 auf die „Verhütung, Aufdeckung, Ermittlung, Verfolgung und Ahndung von Straftaten und Ordnungswidrigkeiten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung“ beschränkt, wobei die Ahndungskompetenz auf Ordnungswidrigkeiten beschränkt ist.

Der im Vergleich zur bisherigen Rechtslage engere Anwendungsbereich ergibt sich im Besonderen aus den Vorgaben der Richtlinie. Dort findet sich in Erwägungsgrund (ErwG) 12 folgender Rahmen:

> „Die Tätigkeiten der Polizei oder anderer Strafverfolgungsbehörden sind hauptsächlich auf die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten ausgerichtet, dazu zählen auch polizeiliche Tätigkeiten in Fällen, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht. Solche Tätigkeiten können ferner die Ausübung hoheitlicher Gewalt durch Ergreifung von Zwangsmitteln umfassen, wie polizeiliche Tätigkeiten bei Demonstrationen, großen Sportveranstaltungen und Ausschreitungen. Sie umfassen auch die Aufrechterhaltung der öffentlichen Ordnung als Aufgabe, die der Polizei oder anderen Strafverfolgungsbehörden übertragen wurde, soweit dies zum Zweck des Schutzes vor und der Abwehr von Bedrohungen der öffentlichen Sicherheit und Bedrohungen für durch Rechtsvorschriften geschützte grundlegende Interessen der Gesellschaft, die zu einer Straftat führen können, erforderlich ist.“

Die Umsetzung dieser Vorgaben im SPolDVG beschränkt sich aufgrund der Gesetzgebungskompetenz des Bundes im Bereich des Strafrechts und des gerichtlichen Verfahrens (vgl. Artikel 74 Absatz 1 Nummer 1 des Grundgesetzes) lediglich auf den Bereich der Prävention bzw. der Gefahrenabwehr. Der Begriff der „Gefahrenabwehr“ im Sinne der Richtlinie umfasst dabei die straftatenbezogene Gefahrenabwehr unter Einbeziehung der Ordnungswidrigkeiten. Auch polizeiliche Tätigkeiten im Bereich der Gefahrenvorsorge und der vorbeugenden Bekämpfung von Straftaten sind von der Richtlinie und somit vom Anwendungsbereich des SPolDVG umfasst.

Der Begriff der straftatenbezogenen Gefahrenabwehr ist dabei weit auszulegen. Hierunter fallen auch alle Sachverhalte, bei denen nicht auszuschließen ist, dass sie zu einer Straftat (oder einer Ordnungswidrigkeit) führen können. Die Anforderungen an der Grad der Wahrscheinlichkeit sind gering. Auch Sachverhalte, bei denen nicht klar ist, ob eine Straftat (oder Ordnungswidrigkeit) im Raum steht, sind unter den Anwendungsbereich der Richtlinie zu subsumieren und fallen damit unter den Anwendungsbereich des SPolDVG.
So werden vom Geltungsbereich der Richtlinie (und somit vom Anwendungsbereich des SPolDVG) beispielhaft folgende Fallgruppen umfasst:

- Vermisstendatei, siehe ErwG 12 Satz 1 Halbsatz 2,
- unklarer Todesfall, siehe ErwG 12 Satz 1 Halbsatz 2,
- Standorterfassungen, siehe ErwG 12 Satz 1Halbsatz 2,
- doppelfunktionale Maßnahmen, siehe ErwG 1 Satz 1 Halbsatz 2,
- Verkehrsregister ErwG 12 Satz 1 und ErwG 13,
- Zuverlässigkeitsüberprüfungen, siehe ErwG 12 Satz 3.

Lediglich in einigen wenigen Fällen kommt das SPolDVG bei der polizeilichen Verarbeitung personenbezogener Daten nicht zur Anwendung. Das kann bei Sachverhalten der Fall sein, bei denen jedweder Bezug zu einer Straftat oder Ordnungswidrigkeit von vornherein ausgeschlossen ist. Auch die Verarbeitung personenbezogener Daten zum Schutz privater Rechte (vgl. §§ 1 Absatz 3 SPolG) fällt nicht in den Anwendungsbereich des SPolDVG. In solchen Fällen greift der Absatz 3.
Absatz 2 regelt bzw. verdeutlicht das Verhältnis zwischen dem SPolDVG und dem SPolG sowie spezialgesetzlicher Normen, in denen Befugnisse zur Verarbeitung personenbezogener Daten vorhanden sind. Im SPolG verbleiben nach Inkrafttreten des SPolDVG weiterhin mehrere Datenerhebungsnormen. Durch die abschließende Auflistung dieser Befugnisse in Absatz 2 wird deutlich, dass diese Erhebungsnormen den einschlägigen Erhebungsnormen des SPolDVG – insbesondere in § 18 - vorgehen. Gleiches gilt, wenn in spezialgesetzlichen Regelungen auf Landesebene Befugnisse zur Datenverarbeitung vorhanden sind. Bundesgesetzliche Regelungen gehen gemäß Artikel 31 Grundgesetz stets landesgesetzlichen Regelungen vor.
Absatz 3 stellt eine Auffangvorschrift dar, nach der für jede nicht spezialgesetzlich geregelte Verarbeitung personenbezogener Daten durch die Polizei die „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung- DSGVO) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72)“ beziehungsweise das zu deren Umsetzung zu erlassende Saarländische Datenschutzgesetz (SDSG) anzuwenden ist.
Die §§ 80, 85 des Saarländischen Polizeigesetzes, in welchen die grundsätzlichen Aufgabenzuweisungen an Verwaltungs- beziehungsweise Vollzugspolizei normiert sind, bleiben unberührt.

Zu § 2, Begriffsbestimmungen:

§ 2 enthält Begriffsbestimmungen und gibt den Regelungsgehalt des § 46 BDSG 2018 wieder, der wiederum nahezu wörtlich Artikel 3 der Richtlinie umsetzt. Ergänzend dazu wird in Absatz 6 die Anonymisierung definiert, indem § 3 Absatz 8 Satz 1 des Saarländischen Datenschutzgesetzes vom 24. März 1993 in der Fassung der Bekanntmachung vom 28. Januar 2008 (Amtsbl. I S. 293), zuletzt geändert durch das Gesetz vom 13. Oktober 2015 (Amtsbl. I S. 790) [im Folgenden: SDSG (alt)], unverändert übernommen wird.
Absatz 19 definiert diejenigen personenbezogenen Daten (Grunddaten einer Person), welche unter weniger strengen Vorgaben nach § 23 Absatz 2 Satz 2 zur Identifizierung verarbeitet werden können.

Der Umfang der Grunddaten ist bewusst nicht abschließend geregelt, um sicher zu stellen, dass die Übernahme weitere Datenkategorien durch die Rechtslage gedeckt ist. Dies wird in der Praxis insbesondere die in der BKA-Daten-Verordnung aufgeführten personenbezogenen Daten betreffen.

Zu § 3, Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten:

§ 3 Absatz 1, 3 entspricht dem bisherigen § 25 Absatz 1, 2 SPolG.
Absatz 2 setzt Artikel 4 der Richtlinie unter Aufgreifen der Formulierung des § 47 BDSG 2018 um und führt einige allgemeine Verarbeitungsgrundsätze an zentraler Stelle zusammen.
Absatz 4 entspricht § 25 Absatz 3 SPolG (alt), ergänzt um den Hinweis, dass eine verdeckte Erhebung auch auf Grundlage eines Gesetzes erfolgen kann.
Absatz 5 wiederum entspringt dem bisherigen § 25 Absatz 5 SPolG, ergänzt allerdings um die bislang verwiesenen Regelungen des § 11 Absatz 1 Satz 3 bis 6.
Der bisherige § 25 Absatz 4 SPolG, Einwilligung, wurde in § 10 eingearbeitet.

## 2. Abschnitt
## Datenschutzkontrolle

Zu § 4, Aufsichtsbehörde:

Die Vorschrift definiert die oder den Landesbeauftragten für Datenschutz als die nach Artikel 41 der Richtlinie einzurichtende Aufsichtsbehörde.

Zu § 5, Aufgaben der Aufsichtsbehörde:

§ 5 definiert in Umsetzung des Artikels 46 der Richtlinie die Aufgaben der Aufsichtsbehörde nach § 4.
Absatz 1 orientiert sich am Wortlaut des § 14 Absatz 1 BDSG.
Absatz 2 dient der Sicherstellung des Schutzes personenbezogener Daten, die durch verdeckte oder besonders eingriffsintensive Maßnahmen erhoben wurden. Die hierzu in § 42 Absatz 1, 2 vorgeschriebene Protokollierung wird künftig regelmäßig durch die Aufsichtsbehörde kontrolliert.
Absatz 3 setzt in Anlehnung an § 15 BDSG 2018 Artikel 49 der Richtlinie um.

Zu § 6, Befugnisse der Aufsichtsbehörde:

Die Vorschrift setzt Artikel 47 der Richtlinie um. Der Wortlaut ist orientiert an § 16 BDSG 2018. Der Maßnahmenkatalog hingegen stützt sich direkt auf die Empfehlungen des Artikels 47, ergänzt um Handlungshinweise zum Beanstandungsverfahren. Das Beanstandungsverfahren selbst ist im Landesrecht seit dem ersten Saarländischen Datenschutzgesetz vom 17.Mai 1978, Amtsbl. S. S. 581, normiert und regelte bis zum Inkrafttreten des novellierten Saarländischen Datenschutzgesetzes am 25. Mai 2018 subsidiär auch die polizeiliche Verarbeitung personenbezogener Daten. Da dieses Gesetz jedoch der Umsetzung der Datenschutzgrundverordnung dient und daher auf die polizeiliche und justizielle Verarbeitung personenbezogener Daten gerade nicht anwendbar ist, bedurfte es allein schon zur Vermeidung von Missverständnissen einer weiteren Normierung des Verfahrens.
Eine weitere Besonderheit im Zusammenhang mit den Sanktionsoptionen des Absatzes 2 Satz 2 Nummer 1 bis 3 liegt in dem geforderten Einvernehmen mit den zuständigen Aufsichtsbehörden im Falle der in Absatz 2 Satz Nummer 3 geregelten Beschränkung bis hin zum Verbot einer Verarbeitung.

Dabei handelt es sich um eine die Aufgabenwahrnehmung derart stark restringierende Maßnahme, dass es hier des Einvernehmens der zuständigen Landespolizeibehörde, im Falle der Vollzugspolizei etwa des Ministeriums für Inneres, Bauen und Sport, bedarf.

Zu § 7, Gegenseitige Amtshilfe:

Die Vorschrift dient der Umsetzung des Artikels 50 der Richtlinie unter Anlehnung an den Wortlaut des § 82 BDSG 2018. Soweit in § 7 nichts anderes geregelt ist, richtet sich die Amtshilfe selbst nach den §§ 4ff. des Saarländischen Verwaltungsverfahrensgesetzes (SVwVfG). Da Artikel 50 der Richtlinie und § 82 BDSG auf eine in § 23 Absatz 1 vergleichbare Regelung verzichten und zudem Absatz 3 fehlendes sprachliches Textverständnis nicht als Ablehnungsgrund zulässt, darf ein Amtshilfeersuchen in jeder der aktuell 24 Amtssprachen der EU gestellt werden.
Absatz 1 regelt den Amtshilfeanspruch der ersuchenden Behörde dem Grunde nach. Eine Besonderheit stellt Absatz 1 Satz 1 2. Halbsatz dar, indem – in Analogie zu den Übermittlungsregelungen - die dort genannten Aufsichtsbehörden denen der Mitgliedstaaten gleichgestellt werden.
Absatz 2 dient dazu, sicherzustellen, dass dem Ersuchen zügig nachgekommen wird.
Absatz 3 beschränkt die Möglichkeit, Amtshilfeersuchen abzulehnen, abschließend auf die dort genannten Optionen Unzuständigkeit und Verstoß gegen Rechtsvorschriften. § 5 Absatz 1 Nummer 2 SVwVfG, „wenn durch die Hilfeleistung dem Wohl des Bundes oder eines Landes erhebliche Nachteile bereitet würden“, kommt nicht zum Tragen.
Absatz 4 regelt die Verpflichtung der oder des Landesbeauftragten für Datenschutz zu einem transparenten Handeln gegenüber der ersuchenden Behörde.
Absatz 5 schreibt nahezu abschließend den Informationsweg vor. In Konsequenz darf von der elektronischen Darstellung nur in begründeten Fällen abgewichen werden.
Absatz 6 regelt den Kostenerstattungsverzicht.
Absatz 7 korrespondiert mit Absatz 1, indem der Fall des Amtshilfeersuchens der oder des Landesbeauftragten für Datenschutz geregelt wird. Die Anforderungen an das Ersuchen gelten auch für an sie oder ihn gestellte Amtshilfeersuchen.

Zu § 8, Datenschutzbeauftragte:

Die Artikel 32 bis 34 der Richtlinie verpflichten zur Benennung eines oder einer Datenschutzbeauftragten. Da die Neuregelung des SDSG diesbezüglich jedoch keine allgemeinen Vorgaben enthält, normiert § 8 SPolDVG Ernennung, Anforderungen und Aufgaben. Absatz 1 Satz 3 stellt klar, dass auch solche Personen zu Datenschutzbeauftragten benannt werden können, denen bereits nach der Datenschutzgrundverordnung (Verordnung (EU) 2016/679) eine solche Aufgabe übertragen wurde.
Die nicht abschließende Aufzählung der Aufgaben des oder der Datenschutzbeauftragten in Absatz 2 orientiert sich an Artikel 34 der Richtlinie sowie an § 7 Absatz 1 BDSG 2018.
Absatz 3 greift den Regelungsgehalt des § 8 Absatz 3 SDSG (alt) auf.

## 3. Abschnitt
## Rechte der betroffenen Person

Zu § 9, Allgemeine Informationen zu Datenverarbeitungen:

§ 9 setzt die in Artikel 13 Absatz 1 der Richtlinie vorgesehenen Transparenzpflichten um. Der Wortlaut entspricht § 55 BDSG 2018. Es handelt sich hierbei um einen Informationsanspruch gegenüber der jeweiligen Polizeibehörde, der keine eigene konkrete Betroffenheit voraussetzt. Die Information kann über öffentlich zugängliche Telemedienangebote, z. B. Homepages oder in sozialen Medien, erfolgen.

Zu § 10, Benachrichtigung der betroffenen Person:

§ 10 setzt Artikel 13 Absatz 2 der Richtlinie um, wobei der Wortlaut – mit Ausnahme der Absätze 5 und 6 - an § 56 BDSG 2018 orientiert ist. Die Vorschrift regelt die Sachverhalte, bei denen eine Informationspflicht infolge der Verarbeitung personenbezogener Daten der betroffenen Person entsteht. Die Informationspflicht kann nur infolge spezialgesetzlicher Vorgaben eintreten, weshalb § 10 Absatz 1 bis 4 im Wesentlichen das grundlegende Verfahren sowie den Datenumfang regelt.
Absatz 2 regelt die Voraussetzungen, unter denen eine Benachrichtigung aufgeschoben, eingeschränkt oder unterlassen werden kann.
Absatz 3 privilegiert mittelbar die Datenverarbeitung der Nachrichtendienste, indem die Benachrichtigung unterbleibt bis zu deren Einwilligung. Gleiches gilt, wenn die Sicherheit eines Landes oder des Bundes tangiert ist. Bei dieser Konstellation hängt die Benachrichtigung ebenfalls von dem Votum der zuständigen Stelle ab.
Absatz 4 regelt unter Verweis auf § 11 Absatz 7 die Möglichkeit, die oder den Landesbeauftragten für Datenschutz anzurufen. Ebenfalls über § 11 Absatz 7 erschließt sich das darauffolgende Verfahren. Über den Verweis auf § 11 Absatz 8 wird die Polizei verpflichtet, die Gründe für eine nur eingeschränkte Information der betroffenen Person zu dokumentieren.
Absatz 5 und 6 greifen als spezielle Vorschriften die Unterrichtungspflichten des bisherigen § 28a Absatz 5 und des § 28d Absatz 2 Satz 6 SPolG (alt) bei besonders eingriffsintensiven verdeckten Maßnahmen auf und ergänzen und konkretisieren diese. Absatz 5 und 6 orientieren sich an den einschlägigen Bestimmungen des § 101 Absatz 5, 6 der Strafprozessordnung (StPO) sowie § 74 des Bundeskriminalamtgesetzes.
Absatz 5 führt einerseits die Maßnahmen auf, bei denen grundsätzlich eine Benachrichtigung zu erfolgen hat, setzt aber gleichzeitig die Voraussetzungen fest, unter denen eine Benachrichtigung zurückgestellt werden kann. Neu eingeführt wurde, dass in den Fällen, bei denen eine Benachrichtigung mehr als zwölf Monate zurückgestellt wird, eine richterliche Entscheidung herbeizuführen ist.
Absatz 6 legt die Fälle fest, in denen eine Benachrichtigung generell unterbleiben muss.

Zu § 11, Auskunftsrecht der betroffenen Person:

§ 11 setzt die Artikel 14 und 15 der Richtlinie um. Bislang war das Auskunftsrecht in § 40 SPolG (alt) geregelt. Wegen des weitergehenden Regelungsumfangs der Richtlinie kann diese Vorschrift nicht unverändert oder nur gering modifiziert in das SPolDVG übernommen werden. Daher entspricht der Wortlaut § 57 BDSG 2018.
Absatz 1 regelt die Einzelkriterien des Auskunftsanspruchs, wobei die Nummern 1 bis 3 in anderer Reihenfolge den Anspruch nach § 40 Absatz 1 Satz 1 und 2 SPolG (alt) abbilden. Neu aufgenommen sind die Nummern 4 bis 8.
Absatz 2 greift § 20 Absatz 1 Satz 2 SDSG (alt) auf und schafft insofern neues materielles Recht, als die Auskunftsverweigerung bislang abschließend in § 40 Absatz 2 SPolG (alt) geregelt war und den in Absatz 2 aufgeführten Ausschlusstatbestand nicht umfasste.

Absatz 3 ist ebenfalls materiell und systematisch neu. Danach ist die Auskunftsverweigerung auch in Abhängigkeit von der Kooperation der betroffenen Person zulässig.
Absatz 4 eröffnet die Möglichkeit unter Verweis auf die Versagungsgründe des § 10 Absatz 2, 5 oder 6 ebenfalls die individuelle Auskunft auf Antrag zu verweigern. Selbstverständlich hat die Ablehnungsentscheidung neben den dort genannten Voraussetzungen dem Grundsatz der Verhältnismäßigkeit zu entsprechen.
Absatz 5 greift den Regelungsgedanken des bisherigen § 40 Absatz 2 SPolG auf.
Absatz 6 Satz 1 und 2 dient der Umsetzung von Artikel 15 Absatz 3 Satz 1 und 2 der Richtlinie. Die Vorschrift orientiert sich am Wortlaut des § 57 Absatz 6 BDSG 2018. Sie eröffnet der Polizei die Möglichkeit, ein Auskunftsverlangen unbeantwortet zu lassen. Satz 3 führt den Regelungsgedanken des bisherigen § 20 Absatz 4 Satz 1 SDSG (alt) fort.
Absatz 7 greift § 20 Absatz 4 Satz 2 SDSG (alt) auf und regelt in Anlehnung an § 57 Absatz 7 BDSG 2018 dezidiert das Verfahren.
Absatz 8 setzt Artikel 15 Absatz 4 der Richtlinie um, orientiert an § 57 Absatz 8 BDSG 2018.

Zu § 12, Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung:

Die Vorschrift bildet in Umsetzung des Artikels 16 der Richtlinie den bisherigen § 21 SDSG (alt) fort. Der Wortlaut orientiert sich an § 58 BDSG 2018, wobei die Absätze 3 und 5 nicht aufgegriffen wurden, da deren Regelungsgehalt durch § 26 Absatz 3 und § 43 Absatz 8 umgesetzt wird.
Absatz 1 setzt Artikel 16 Absatz 1 der Richtlinie um und regelt das Recht auf Berichtigung unrichtiger bzw. auf Vervollständigung unvollständiger Daten. Satz 2 dient der Berücksichtigung der im Erwägungsgrund 30 der Richtlinie vorzufindenden Aussage, dass der Grundsatz der sachlichen Richtigkeit sich nicht auf die Richtigkeit einer Aussage beziehen sollte, sondern lediglich auf die Tatsache, dass eine bestimmte Aussage gemacht worden ist. Gleichzeitig findet sich der in Erwägungsgrund 47 der Richtlinie enthaltende Gedanke wieder, wonach zur Vermeidung massenhafter und nicht erfolgversprechender Anträge klargestellt wird, dass sich die Berichtigung auf Tatsachen bezieht, welche die betroffenen Personen berühren, und nicht etwa auf den Inhalt von Zeugenaussagen. Hiervon umfasst sind auch polizeifachliche Bewertungen.
Absatz 2 regelt den Anspruch auf Löschung aus Artikel 16 Absatz 2 der Richtlinie. Die Vorschrift greift den Regelungsgedanken des § 21 Absatz 3 SDSG (alt) auf und ergänzt die dort geregelte Löschungspflicht um den Tatbestand einer rechtlichen Verpflichtung zur Löschung.
Absatz 3 regelt eine eigenständige Kennzeichnungspflicht für nur eingeschränkt zulässige Verarbeitungen; der Wortlaut entspricht § 58 Absatz 4 BDSG 2018.
Absatz 4 dient der Umsetzung von Artikel 16 Absatz 4 der Richtlinie und führt den Regelungsgedanken des § 11 Absatz 6 für eine eventuell unterlassene Löschung bzw. eine Einschränkung fort. Der Wortlaut orientiert sich an § 58 Absatz 6 BDSG 2018.
Absatz 5 verweist auf entsprechend anwendbare Regelungen im SPolDVG.

Zu § 13, Anrufung der oder des Landesbeauftragten für Datenschutz:

§ 13 regelt das Recht, die oder den Landesbeauftragten für Datenschutz anzurufen und schreibt in Absatz 1 das bisher in § 23 SDSG (alt) normierte Anrufungsrecht betroffener Personen fort.
Absatz 2 enthält die zwingende Verpflichtung der oder des Landesbeauftragten für Datenschutz, Eingaben unverzüglich an die zuständige Aufsichtsbehörde weiter zu leiten.
Die Vorschrift setzt Artikel 52 der Richtlinie um und ist im Wortlaut an § 60 BDSG 2018 angelehnt.

Zu § 14, Rechtsschutz gegen Entscheidungen der oder des Landesbeauftragten für Datenschutz oder bei deren oder dessen Untätigkeit

Die Vorschrift setzt Artikel 53 der Richtlinie um und übernimmt dabei den Wortlaut des § 61 BDSG 2018.
Absatz 1 regelt den gerichtlichen Rechtsschutz gegen Entscheidungen der oder des Landesbeauftragten für Datenschutz.
Absatz 2 enthält die Parallelregelung für den Fall der Untätigkeit oder der nicht rechtzeitigen Befassung. Die Frist von drei Monaten greift die in § 75 Satz 2 der Verwaltungsgerichtsordnung geregelte Zeitspanne für die Einreichung einer Untätigkeitsklage.

Zu § 15, Verfahren für die Ausübung der Rechte der betroffenen Person:

§ 15 setzt Artikel 12 der Richtlinie um, indem weitgehend der Wortlaut des § 59 BDSG 2018 übernommen wird. Absatz 4 enthält eine eindeutiger formulierte Anweisung für die Fälle, in denen begründete Zweifel an der Identität der Antragstellerin oder des Antragsstellers bestehen.

Zu § 16, Schadensersatz:

Die Vorschrift setzt Artikel 56 der Richtlinie um und stellt im Vergleich zu § 839 des Bürgerlichen Gesetzbuchs i. V. m. Artikel 34 des Grundgesetzes eine vorrangige Spezialnorm dar. Der Wortlaut ist an § 83 BDSG 2018 angelehnt.

## Zweiter Teil
## Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Zu § 17, Kategorien betroffener Personen:

§ 17 greift die bisherigen Personenkategorien des § 26 SPolG (alt) und ergänzt diese um drei Kategorien (Verurteilte, Beschuldigte, Personen, die einer Straftat verdächtig sind und wegen der Art oder Ausführung der Tat, der Persönlichkeit der betreffenden Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind, § 17 Absatz 2 Nummer 5 bis 7). Die Erweiterung war erforderlich, da die Daten zu solchen Personen nach Maßgabe des SPolDVG zwar nicht erhoben, aber verarbeitet werden dürfen (vgl. § 23 Absatz 5 und 6).
Während § 26 SPolG (alt) lediglich die Erhebung personenbezogener Daten regelte, kann die Polizei bzw. die Vollzugspolizei personenbezogene Daten der nach § 17 einschlägigen Kategorien nach Maßgabe der §§ 18 bis 29, 31 bis 52 verarbeiten. Diese Vorschrift greift den Regelungsgedanken des Artikels 6 der Richtlinie auf und orientiert sich an §§ 18, 19 des Bundeskriminalamtgesetzes. Hiernach soll bei der Verarbeitung personenbezogener Daten so weit wie möglich zwischen verschiedenen Kategorien personenbezogener Daten betroffener Personen klar unterschieden werden.

Zu § 18, Erhebung personenbezogener Daten:

Die Regelung greift den bisherigen § 26 SPolG auf, Parallelregelungen im BDSG 2018 oder im neu zu erlassenden SDSG existieren nicht.
Absatz 1 regelt die die Zulässigkeit des Erhebens personenbezogener Daten zu Zwecken der Gefahrenabwehr und richtet sich sowohl an die Verwaltungs- als auch an die Vollzugspolizei.

Absatz 2 bevollmächtigt ausschließlich die Vollzugspolizei zur Erhebung personenbezogener Daten zum Zweck der vorbeugenden Straftatenbekämpfung und beschränkt die Zulässigkeit zudem auf einen vergleichsweise engen Personenkreis.
Absatz 3 wiederum lässt die Erhebung personenbezogener Daten eines speziellen Personenkreises, der in den jeweils geregelten Fällen zur Hilfeleistung in Gefahrenabwehrfällen herangezogen werden kann, zu. Die Vorschrift ermächtigt sowohl die Verwaltungs- als auch an die Vollzugspolizei.

Zu § 19, Einwilligung:

§ 19 ist eine Hybridregelung. Die Richtlinie sieht zwar die Möglichkeit der Einwilligung als Rechtsgrundlage für die Verarbeitung nicht vor, lässt sie allerdings in Auslegung von Erwägungsgrund 35, letzter Satz zu: „Dies sollte die Mitgliedstaaten nicht daran hindern, durch Rechtsvorschriften vorzusehen, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke dieser Richtlinie zustimmen kann, beispielsweise im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung ihres Aufenthaltsorts mittels elektronischer Fußfessel zur Strafvollstreckung.“ Die DSGVO sieht hingegen in Artikel 7ff. DSGVO schon die Option der Einwilligung vor.
Der Wortlaut des § 19 greift in Absatz 1 Satz 1 den bisherigen § 25 Absatz 4 SPolG, in Absatz 1 Satz 2 § 4 Absatz 2 Satz 2 SDSG (alt) und ansonsten § 51 BDSG 2018 auf. Neu ist der der Regelungsgedanke des Absatzes 1 Satz 2, wonach die Einwilligung in der Regel schriftlich erfolgen muss.

Zu § 20 Verarbeitung besonderer Kategorien personenbezogener Daten:

Die Vorschrift des § 20 ist § 48 BDSG 2018 nachgebildet und dient der Umsetzung von Artikel 10 der Richtlinie. Danach ist die Verarbeitung besonderer Kategorien personenbezogener Daten nur unter den in Absatz 1 genannten Voraussetzungen zulässig, zunächst der unbedingten Erforderlichkeit zur Aufgabenerfüllung und komplementär eine der unter 1 bis 4 genannten Bedingungen.
In Absatz 2 wird in Satz 1 die Forderung der Artikels 10 der Richtlinie nach geeigneten Garantien dem Grunde nach umgesetzt; Satz 2 konkretisiert dies in Form von Regelbeispielen.

Zu § 21, Speicherung, Veränderung und Verwendung personenbezogener Daten:

§ 21 greift den Regelungsgedanken der bisherigen § 30 SPolG und § 31 SPolG auf und führt ihn richtlinienkonform fort. Absatz 1 Satz 1 und 2 regelt die zweckgebundene Speicherung, Veränderung und Verwendung von personenbezogenen Daten. Für die Polizeiverwaltungsbehörden wird diese strikte Zweckbindung in Satz 3 durchbrochen (analog § 30 Absatz 1 Satz 3 SPolG alt). Eine zweckändernde Speicherung, Veränderung und Verwendung personenbezogener Daten richtet sich für die Vollzugspolizei nach § 23. Aus diesem Grund wurden die bisherigen § 30 Absatz 2 und 3 SPolG (alt) ebenfalls in die Regelungstatbestände des § 23 übernommen.
Absatz 2 Satz 1 stellt die dezidierte Rechtsgrundlage für die Speicherung und die weitere polizeiliche Verwendung von personengebundenen (PHW) und ermittlungsunterstützenden Hinweisen (EHW), beide abschließend geregelt in den jeweiligen Leitfäden des BKA, orientiert an § 16 Absatz 6 BKAG 2018, dar.
Absatz 3 greift den Regelungsgedanken des § 73 BDSG 2018 und des Artikels 7 Absatz 1 der Richtlinie auf. Regelungsziel ist es, sicherzustellen, dass ohne weitere Prüfung der Datensätze zwischen einer subjektiven Einschätzung und einer objektiven Bewertung unterschieden werden kann.
Absatz 4 entspricht § 30 Absatz 5 SPolG (alt).

Zu § 22, Kennzeichnung:

§ 22 ist Ausfluss aus dem Urteil des Bundesverfassungsgerichts zum Bundeskriminalamtgesetz. Das Bundesverfassungsgericht hat festgelegt, dass personenbezogene Daten, die durch verdeckte und eingriffsintensive Maßnahmen erhoben wurden, nur unter ganz gewissen Voraussetzungen zweckändernd verarbeitet werden dürfen. Hierzu hat es den Begriff der „hypothetischen Datenneuerhebung“ (ins Leben gerufen. Dabei hat das Bundesverfassungsgericht keine Anforderungen an die Kennzeichnung postuliert, sondern diese selbst vielmehr als „conditio sine qua non“ für eine zulässige hypothetische Datenneuerhebung definiert. Um die Voraussetzungen für eine solche zweckändernde Nutzung zu schaffen, müssen daher die betroffenen personenbezogenen Datenentsprechend gekennzeichnet werden.
§ 22 setzt die Kennzeichnungspflicht entsprechend um. Zur Gewährleistung des Grundsatzes der hypothetischen Datenneuerhebung normiert die Vorschrift als technisch-organisatorische Folgeregelung die notwendige Kennzeichnung personenbezogener Daten. Die bewusst technikoffene Formulierung verzichtet auf die konkrete Bezugnahme auf Informations-/Dateisysteme oder Verfahren. Damit werden aber die in polizeilichen Informationssystemen gespeicherten Daten gerade nicht von der Kennzeichnung ausgenommen; vielmehr tritt die Kennzeichnungspflicht ausschließlich bei der automatisierten Verarbeitung personenbezogener Daten ein. Bei der Verarbeitung personenbezogene Daten in IT-Systemen, welche der Wahrnehmung der Aufgabe der Gefahrenabwehr einschließlich der vorbeugenden Bekämpfung von Straftaten zu Zwecken des Informationsaustausches, der Auskunft oder der Recherche betrieben werden, erfolgt eine zweckändernde Verwendung, welche die Kennzeichnungspflicht bedingt. Insbesondere zielt die Vorschrift auf die Teilnahme am gemeinsamen Informationsverbund nach § 29 BKAG ab, etwa in Form der Informationssystem POLIS oder PIAV. Die Kennzeichnungspflicht kann sich in Abhängigkeit von deren Nutzung auch bei landesweit betriebenen Verfahren, so beispielsweise bei Vorgangsbearbeitungs-/-verwaltungssystemen manifestieren. § 22 orientiert sich dabei eng an der Vorschrift des § 14 BKAG 2018.
Absatz 1 Satz 1 und 2 legt den Umfang der Kennzeichnungspflicht fest. In Satz 3 werden die sogenannten „aufgedrängten“ Daten geregelt. Dies sind Daten, die nicht selbst durch die Vollzugspolizei erhoben wurden. Diese sind nur soweit möglich nach den Vorgaben des Satz 1 zu kennzeichnen.
Absatz 2 legt ein Verarbeitungsverbot fest, falls die Daten nicht entsprechend des Absatzes 1 gekennzeichnet sind.
Absatz 3 verpflichtet die datenempfangende Stelle, die Kennzeichnung aufrecht zu erhalten.
Die technische Umsetzung der Kennzeichnungspflicht kann nicht sofort und vollständig nach Inkrafttreten des Gesetzes erfolgen. Aus diesem Grund sieht Artikel 5 Absatz 2 eine entsprechende Übergangsvorschrift vor.

Zu § 23, Zweckbindung, Grundsatz der hypothetischen Datenneuerhebung, Datenverarbeitung zu anderen Zwecken:

§ 23 legt fest, unter welchen Voraussetzungen die Vollzugspolizei Daten verarbeiten kann. Das Bundesverfassungsgericht hat in seinem Urteil zum Bundeskriminalamtgesetz Aussagen sowohl zu der nicht zweckändernden Verarbeitung als auch zu der zweckändernden Verarbeitung getroffen. Für letztere wurde der Begriff der sog. „hypothetischen Datenneuerhebung“ (hyDaNe) als Rechtsfigur geschaffen. Die Frage, ob personenbezogene Daten zweckändernd verarbeitet werden dürfen, richtet sich maßgeblich nach den Umständen (Anlass, Maßnahmen etc.), unter welchen die Daten erhoben wurden. Um eine entsprechende Prüfung durchführen zu können, müssen diese personenbezogenen Daten entsprechend gekennzeichnet sein (§ 22).

Für besonders eingriffsintensive Maßnahmen – im Saarland ist das lediglich die Informationserhebung in oder aus Wohnungen – verlangen die Vorgaben des Bundesverfassungsgerichts immer noch die Beachtung des sog. „hypothetischen Ersatzeingriffs“ (vgl. § 161 Absatz 2 StPO).
Die Absätze 1 – 3 konkretisieren in Anlehnung an § 12 BKAG 2018 die vom Bundesverfassungsgericht gestellten Anforderungen an die Zweckbindung und die hypothetische Datenneuerhebung.
Absatz 1 Satz 1 regelt, unter welchen Voraussetzungen personenbezogene Daten zum gleichen Zweck verarbeitet werden können. Absatz 1 Satz 2 regelt den Fall der sog. „aufgedrängten Daten“, bei denen keine Erhebung durch die Vollzugspolizei erfolgt ist. Hier ist der Zweck der ersten Speicherung maßgeblich.
Absatz 1 Satz 3 geht auf die Besonderheit bei der Informationserhebung in oder aus Wohnungen ein und durchbricht damit den Grundsatz aus Satz 1.
Absatz 2 Satz 1 stellt die eigentliche Kernvorschrift für die zweckändernde Verarbeitung personenbezogener Daten unter Beachtung der hyDaNe dar. Abweichungen ergeben sich bei der Verarbeitung der Grunddaten einer Person zur Identifizierung (Satz 2) sowie bei aufgedrängten Daten (Satz 4). Satz 3 stellt klar, dass speziellere Normen den Vorgaben des Absatzes 2 vorgehen.
Absatz 3 Satz 2 regelt den hypothetischen Ersatzeingriff bei Informationserhebungen in oder aus Wohnungen. Die ausführliche Regelung der zulässigen Verwendungen setzt einfachgesetzlich die verfassungsrechtlichen Vorgaben um.
Absatz 4 enthält eine Sonderregelung für die Speicherung, Veränderung und Verwendung von personenbezogenen Daten, die im Rahmen von Ermittlungsverfahren erhoben wurden. Der Verweis auf Absatz 1 und 2 verdeutlicht, dass in den Fällen der Veränderung und Verwendung die hyDaNe zu beachten ist, s. a. Absatz 5.
Die Vorschrift orientiert sich am Regelungsgedanken des bisherigen § 30 Absatz 2 SPolG, verzichtet allerdings auf eine Negativprognose. Die anstehende umfassende Neustrukturierung des polizeilichen Informationsverbundes, Programm Polizei 2020 und „Saarbrücker Agenda“ erfordern eine möglichst frühzeitige Bereitstellung qualitativ hochwertiger Datensätze. Die bisher geregelte saarländische Spezialität, eine Negativprognose bei Tatverdächtigen und Verurteilten zu fordern, wirkte dieser Forderung teilweise entgegen, da häufig erst zu einem späteren Zeitpunkt ausreichende Erkenntnisse vorliegen, die eine substantiierte Prognose einer Legalbewährung ermöglichen. Die bisherige Verfahrensweise mit einer zeitlich verzögerten Bereitstellung von personenbezogenen Daten wirkte sich dahingehend nachteilig aus, dass zum Beispiel im Rahmen von Recherchen bzw. Personensuchen zur Verhinderung terroristischer Straftaten kein tagesaktueller Datenbestand genutzt werden durfte. Der Kooperationspartner Rheinland-Pfalz verzichtet bereits auf eine Negativprognose, nach aktuellen Stand ebenso Bayern, Berlin, Brandenburg, Sachsen-Anhalt, Sachsen, Thüringen, Nordrhein-Westfalen und Hessen.
Absatz 5 greift die Bestimmungen des § 30 Absatz 3 SPolG (alt) auf und ergänzt somit den Absatz 4. Hiernach kann die Polizei personenbezogene Daten auch zu Personen, die keine Verdächtigen, Beschuldigten oder Verurteilten (§ 17 Absatz 2 Nummer 1 bis 4) sind, zur vorbeugenden Bekämpfung von Straftaten speichern, verändern und verwenden. Satz 2 und 3 legen für bestimmte Personenkategorien (§ 17 Absatz 1 Nummer 2 bis 4) abweichend von § 26 Absatz 2 Satz 2 kürzere Speicherfristen (3 Jahre) fest und geben Prüffristen vor. Der Verweis auf Absatz 1 und 2 verdeutlicht, dass in den Fällen der Veränderung und Verwendung die hyDaNe zu beachten ist.
Absatz 6 lässt unter engen Voraussetzungen die Nutzung personenbezogener Daten zur Erstellung von Lagebildern zu.
Absatz 7 ist angelehnt an § 22 Absatz 1 BKAG 2018 und regelt generell, dass - soweit durch dieses Gesetz oder anderweitige Vorschriften nicht ausgeschlossen – gespeicherte personenbezogene Daten zur Aus- und Fortbildung genutzt werden dürfen. Die Vorschrift zielt unter anderem darauf ab, die Verwendung von Videomaterial zu Schulungszwecken zu ermöglichen.

Absatz 8 greift den Regelungsgedanken des § 11 Absatz 3 SDSG (alt) und lässt zu den genannten Zwecken als Ausnahmetatbestand auch eine offene Verarbeitung zu.
Absatz 9 stützt die dort geregelte Datenverarbeitung konsequent auf das allgemeine Datenschutzrecht, da die in der Vorschrift geregelte Verwendung nicht mehr vom Anwendungsbereich der Richtlinie (polizeiliche und justizielle DV) gedeckt ist.
Absatz 10 entspricht § 12 Absatz 5 BKAG 2018 und verweist – insoweit – verstärkend – auf die Verpflichtung zur Umsetzung technisch-organisatorischer Maßnahmen zur Gewährleistung der nicht zweckändernden und zweckändernden Verarbeitung personenbezogener Daten.

Zu § 24, Verarbeitung auf Weisung des Verantwortlichen:

§ 24 setzt Artikel 23 der Richtlinie unter Aufgreifen des Wortlautes von § 52 BDSG 2018 um.

Zu § 25, Automatisierte Einzelentscheidung:

§ 25 setzt Artikel 11 der Richtlinie um, indem das grundsätzliche Verbot automatisierter Einzelentscheidungen geregelt wird. Bisher fand sich eine vergleichbare Regelung in § 4 Absatz 3 SDSG (alt). Der Wortlaut orientiert sich an § 54 BDSG 2018. Wie aus Absatz 1 ersichtlich, muss eine Entscheidung eine nachteilige Rechtsfolge für die betroffene Person zeitigen, mithin in der Regel Verwaltungsaktcharakter entfalten. Reine Binnenentscheidungen, so sie denn bei der polizeilichen Datenverarbeitung denkbar sind, fallen nicht unter das Verdikt des Absatzes 1.

Zu § 26, Berichtigung, Löschung und Einschränkung der Verarbeitung von personenbezogener Daten:

§ 26 greift im Wesentlichen den Wortlaut und die Regelungsinhalte des bisherigen § 38 SPolG auf.
Absatz 2 Satz 1 Nummer 3 enthält einen zusätzlichen Löschungstatbestand. Absatz 2 Satz 4 normiert die bisher im SPolG nicht enthaltene sogenannte „Mitziehregel“, um so die wiederholte Delinquenz der jeweils Betroffenen über einen längeren Zeitraum besser nachvollziehen zu können.
Die Regelung selbst korreliert mit § 12, daher verweist Absatz 5 deklaratorisch darauf, dass die dort aufgeführten Rechte betroffener Personen unberührt bleiben.

Zu § 27, Protokolldaten:

§ 27 Absatz 1 bis 3 regelt in Umsetzung des Artikels 25 der Richtlinie die Protokollierungspflichten der Polizei.
Absatz 1 regelt die Mindestanforderungen an den Protokollierungsvorgang und den Umfang der zu protokollierenden Daten.
Absatz 2 regelt die zulässige Verwendung der erhobenen Protokolldaten zur Datenschutzkontrolle und – zweckändernd, aber durch Artikel 25 der Richtlinie vorgesehen – zur Verfolgung von Straftaten.
Absatz 3 regelt die Löschfristen.

## Dritter Teil
## Besondere Befugnisse zur Verarbeitung personenbezogener Daten

Zu § 28, Abgleich personenbezogener Daten, Zuverlässigkeitsüberprüfung:

§ 28 gibt den Regelungsgehalt von § 36 SPolG (alt) wieder und wird erweitert um die ausdrückliche Befugnis, Zuverlässigkeitsüberprüfungen durchzuführen.
Absatz 2 stellt klar, dass speziellere Vorschriften vorgehen.
Absatz 3 regelt eindeutig, dass – ungeachtet vorrangiger gesetzlicher Vorgaben im Sicherheitsüberprüfungsgesetz und im Luftverkehrssicherheitsgesetz – auch Zuverlässigkeitsüberprüfungen im Wege des Abgleichs personenbezogener Daten mit dem polizeilichen Datenbestand zulässig sind, soweit die betroffene Person darin eingewilligt hat.
Die Einwilligung selbst orientiert sich an den Vorgaben des § 19 und kommt zudem nur unter den in Absatz 3 genannten Tatbestandsvoraussetzungen in Frage. Soweit die Vollzugspolizei die Zuverlässigkeitsüberprüfung nicht als Sonderausprägung ihres behördlichen Selbstschutzes durchführt, wird sie ausschließlich auf Ersuchen andere Behörden tätig. Satz 3 regelt den Sonderfall der Veranstaltungen, die auch die Überprüfung bestimmter Personen erfordern. Durch Satz 4 wird die Möglichkeit eröffnet, die Zuverlässigkeitsüberprüfung auch bei Veranstaltung in privater Trägerschaft durchzuführen, wenngleich unter restriktiveren Voraussetzungen als bei solchen, die durch öffentliche Stellen durchgeführt werden.
Absatz 4 beschreibt abschließend das Verfahren der Zuverlässigkeitsüberprüfung, die mit einer Identitätsfeststellung beginnt, da eine Überprüfung eine gesicherte Identifizierung voraussetzt. Ein anderer Ansatz könnte die Gefahr begründen, falsche Ergebnisse zu produzieren. Die Vorgabe des Satzes 1 verpflichtet die Vollzugspolizei mitnichten dazu, selbst die Vorlage von Ausweisdokumenten oder Kopien derselben zu verlangen. Die Vollzugspolizei darf vielmehr die ersuchende Behörde auffordern, ihr gegenüber die Identität nachzuweisen. Zudem wird die Vollzugspolizei nur subsidiär tätig, da es zunächst ureigenste Aufgaben einer jeden Behörde ist, selbst in dem ihr möglichen Umfang Zuverlässigkeitsüberprüfungen vorzunehmen. Die durch Absatz 4 Satz 3 Nummer 4 eröffnete Möglichkeit der Bundeszentralregisterabfrage steht anderen Bedarfsträgern ebenfalls offen. Nur bei einem übersteigenden Informationsbedarf ist die Aufgabe der weitergehenden Überprüfung der Vollzugspolizei übertragen. Soweit in Satz 3 Nummer 3 Bezug genommen wird auf die Verfassungsschutzbehörde, handelt es sich um das vormalige Landesamt für Verfassungsschutz des Saarlandes, welches nunmehr als Abteilung des Ministeriums für Inneres, Bauen und Sport organisiert ist.
Absatz 5 regelt den Umfang der Mitteilung an die ersuchende Behörde, wobei der Katalog des Satzes 1 durch Satz 3 eine entscheidende Einschränkung erfährt. Darin ist geregelt, dass lediglich Gefahrenabwehr- und Justizbehörden alle unter Satz 1 Nummer 1 bis 5 genannten Daten übermittelt werden dürfen. Andere Stellen werden lediglich darüber informiert, ob Sicherheitsbedenken vorliegen. Die Entscheidung, ob die jeweils betroffene Person zuverlässig ist, obliegt immer den Bedarfsträgern in Form der ersuchenden Stellen. Zur Verfassungsschutzbehörde s. o.
Absatz 6 regelt den Fall der Wiederholungsüberprüfung. Die Entscheidung darüber obliegt der jeweiligen Stelle selbst. Eine Wiederholungsüberprüfung unterliegt denselben Anforderungen wie eine erstmalige. Daher muss eine Einwilligung in die Wiederholungsüberprüfung eingeholt werden und auch die sonstigen Tatbestandsmerkmale des Absatzes müssen vorliegen. Dass eine oder mehrere Voraussetzungen des Satzes 2 Nummer 1 bis 6 vorliegen hat die ersuchende Behörde zugleich mit dem Ersuchen zu bestätigen. Liegen die Voraussetzungen nicht mehr vor, bedarf es keines Ersuchens mehr, ebenso wenig einer Unterrichtung über deren Wegfall und die gespeicherten Datensätze werden nach Absatz 7 automatisch gelöscht.
Absatz 7 regelt die Löschung der im Rahmen von Zuverlässigkeitsüberprüfungen angelegten Datensätze. Die Frist ist bewusst gewählt, um im Falle von Wiederholungsüberprüfungen auf die Daten zurückgreifen zu können.

Zu § 29, Besondere Formen des Abgleichs personenbezogener Daten:

Die Vorschrift übernimmt nahezu unverändert den bisherigen § 37 SPolG. Absatz 4 erfährt demgegenüber eine Präzisierung dahingehend, dass § 34 des FamFG, persönliche Anhörung, nicht anzuwenden ist, da diese dem Zweck einer klandestinen Maßnahme zuwiderliefe.

Zu § 30, Verarbeitung von DNA-Identifizierungsmustern zur Erkennung von DNA-Trugspuren:

§ 30 übernimmt fast wortgleich die Regelung des § 24 des Bundeskriminalamtgesetzes. Er räumt der Vollzugspolizei die Möglichkeit ein, eine DNA-Referenzdatenbank zu führen, um sog. DNA-Trugspuren, die durch Verunreinigungen der betreffenden Spurenträger insbesondere bei der Tatortarbeit sowie der anschließenden Asservierung, Verwendung und Versand entstehen können, auszuschließen. Hierdurch können aufwändige Ermittlungsmaßnahmen die aufgrund von DNA-Trugspuren initiiert werden, vermieden werden.
Die DNA-Analyse nimmt für die Aufklärung von Straftaten eine wesentliche Rolle ein. Die Methoden haben sich dabei in den vergangenen Jahren ständig weiterentwickelt und verfeinert. Mittlerweile ist es möglich, an Kleinstmengen von DNA-Material (Nanogramm) bereits DNA-Identifizierungsmuster festzustellen. Dieser Fortschritt hat jedoch auch den Nachteil, dass die Gefahr der Kontamination solcher Spuren bzw. Spurenträger ebenfalls deutlich gewachsen ist. Die umfangreichen Ermittlungen in den Jahren 2007 und 2008 anlässlich des Mordes an einer Polizistin in Heilbronn nach der mutmaßlichen Täterin (das „Phantom von Heilbronn“) haben gezeigt, wie DNA-Spurenträger durch falsche Handhabung und/oder Unachtsamkeit kontaminiert werden können. In diesem Fall fand die Kontamination im Rahmen der Herstellung der Stäbchen statt, die für die Sicherung solcher Spuren eingesetzt werden. In anderen Fällen wurde aber die Kontamination auch durch Polizeibeamtinnen und Polizeibeamte verursacht, die nicht mit der notwendigen Sorgfalt bei der Spurensicherung, Asservierung und/oder anschließenden Untersuchung vorgingen.
Das erhobene DNA-Identifizierungsmuster der betroffenen Mitarbeiterinnen und Mitarbeiter darf hierzu pseudonymisiert gespeichert werden. Eine unter Datengesichtspunkten weniger belastende anonymisierte Speicherung ist nicht möglich. Denn neben der Feststellung, dass es sich um eine Trugspur handelt, ist es von wesentlicher Bedeutung zu ermitteln, auf welche Weise das Spurenmaterial verunreinigt wurde. Nur auf diese Weise lässt sich für künftige Fälle das Risiko einer erneuten Verunreinigung minimieren. Mit einer anonymisierten Speicherung ist dies nicht möglich.
Die Absätze 1 bis 3 lassen die Verarbeitung solcher DNA-Identifizierungsmuster nur unter engen Vorgaben zu. Die Entnahme der Körperzellen bei den betroffenen Mitarbeiterinnen und Mitarbeiter darf nicht erzwungen werden, wobei auch eine bloße Mitwirkung nicht ausreicht. Die Untersuchung der Körperzellen wird strikt begrenzt; ebenfalls die anschließende Verwendung. Nach Absatz 3 erfolgt die Speicherung in einem gesonderten Dateisystem, wobei strikte Löschfristen zu beachten sind.

Zu § 31, Besondere Formen der Erhebung personenbezogener Daten:

§ 31 lehnt sich im Regelungsgehalt an den bisherigen § 28 SPolG (alt) an.
Eine Änderung erfolgt in Absatz 1 mit Blick auf das BKAG-Urteil des Bundesverfassungsgerichts und die dadurch verworfene Parallelvorschrift des BKAG aufgrund deren mangelnden Bestimmtheit. Die neue Vorschrift orientiert sich an § 45 BKAG 2018.
Absatz 2 wird erweitert um besondere technische Mittel (sonstige besondere für Observationszwecke bestimmte technische Mittel, vgl. § 45 Absatz 2 Nummer 3 BKAG 2018).

Absatz 3 erhält eine im Vergleich zur Vorgängervorschrift übersichtlichere Systematik. Zudem werden die Maßnahmen, welche unter Richtervorbehalt stehen, ausgeweitet. Dadurch wurde der Vorgabe des Bundesverfassungsgerichts entsprochen, welches in seinem Urteil zum Bundeskriminalamtgesetz dies für eingriffsintensive Eingriffs- und Überwachungsmaßnahmen aus Verhältnismäßigkeitsgründen eingefordert hat.
Absatz 4 entspricht dem bisherigen § 28 Absatz 4 SPolG (alt).
Der bisherige § 28 Absatz 5 SPolG (alt) entfällt, da die Unterrichtung der betroffenen Person nunmehr abschließend in § 10 geregelt wird.

Zu § 32, Offene Bild- und Tonaufzeichnungen:

Bislang war die Verarbeitung personenbezogener Daten mittels Bild- und Tonaufzeichnungen in § 27 SPolG (alt) geregelt. § 32 greift die dortigen Vorgaben auf und modifiziert sie:
Absatz 1 greift den Regelungsgedanken des § 21 Absatz 1 des Polizeigesetzes Baden-Württemberg auf. Aus der in Nummer 1 geforderten Gefährdungsanalyse muss sich ein signifikant erhöhtes Gefährdungsrisiko ergeben, das sich auf Tatsachen oder zumindest belastbare Informationen bzw. Erkenntnisse stützt. Wenn entsprechende Erkenntnisse vorliegen, darf die Vollzugspolizei Bild- und Tonaufzeichnungen anfertigen, auch wenn von der davon betroffenen Person keine Störungen ausgehen.
Nummer 2 lässt die Anfertigung von Bild- und Tonaufzeichnungen auch dann zu, wenn keine terroristische Gefährdung indiziert ist. Das hier geforderte besondere Gefährdungsrisiko ist auch dann gegeben, wenn auf Grund der Art und Größe der Veranstaltungen und Ansammlungen erfahrungsgemäß erhebliche Gefahren für die öffentliche Sicherheit entstehen können. Auch hier muss sich das Gefährdungsrisiko aus konkreten, durch Tatsachen gestützten Erfahrungswerten ergeben.
Soweit Art und Größe der Veranstaltung oder Ansammlung nicht den Schluss auf ein besonderes Gefährdungsrisiko zulassen, greift Nummer 3 die bisherige Regelung auf und stellt somit sicher, dass auch dort unter den fortgeltenden Tatbestandsvoraussetzungen personenbezogene Daten von Störerinnen oder Störern bzw. von entsprechenden Gruppen mittels Bild- und Tontechnik erhoben werden dürfen.
Absatz 2 Satz 1 Nummer 1 regelt die vollzugspolizeiliche Befugnis, gefährliche Orte mittels Bildaufzeichnungstechnik zu überwachen, dahingehend neu, dass die Überwachung sog. Kriminalitätsbrennpunkte nunmehr auch ohne konkreten Anlass ermöglicht wird. Die Norm orientiert sich an § 8 Absatz 3 des Hamburgischen Gesetzes über die Datenverarbeitung der Polizei. Diese Vorschrift ermöglicht - zulässig nach dem Urteil des Bundesverwaltungsgerichts vom 25. Januar 2012 (6 C 9711) - die anlasslose Videoüberwachung sog. Kriminalitätsbrennpunkte. Der Begriff „anlasslos“ bezieht sich dabei auf das Fehlen eines konkreten Anlasses, nicht darauf, dass an den Einsatz von Videotechnik überhaupt keine tatbestandlichen Voraussetzungen geknüpft wären.
Absatz 2 Satz 1 Nummer 2 soll die Vollzugspolizei in die Lage versetzen, die Risikoabschätzung und die Gefahrenprognose zu den sog. gefährdeten Orten auf Lagebilder und Erfahrungswerte zu stützen und so auch aufgrund einer ausreichend hohen abstrakten Gefahr etwa für bedeutende infrastrukturelle Einrichtungen Bildaufzeichnungen als Mittel der Gefahrenabwehr einzusetzen.
Absatz 3 setzt das Ergebnis der Prüfung um, inwiefern die rechtlichen Rahmenbedingungen für eine Erweiterung des Einsatzbereichs von Körper-Kameras („Body-Cams“) geschaffen werden können, insbesondere hinsichtlich des polizeilich vielfach geforderten Einsatzes in Wohnungen (Satz 2). Die Verfassungskonformität war Gegenstand eines durch das Ministerium für Inneres, Bauen und Sport in Auftrag gegebenen Gutachtens zu „Verfassungsfragen des präventivpolizeilichen Einsatzes sog. Body-Cams in Wohnungen“. Die beiden Gutachter Prof. Dr. Dr. Markus Thiel und Dr. Knud Dietrich, beide von der Deutschen Hochschule der Polizei kommen darin zu dem Ergebnis, dass ein solcher Einsatz an Artikel 13 Absatz 5 des Grundgesetzes angelehnt werden kann. Dem folgt der Gesetzentwurf.

Demnach ist der Einsatz in Wohnungen nur zulässig zum Schutz der eingesetzten Polizeivollzugsbeamtinnen und –beamten und, als kumulative Voraussetzung, soweit dies zur Abwehr einer dringenden Gefahr für deren Leib oder Leben erforderlich ist:

> Zusammenfassend ist also festzuhalten, dass für die Qualifikation einer Gefahr als dringend sowohl die zeitliche Nähe und die Wahrscheinlichkeit des Schadenseintritts als auch das Ausmaß des zu erwartenden Schadens, und hier vor allem die Hochrangigkeit des gefährdeten Rechtsguts, von Bedeutung sind. Die besonders ausgeprägte Verwirklichung einer der Komponenten kann dazu führen, dass an eine jeweils andere weniger hohe Anforderungen zu stellen sind.
> (Maunz/Dürig/Papier, 87. EL März 2019, GG Art. 13 Rn. 95)

Nicht erforderlich ist, dass die Gefahr bereits eingetreten ist oder unmittelbar bevorsteht.
Aufgrund der Beschränkung auf die reine Eigensicherung bedarf es keiner besonderen Vorgaben zur Anordnungsbefugnis, diese liegt bei der Einsatzleitung vor Ort im Rahmen des Einsatzes; Satz 2 2. Halbsatz setzt damit die Forderung aus Artikel 13 Absatz 5 Satz 1 des Grundgesetzes nach einer gesetzlichen Festlegung der Anordnungsbefugnis um.
Abweichend von § 34 Absatz 1 Satz 1 ist der Einsatz der Kameras in Wohnungen nicht zulässig zum Schutz Dritter, wenngleich der Einsatz der Vollzugspolizei in Wohnungen in der überwiegenden Mehrheit der Fälle durch häusliche Gewalt begründet ist. Lediglich der polizeiliche Einsatz selbst dient damit in aller Regel dem Schutz dritter Personen, also der Vornahme klassischer vollzugspolizeilicher Maßnahmen präventiven Charakters. Der Einsatz von Bild- und Tonaufzeichnungstechnik verfolgt hingegen einem anderen Zweck, dem ausschließlichen Schutz der eingesetzten Polizeivollzugsbeamtinnen und-beamten; der Zweck des Einsatzes wirkt sich mithin nicht auf den eigensichernden Charakter der eingesetzten technischen Mittel aus. Eine an Artikel 13 Absatz 5 des Grundgesetzes orientierte Rechtsgrundlage muss eben dies gewährleisten und darf nicht generell dritte Personen einbeziehen.
Dies schließt jedoch eine diesbezüglich zweckändernde Nutzung nicht völlig aus, da Artikel 13 Absatz 5 Satz 2 des Grundgesetzes diese unter dem Vorbehalt erlaubt, dass zuvor die Rechtmäßigkeit der anderweitigen Verwendung richterlich festgestellt ist:

> „Obwohl der einzige Zweck der technischen Überwachung in dem Schutz der eingesetzten Personen liegt, lässt sich natürlich trotzdem nicht ausschließen, dass hierdurch Erkenntnisse gewonnen werden, die für die Strafverfolgung oder für die Gefahrenabwehr von Bedeutung sind. Eine solche anderweitige Verwertung gestattet Art. 13 Abs. 5 Satz 2, 1. Halbsatz unter der Voraussetzung, dass zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt ist. Mit „Gefahrenabwehr“ ist hierbei die über den Schutz der im Einsatz befindlichen Person hinausgehende Abwehr von Gefahren gemeint. Diese letztgenannten Fälle dürften jedoch selten praktisch werden, weil für die Gefahrenabwehr unproblematisch auch die Wahrnehmung der im Einsatz befindlichen Person verwendet werden kann und daher auf die Aufzeichnung gar nicht zurückgegriffen werden muss.
> Die richterliche Entscheidung betrifft dabei (zunächst) nur die Frage, ob die Voraussetzungen des Art. 13 Abs. 5 bzw. der entsprechenden einfachgesetzlichen Vorgaben eingehalten worden sind.“ (Maunz/Dürig/Papier, 87. EL März 2019, GG Art. 13 Rn. 108, 109)

Klarstellend verweist Satz 3 deshalb darauf, dass in den in der zitierten Kommentierung beschriebenen Konstellationen eine richterliche Entscheidung zwingend ist.
Auch die so mögliche anderweitige Verwendung der erhobenen personenbezogenen Daten, etwa zur Strafverfolgung oder zur (allgemeinen) Gefahrenabwehr ändert nichts an den relativ niedrigschwelligen Einsatzvoraussetzungen.
Absatz 4 übernimmt unverändert den bisherigen § 27 Absatz 4 SPolG (alt).
Absatz 5 regelt die Hinweispflichten, wobei der Umfang der Hinweispflicht an § 25 Absatz 2 SDSG 2018 orientiert ist. Im Unterschied zu dieser Regelung ist Satz 2 zweiter Halbsatz offener formuliert, um so auch QR-Codes o. ä. verwenden zu können.

Die umfassende Informationspflicht ist bei Einsatz von Body-Cams nicht in dem Maße erforderlich, da hier Vollzugskräfte und den Betroffene in direkter Interaktion stehen.
Absatz 6 regelt die Löschfristen. Diese sind für die in Nummer 2 geregelten Fallgruppen im Vergleich zum § 27 Absatz 6 Nummer 2 SPolG (alt) auf einen Monat verlängert, was einer Forderung der Praxis entspricht.

Zu § 33, Erhebung und Speicherung von Anrufen und des Sprechfunks:

Die Regelung des § 33 Absatz 1 war bisher in § 27 Absatz 5 SPolG enthalten und dort systematisch fehl am Platz. Daher ist im SPolDVG ein eigener Paragraf vorgesehen. Anders als bisher erfolgt die Aufzeichnung künftig obligatorisch, was nicht für sonstige Anrufe gilt.
Absatz 2 greift die Speicherungsfrist des § 32 Absatz 6 Nummer 2 für Ton- und Bildaufzeichnungen auf und stellt so eine Parallelität her.
Absatz 3 geht zurück auf Forderungen aus der Praxis. Bislang war die Aufzeichnung des polizeilichen Sprechfunkverkehrs nicht gesetzlich geregelt. Die Speicherungsfrist ergibt sich aus Absatz 2.
Absatz 3 regelt die entsprechende Anwendung für den polizeilichen Sprechfunk. Hinweisen an anrufende Personen auf die Aufzeichnung des Gesprächs bedarf es nicht.

Zu § 34, Erhebung personenbezogener Daten in oder aus Wohnungen:

Die Vorschrift ersetzt die Regelung des bisherigen § 28a SPolG. Die tatbestandlichen Voraussetzungen des Absatzes 1 wurden an die Vorgaben des Bundesverfassungsgerichts zum Bundeskriminalamtgesetz angepasst; die Vorschrift orientiert sich dabei an § 46 des Bundeskriminalamtgesetzes. Die bislang in § 28a Absatz 1 Satz 2 SPolG enthaltene Kennzeichnungspflicht entfällt, da sie bereits von der Neuregelung des § 22 umfasst ist.
Absatz 2 und 3 entsprechen in wesentlichen Teilen den bisherigen Regelungen des § 28a Absatz 2 und 3 SPolG. Im Vergleich hierzu neu ist Absatz1 Satz 1 2. Halbsatz. Dieser setzt die Forderungen des Bundesverfassungsgerichts (1BvR 966/09, 1 BvR 1140/09, zum BKAG) an einen hinreichend substantiierten Antrag um, der dem Gericht eine tatsächliche Kontrolle erlaubt. Dabei verweist die Vorschrift statisch auf die Korrespondenznorm des § 46 des Bundeskriminalamtgesetzes.
Absatz 4 entspricht weitgehend dem bisherigen § 28a Absatz 4 SPolG. Lediglich die Begrifflichkeit „Sperren“ wurde durch die Vorgabe der Richtlinie in „Einschränken“ geändert.
Die bislang in § 28a Absatz 5 SPolG geregelten Berichtspflichten werden zentral in § 66 zusammengeführt.

Zu § 35, Überwachung und Aufzeichnung der Telekommunikation:

§ 35 regelt die bisher in § 28b SPolG normierte Überwachung der Telekommunikation, wobei die bisherigen Absätze 1, 2, 3, 6 und 7 weitestgehend materiell unverändert bleiben. Der Erweiterung des Personenkreises in Absatz 1 Nummer 3 a), b) dient der Aufnahme der sog. Nachrichtenmittler, s.a. § 100a Absatz 3 StPO, § 51 Absatz 1 Nummer 4, 5 BKAG. Die Erweiterung ist verfassungsrechtlich insoweit unbedenklich, als der Nachrichtenmittler von der Zielperson gezielt in die Tatausführung eingebunden wird, vgl. BVerfG, a. a. O., RN 233 zu § 20 Absatz 1 Nummer 3, 4 BKAG: „Die Vorschrift erlaubt es demnach nicht, „Überwachungsmaßnahmen ins Blaue hinein auf alle Personen zu erstrecken, die mit der Zielpersonen Nachrichten ausgetauscht haben, sondern setzt eigene in der Anordnung darzulegende Anhaltspunkte voraus, dass der Nachrichtenmittler von der Zielperson in die Tatdurchführung eingebunden wird und somit eine besondere Tat- oder Gefahrennähe aufweist.“ Dem folgt auch der Regelungsgedanke des Absatzes 1 Nummer 3.

Absatz 2 regelt neu die Quellen-TKÜ, materiell orientiert an § 51 Absatz 2 BKAG 2018 i. V. m. § 49 BKAG 2018. Diese Vorschriften werden adaptiert und ergänzt durch die zusätzliche Regelung des Absatzes 2 Satz 1 Nummer 2, wodurch die Vollzugspolizei in die Lage versetzt wird, auch solche Daten zu erheben, die im jeweiligen informationstechnischen System gespeichert sind. Die Regelung lehnt sich an § 100a Absatz 1 Satz 3 StPO an und stellt klar, dass über die laufende Kommunikation auch die bereits abgeschlossene und gespeicherte überwacht und aufgezeichnet werden darf, soweit diese im überwachten System gespeichert sind. Die Regelung zielt insbesondere auf den infolge der Nutzung von über Messenger-Dienste generierten Datenverkehr ab, der aufgrund der verwendeten Verschlüsselungstechniken mit herkömmlicher Telekommunikationsüberwachung kaum noch zu überwachen ist. Dabei ist die Erhebung auf solche Daten zu beschränken, die auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form erhoben werden könnten.
Absatz 3 entspricht dem bisherigen § 28b Absatz 3 SPolG, wobei Satz 2 den Einsatz technischer Mittel (insbesondere der sog. „IMSI-Catcher“) zur Feststellung des Standortes eines mobilen Telekommunikationsgeräts konkretisiert.
Absatz 4 Satz 7 und 8 regelt, dass der Einsatz des sog. IMSI-Catcher (oder vergleichbarer technischer Geräte), der lediglich dazu dienen soll, den Aufenthaltsort einer der dort genannten Personen oder eines potentiellen Suizidanten festzustellen, auch ohne richterliche Entscheidung erfolgen darf. Dies gilt auch für solche Fälle, bei denen im Rahmen der Überwachung und Aufzeichnung der Telekommunikation nach den Absätzen 1 und 2 sog. Stille SMS („Stealth ping“) zur überwachten Nummer gesandt werden, um durch die auf diese Weise erzeugten Verkehrsdaten verdeckt den Aufenthaltsort der überwachten Person festzustellen.
Nach der Rechtsprechung des Bundesverfassungsgerichts stellt insbesondere der Einsatz von IMSI-Catchern keinen Eingriff in das durch Artikel 10 des Grundgesetzes geschützte Fernmeldegeheimnis dar, sondern einen solchen in das Grundrecht auf informationelle Selbstbestimmung (Beschluss vom 22. August 2006, 2 BvR 1345/03). Dieser steht jedoch auch unter dem Vorbehalt einer richterlichen Entscheidung. Gleiches gilt grundsätzlich auch für das Versenden der sog. stiller SMS (vgl. BGH, Beschluss vom 8. Februar 2018, 3 StR 400/17), die demnach zumindest bei repressivem Einsatz jeweils einer richterlichen Anordnung nach § 35 Absatz 4 Satz 1; dies gilt auch für die in Absatz 1 geregelten Voraussetzungen mit Ausnahme der in Absatz 4 aufgeführten Fallgruppen. Die Maßnahmen dienen dann ausschließlich dem Schutz der betreffenden Personen, so dass die verfahrensbegleitenden Anforderungen geringer sein dürfen.
Absatz 5 entspricht dem bisherigen § 28b Absatz 2 SPolG.
Der bisherige § 28b Absatz 5 SPolG entfällt, da die Regelung in der Vergangenheit bei Vollzugspolizei und Telekommunikationsunternehmen bisweilen zu Fehlinterpretationen verleitete. Eine Standortbestimmung mittels Erhebung von Verkehrsdaten nach § 96 Absatz 1 Nummer 1 TKG richtet sich nun ausschließlich nach § 36 Absatz 1 Satz 2. Die Aufzeichnung und Überwachung von Telekommunikationsinhalten – auch wenn durch die Auswertung der Inhalte nur der Standort der überwachten Personen festgestellt werden soll – richtet sich nach § 35 Absatz 1 oder 2.

Zu § 36, Erhebung von Telekommunikationsdaten und Nutzungsdaten von Telemedien bei Diensteanbietern:

Die Vorschrift greift die bisherige Regelung des 28c SPolG auf und modifiziert diese.
Absatz 1 Satz 2 regelt den Umfang der zulässigen Datenabfrage bei ausschließlicher Verwendung der angefragten Daten zur Standortbestimmung. Ansonsten übernimmt Absatz 1 unverändert den § 28c Absatz 1 SPolG unverändert.
Absatz 2 greift den bisherigen § 28c Absatz 2 SPolG auf.

Absatz 3 erlaubt unter den Voraussetzungen des Absatzes 1 die Erhebung von Bestandsdaten nach § 14 Absatz 1 und von Nutzungsdaten nach § 15 Absatz 1 des Telemediengesetzes (TMG). Da letzteres die Möglichkeit eröffnet, diese Daten an Sicherheitsbehörden zu übermitteln, hat der Bundesgesetzgeber seines getan, so dass es für eine Erhebung durch eben diese Stellen einer entsprechenden fachgesetzlichen Regelung bedarf. Durch § 14 Absatz 2 i. V. m. § 15 Absatz 5 Satz 4 TMG ist keine Auskunftsverpflichtung, sondern lediglich eine Übermittlungsberechtigung geschaffen. Nach dem Doppeltürmodell (BVerfGE 130, 151) bedarf es aber auf Seiten der grundsätzlich abrufberechtigten Vollzugspolizei einer Erhebungsbefugnis; diese wird in § 36 Absatz 3 geschaffen.
Inhaltlich greift Absatz 3 § 52 Absatz 2 BKAG 2018 auf, dessen Vorgängerregelung in Form von § 20m Absatz 2 BKAG alt vom Bundesverfassungsgericht in der bereits mehrfach zitierten Entscheidung zum BKAG alt nicht verworfen wurde. Die durch die Regelung erlaubte Erhebung von Nutzungsdaten nach dem Telemediengesetz begegnet somit keinen verfassungsrechtlichen Bedenken.
Absatz 4 erlaubt unter den Voraussetzungen der Absätze 2, 3 auch die Abfrage der zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse und stellt so auch für diese Datenerhebung den durch das Bundesverfassungsgericht geforderten zweiten Flügel des Doppeltürmodells dar.
Absatz 5 regelt für jede einzelne Maßnahme die Anordnungsbefugnis.

Zu § 37, Unterbrechung von Telekommunikationsdiensten:

§ 37 zielt darauf ab, die Mobilfunkkommunikation situativ zu unterdrücken. Hierzu wird der Einsatz sog. Jammer unter abschließend definierten Bedingungen zugelassen. Solche Maßnahmen können erforderlich werden, wenn etwa der begründete Verdacht besteht, dass ein Sprengsatz durch Mobilfunk gezündet werden soll.
Bislang existieren zumindest in zwei Polizeigesetzen Regelungen zur Unterdrückung der Mobilfunkkommunikation:

- § 29a des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin regelt, dass die Polizei bei einer dringenden Gefahr für Leib oder Leben im Nahbereich einer Sprengvorrichtung zur Entschärfung den Mobilfunkverkehr blockieren kann.
- § 33 des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt enthält eine Norm, die Gegenstand einer Verfassungsklage war und durch das Landesverfassungsgericht für verfassungskonform befunden wurde (Landesverfassungsgericht des Landes Sachsen-Anhalt, Urteil vom 11. November 2014 – LVG 9/13).

§ 37 SPolDVG orientiert sich in Wortlaut und Regelungsumfang an der verfassungsfesten Norm des § 33 SOG LSA und eröffnet so ausschließlich der Vollzugspolizei, die Möglichkeit, die mobile Kommunikation örtlich und zeitlich begrenzt unter engen Voraussetzungen unterbrechen zu lassen oder selbst zu unterbrechen.
Absatz 1 verpflichtet die Telekommunikationsanbieter die Telekommunikation die Kommunikation zu unterdrücken. Zulässig ist dies nur zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person.
Absatz 2 regelt den aktiven Einsatz sog. Jammer durch die Vollzugspolizei.
Absatz 3 weist die Anordnungsbefugnis der Behördenleitung oder eine von ihr beauftragte Beamtin oder einen von ihr beauftragten Beamten des höheren Polizeivollzugsdienstes zu. In der Anordnung sind Raum und Zeit der Unterbrechung zu definieren. Da die Maßnahme im Vergleich mit einer Telekommunikationsüberwachung von einer geringen Eingriffsintensität ist, bedarf es lediglich einer richterlichen Bestätigung.

Zu § 38, Elektronische Aufenthaltsüberwachung:

Die Vorschrift stellt eine Neuregelung dar, die die saarländische Vollzugspolizei in die Lage versetzt, insbesondere im Rahmen der Abwehr von Gefahren durch den internationalen Terrorismus den Aufenthaltsort der jeweiligen Gefährderin oder des Gefährders zu überwachen. Mittels der elektronischen Aufenthaltsüberwachung kann die betroffene Person im Geltungsbereich des SPolDVG aufgrund einer richterlichen Entscheidung ein den jeweiligen Aufenthaltsort eindeutig bestimmbares technisches Mittel („elektronische Fußfessel“) mit sich führen, genauer: dessen Anbringung dulden.
Bislang war die Anordnung der elektronischen Aufenthaltsüberwachung nur im Rahmen der strafprozessualen Führungsaufsicht, also nach Strafverbüßung möglich, nunmehr wird dieses Instrument auch auf der präventiven Ebene eingeführt, um so den Aufenthaltsort von Personen, von denen eine Gefahr im Sinne des Absatzes 1 oder 2 ausgeht, ständig zu überwachen und so die Wahrscheinlichkeit der Begehung derartiger Straftaten zu minimieren.
Der Wortlaut der Vorschrift orientiert sich an den Abschlussbericht Bund-Länder-Arbeitsgruppe des UA Recht und Verwaltung unter Beteiligung der AG Kripo und des UA FEK (Führung, Einsatz, Kommunikation) „Gesetzgeberische Handlungsempfehlungen im Zusammenhang mit islamistischem Terrorismus“, Stand Mai 2017.
Absatz 1 nennt die Tatbestände, welche die Anordnung einer elektronischen Aufenthaltsüberwachung rechtfertigen. Hauptziel ist die Abwehr hinreichend konkretisierender Gefahren mit einem sehr hohen Schadenspotenzial. Der Abwägung mit den Rechten der betroffenen Person im Sinne einer Prüfung der Verhältnismäßigkeit der Maßnahmen wird bereits auf normativer Ebene vorgegeben, indem in Satz 1 eine Beschränkung auf die Gefahr schwerer Straftaten vorgenommen wird. Satz 2 regelt die Befugnis, ein Aufenthaltsverbot nach § 12 Absatz 4 SPolG zu verhängen, soweit die Maßnahme zur Abwehr einer in § 38 Absatz 1 Satz 1 SPolDVG genannten Straftat dient.
Absatz 2 regelt vergleichbar § 56 Absatz 2 BKAG 2018 die Befugnisse der Vollzugspolizei im Rahmen von Maßnahmen nach § 38 SPolDVG, wobei Satz 1 die Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten der betroffenen Person enthält. Eine Datenerhebung aus Wohnungen hat sich auf die Information darauf zu beschränken, dass sich die betroffene Person in der Wohnung aufhält, eine genauere Ortung dort ist unzulässig. Die Verarbeitung personenbezogener Daten hat automatisiert zu erfolgen, um so jegliche weitere Einflussnahme insbesondere im Rahmen des Erhebungsprozesses zu vermeiden und sicher zu stellen, dass die Vollzugspolizei nur die Daten erhält, die zur Aufgabenerfüllung erforderlich sind.
Absatz 3 greift § 56 Absatz 5 bis 8 BKAG 2018 auf und fasst die dortigen Regelungsgedanken zusammen. Generell unterliegt eine Maßnahme nach Absatz 1 dem Richtervorbehalt, von dem nur in der in Satz 3 genannten Fallgruppe abgewichen werden darf, hierbei ist eine richterliche Bestätigung unabdingbar. Satz 2 regelt, dass, abweichend von den sonstigen Vorgaben zum richterlichen Verfahren in diesem Gesetz, das gesamte Erste Buch des FamFG entsprechend anzuwenden ist und damit auch die Anhörung der oder des Beteiligten. Der Grund liegt darin, dass die Anordnung der elektronischen Aufenthaltsüberwachung auf eine offene Maßnahme abzielt, die der Adressatin oder dem Adressaten eine Duldung auferlegt. Satz 4 und 5 normiert die Anforderungen an den vollzugspolizeilichen Antrag und die richterliche Anordnung. Satz 6 regelt insbesondere die Höchstdauer, Satz 7 die Möglichkeit, die Maßnahmen auch mehrfach zu verlängern. Satz 8 gibt zwingend vor, dass die Maßnahme bei Wegfall der Anordnungsvoraussetzungen unverzüglich zu beenden ist.
Absatz 4 regelt die Löschfristen sowie die Voraussetzungen einer darüber hinaus gehenden weiteren Verarbeitung. Weiter ist eine dezidierte Protokollierungspflicht vorgegeben. Darüber hinaus regeln die Sätze 5 bis 7 den Umgang mit in Wohnungen abweichend von Absatz 2 Satz 3 erhobenen Daten.

Absatz 5 enthält eine Strafvorschrift. Da das Strafrecht der konkurrierenden Gesetzgebung nach Artikel 74 Absatz 1 Nummer 1 GG unterliegt, ist der Landesgesetzgeber gemäß Artikel 72 Absatz 1 GG zu einer Regelung befugt, soweit und solange der Bundesgesetzgeber von seiner Regelungsbefugnis keinen Gebrauch macht. Da der Bund im Rahmen seiner Vorschriften eine Strafbarkeit lediglich für Verstöße gegen die bundesrechtlichen Anordnungen normiert, sind die Landesgesetzgeber nicht daran gehindert, ihrerseits Verstöße zu pönalisieren

Zu § 39, Anlassbezogene automatische Kennzeichenfahndung:

§ 39 greift den Regelungsgedanken des bis zum Inkrafttreten des Polizeirechtsänderungsgesetzes vom 12. November 2014 (Amtsbl. I S. 1465) geltenden § 27 Absatz 3 SPolG (ganz alt) auf. Auch danach durfte die Vollzugspolizei Kraftfahrzeugkennzeichen automatisiert erheben. Die seinerzeitige Regelung wurde auch wegen ihrer unter den durch das Bundesverfassungsgericht im Urteil vom 11. März 2008 (BVerfGE 120, 378) entwickelten Grundsätzen wohl überwiegenden Verfassungswidrigkeit nie angewandt.
Die nunmehrige Regelung orientiert sich hinsichtlich der in Satz 1 genannten Eingriffsvoraussetzungen an der Vorschrift des § 36a des Brandenburgischen Polizeigesetzes, welche vom BVerfG ausdrücklich als zulässige Eingriffsnorm bezeichnet wird. Die eng gesteckten Grenzen des Eingriffszwecks lassen auch die Statuierung eines weiten Verwendungszwecks zu, so das BVerfG. Die weiter vorgesehenen Regelungen zur Verwendung der erfassten Daten sehen daher wiederum den Abgleich zu Fahndungszwecken vor, definieren diesen aber abschließend.
Absatz 3 greift die Forderung des Bundesverfassungsgerichts im Beschluss vom 18. Dezember 2018, 1 BvR 142/15, zum verdeckten Einsatz von automatisierten Kennzeichenerfassungssystemen nach einer verpflichtenden Dokumentation des Einsatzes solcher Systeme gefordert, um so die Entscheidung für und die Durchführung solcher Maßnahmen nachvollziehen zu können. Dem folgt § 39 Absatz 3 unter Rückgriff auf die Löschfristen des § 27 Absatz 3.

Zu § 40, Polizeiliche Beobachtung:

§ 40 entspricht dem bisherigen § 29 SPolG mit Ausnahme der Überschrift und somit der Bezeichnung der polizeilichen Maßnahme. Der bisherige § 29 SPolG regelte die polizeiliche Beobachtung als „Kontrolle“, § 40 greift die weiter verbreitete Diktion „Beobachtung“ auf, vgl. etwa § 32 POG RP.

Zu § 41, Schutz des Kernbereichs privater Lebensgestaltung und Schutz zeugnisverweigerungsberechtigter Personen:

Die Vorschrift greift in Absatz 1 bis 3 den Regelungsgedanken des bisherigen § 28d SPolG (alt) auf und entwickelt diesen – ergänzt um die Vorgaben des Bundesverfassungsgerichts[2] - weiter. Demnach darf eine Maßnahme zur Wohnraumüberwachung nach § 34 Absatz 1 Satz 1 nur angeordnet und durchgeführt werden, soweit nach einer Prognoseentscheidung anzunehmen ist, dass kernbereichsrelevante Inhalte nicht erfasst werden. Besteht die Wahrscheinlichkeit, dass die beabsichtigte Maßnahme in den Kernbereich privater Lebensgestaltung eingreift, ist sie zu unterlassen.
Anders die Systematik in Absatz 1 Satz 2, wonach eine der dort unter Nummer 1 -4 aufgeführten Maßnahmen dann unzulässig ist, wenn eine Prognoseentscheidung den Schluss nahelegt, dass hierdurch ausschließlich kernbereichsrelevante Daten erhoben würden, siehe hierzu auch Begründung zum Polizeirechtsänderungsgesetz vom 12. November 2014, Amtsbl. I S. 1465, Lt.-Drs. 15/899.

[2] Bundesverfassungsgericht, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, RN 198f

Ebenfalls den Vorgaben des Bundesverfassungsgerichts, a. a. O., RN 200, folgt die Änderung des Absatzes 2 Satz 2 im Vergleich zu § 28d SPolG. Demnach ist bereits die Rechtmäßigkeit der Erhebung personenbezogener Daten in oder aus Wohnungen durch eine unabhängige Stelle zu prüfen und zwar noch vor der inhaltlichen Kenntnisnahme durch die erhebende Dienststelle.
Die nach Auswertung der externen Anhörung neu formulierten Absätze 4 bis 7 orientieren sich in Wortlaut und Regelungsumfang an § 62 BKAG 2018 (Bt-Drs. 18/11163), worin wiederum die Vorgängerregelung des § 20u (Bt-Drs. 16/10121) weitestgehend abgebildet ist.
Die Vorschriften dienen dem Schutz zeugnisverweigerungsberechtigter Personen vor verdeckten Maßnahmen. Die an den verschiedenen Berufsgruppen orientierte Differenzierung zwischen absoluten Erhebungsverboten und relativen Verwertungsverboten ist durch das Bundesverfassungsgericht als verfassungskonform bestätigt:
Die Differenzierung zwischen den jeweils von § 160a Absatz 1 und Absatz 2 StPO erfassten Personengruppen ist zudem im Hinblick auf die Anforderungen des Artikels 3 Absatz 1 GG gerechtfertigt. So ist bei den von § 160a Absatz 1 StPO erfassten Berufsgruppen ein absolutes Beweiserhebungs- und -verwertungsverbot jeweils durch besonders gewichtige Gründe gerechtfertigt.
(BVerfG, Beschluss vom 12. Oktober 2011 – 2 BvR 236/08 –, BVerfGE 129, 208-268)
Absatz 4 nennt in Satz 1 die Personengruppen, die absoluten Schutz genießen, demzufolge verdeckte Maßnahmen bereits unzulässig sind, wenn diese überhaupt Erkenntnisse erbringen würden, über die das Zeugnis verweigert werden dürfte. Maßnahmen, die sich gegen andere Personen – etwa einen Beschuldigten oder einen Dritten – richten, bleiben dagegen zulässig, und zwar auch dann, wenn nicht ausgeschlossen werden kann oder gar zu erwarten ist, dass möglicherweise auch die Kommunikation mit den vorgenannten Berufsgeheimnisträgern über vom Zeugnisverweigerungsrecht umfasste Inhalte betroffen sein wird.
Der letztgenannten Konstellation einer zufälligen Betroffenheit auch des Berufsgeheimnisträgers begegnet die Regelung durch das in Satz 5 enthaltene Verbot der Verwertung von Erkenntnissen, die – nicht zielgerichtet – von dem Berufsgeheimnisträger erlangt wurden und über die dieser das Zeugnis verweigern dürfte.
Absatz 5 regelt ein an Verhältnismäßigkeitsaspekten orientiertes Erhebungs- und Verwertungsverbot, das im Einzelfall bei den von Absatz 1 nicht erfassten Berufsgeheimnisträgern, denen das Gesetz ein Zeugnisverweigerungsrecht zubilligt, zum Tragen kommen kann. Erfasst sind nach Absatz 2 namentlich die in § 53 Abs. 1 Satz 1 Nr. 3, 3a und 3b StPO genannten Beratungs- und Heilberufe, die von § 53 Abs. 1 Satz 1 Nr. 5 StPO in Bezug genommenen Medienmitarbeiter sowie die in Nummer 3 genannten Personen, die nicht Rechtsanwälte/-innen oder Kammerrechtsbeistände sind. Im Rahmen der von Absatz 2 geforderten Abwägung ist das primär öffentliche Interesse an einer wirksamen Gefahrenabwehr mit dem öffentlichen Interesse an den durch die zeugnisverweigerungsberechtigten Personen wahrgenommenen Aufgaben und dem individuellen Interesse an der Geheimhaltung der einem Berufsgeheimnisträger anvertrauten oder bekannt gewordenen Tatsachen abzuwägen. Je nach dem Ergebnis der Verhältnismäßigkeitsprüfung kann die im konkreten Fall in Aussicht genommene Maßnahme in vollem Umfang zulässig sein.
Nach Absatz 6 sind Regelungen der Absätze 4 und 5 entsprechend anwendbar, soweit es sich um die in § 53a StPO genannten Berufshelferinnen und -helfer handelt.
Absatz 7 beinhaltet die sogenannte Verstrickungsregelung. Demnach endet der durch die Absätze 4 bis 6 gewährleistete besondere Schutz, wenn Berufsgeheimnisträgerinnen oder -träger selbst für die Gefahr verantwortlich sind, welche mit der in Rede stehenden Maßnahme abgewehrt werden soll. Denn der Schutz der betroffenen Vertrauensverhältnisse oder der Institutionen an sich soll nicht zur Begründung von Geheimbereichen führen, in denen die Verursachung von Gefahren einer staatlichen Aufklärung schlechthin entzogen ist.

Zu § 42, Protokollierung verdeckter oder eingriffsintensiver Maßnahmen

Die Absätze 1 bis 3 enthalten Protokollierungspflichten, die bei der Durchführung von verdeckten oder eingriffsintensiven Maßnahmen zu beachten sind. Das Bundesverfassungsgericht hat in seinem Urteil zum Bundeskriminalamtgesetz eine Protokollierung solcher Maßnahmen angemahnt, um auf diese Weise überhaupt die Voraussetzungen für die Durchführung entsprechender datenschutzrechtlicher Kontrollen zu schaffen (vgl. § 5 Absatz 2 SPolDVG). Absatz 7 enthält enge Verwendungsbeschränkungen für die im Rahmen dieser Maßnahmen erhobenen Daten.
Insgesamt orientiert sich die Vorschrift an den Bestimmungen des § 82 des Bundeskriminalamtsgesetzes.

## Vierter Teil
## Übermittlung personenbezogener Daten

### 1. Abschnitt
### Allgemeine Regelungen

Zu § 43, Allgemeine Regeln der Übermittlung personenbezogener Daten:

§ 43 entspricht in den Absätzen 1 bis 4 weitestgehend unverändert dem bisherigen § 32 SPolG (alt).
Absatz 5 verpflichtet zu Maßnahmen zur Sicherstellung der Datenqualität.
Absatz 6 regelt die Hinweis- und Mitteilungspflicht im Zusammenhang mit der Übermittlung personenbezogener Daten, die aufgrund besonderer Rechtsvorschriften verarbeitet werden.
Absatz 7 konkretisiert die Zweckbindung auch auf Seiten der Empfängerin oder des Empfängers personenbezogener Daten und verstärkt dies durch die bislang in § 3 Satz 2 der Verordnung über die Zulassung der Übermittlung personenbezogener Daten von der Polizei an ausländische Polizeibehörden (InfÜVPol) enthaltene Mitteilungspflicht. Die Verordnung wird in Gänze durch Artikel 3 dieses Gesetzes mit der Folge aufgehoben, dass auch diese Datenübermittlung im SPolDVG zu regeln ist. Neu hinzu kommt die Hinweispflicht der datenempfangenden Stelle auf den Berichtigungsbedarf. Dies folgt der Vorgabe des Artikels 16 Absatz 5 der Richtlinie.
Absatz 8 greift ebenfalls die Mitteilungspflicht des Absatzes 7 auf und erweitert diese auf die Fälle der bereits übermittelten personenbezogenen Daten, bei denen im Nachhinein festgestellt wurde, dass sie unrichtig oder nach § 26 Absatz 2 Satz 1 Nummer 1 zu löschen sind.
Absatz 9 ist neu und wurde insoweit unverändert als allgemeiner Grundsatz aus § 3 Satz 1 InfÜVPol übernommen.
Absatz 10 entspricht § 32 Absatz 7 SPolG (alt).

Zu § 44, Übermittlung personenbezogener Daten zwischen Polizeibehörden:

§ 44 stellt eine Hybridregelung aus dem bisherigen § 33 Absatz 1 SPolG (alt) und § 1 Absatz 1 Satz 2 InfÜVPol dar, wobei Satz 1 und 2 unter Anpassung des Verweises dem bisherigen § 33 Absatz 1 SPolG entsprechen.
Satz 3 enthält den Regelungsgedanken des bisherigen § 1 Absatz 1 Satz 2 InfÜVPol.

Zu § 45, Übermittlung personenbezogener Daten an Behörden, öffentliche oder sonstige Stellen:

Die Vorschrift entspricht im Wesentlichen dem bisherigen § 34 Absatz 1 SPolG. Sie berücksichtigt den Sonderfall, dass andere als originäre Polizeibehörden für die Gefahrenabwehr zuständig und somit nicht vom Anwendungsbereich des § 44 erfasst sind.

Durch Satz 1 wird auch die Datenübermittlung an diese Behörden oder Stellen geregelt.
Satz 2 präzisiert im Vergleich zu § 34 Absatz 1 Satz 2 SPolG die Voraussetzungen, unter denen personenbezogene Daten an sonstige Behörden, öffentliche oder nicht öffentliche Stellen oder Personen übermitteln darf.
Infolge der Aufhebung der InfÜVPol durch Artikel 3 dieses Gesetzes sowie der Umsetzung der Richtlinie erfolgt im 2. und 3. Abschnitt dieses Gesetzes die Neuregelung des bisherigen § 34 Absatz 2, Datenübermittlung an ausländische öffentliche oder zwischenstaatliche Stellen.

Zu § 46, Automatisiertes Abrufverfahren und Datenverbund:

§ 46 Absatz 1 entspricht weitgehend dem bisherigen § 35 SPolG Absatz 1. Absatz 1 Satz 2 erhält in Erweiterung dessen den ergänzenden Hinweis, dass die Verantwortlichen und die Abrufberechtigungen ebenfalls festzulegen sind. Satz 3 und 4 übernehmen den Regelungsgehalt des bisherigen Absatzes 3, wobei Satz 4 über den Verweis auf § 59 eindeutig herausstellt, dass die oder der Landesbeauftragte vor Einrichtung eines solchen Verfahrens anzuhören und nach dessen Einrichtung zu unterrichten ist.
Absatz 2 ersetzt den § 35 Absatz 2 SPolG und transformiert den der Regelungsintention nicht mehr entsprechenden Begriff des automatisierten Abrufverfahrens in den des Datenverbundes und schafft so eine den technischen Anforderungen folgende Rechtsgrundlage für einen qualitativ erhöhten, auch außerhalb des polizeilichen Informationsverbundes im Sinne des BKAG stattfindenden Informationsaustausch zwischen den genannten Polizeibehörden. Der grenzüberschreitende Datenaustausch ist beschränkt auf die in § 48 genannten Stellen: Polizeibehörden und sonstige öffentliche Stellen der Mitgliedstaaten der Europäischen Union, der Staaten, in denen der Schengen-Besitzstand angewandt wird, oder der Europäischen Union. Der Einhaltung des in § 48 Absatz 1 genannten Dienstweges bedarf es im Falle der Vereinbarung eines Datenverbundes nicht.

## 2. Abschnitt
## Grenzüberschreitender Datenverkehr innerhalb der Europäischen Union

Zu § 47, Verarbeitung personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union übermittelt worden sind:

Bislang war die Verarbeitung personenbezogener Daten, die im Rahmen der der Zusammenarbeit mit den Mitgliedstaaten der Europäischen Union übermittelt wurden, in § 34a SPolG geregelt. Diese Vorschrift wird in § 47 überführt, wobei der Wortlaut des Absatzes 1 wegen der Aufhebung des Rahmenbeschluss 2008/977/JI angepasst wurde.
Der bisherige § 34 Absatz 2 SPolG (alt) kann aufgrund der ohnehin normierten Zweckbindung entfallen, ebenso Absatz 3 der Vorschrift, da die darin enthaltene Vorgabe zur Kennzeichnungspflicht durch § 22 generell vorgeschrieben wird.

Zu § 48, Datenübermittlung an Polizeibehörden und öffentliche Stellen der Europäischen Union, der Mitgliedstaaten und der assoziierten Staaten:

Die Vorschrift entspricht § 1 InfÜVPol. Der in Absatz 1 aufgenommene Hinweis auf §§ 44 bis 46 als allgemeine Übermittlungsvoraussetzung verdeutlicht, dass die Datenübermittlung im Schengen-Raum generell unter denselben Voraussetzungen zulässig ist wie die inländische. Daher kann die Aufzählung im bisherigen § 1 Satz 2 InfÜVPol entfallen.

## 3. Abschnitt
## Datenübermittlungen an Drittstaaten und an internationale Organisationen

Zu § 49, Allgemeine Voraussetzungen:

Die Vorschrift setzt Artikel 35 der Richtlinie um und orientiert sich inhaltlich an § 78 BDSG 2018.
Absatz 1 regelt die generellen Voraussetzungen für die Übermittlung personenbezogener Daten an öffentliche Stellen in Drittländern oder an internationale Organisationen, soweit diese nicht von den Regelungen der §§ 47 und 48 umfasst sind. Der Begriff der internationalen Organisationen ist bewusst offen formuliert. Nach Gablers Wirtschaftslexikon handelt es sich dabei um „…Auf Dauer angelegte funktionale Zweckverbindungen von Staaten mit eigenen Organen, deren Einrichtung auf völkerrechtliche Verträge zwischen Staaten oder privatrechtliche Vereinbarungen zurückgeht, wobei (in weiter Auslegung) auch die Rechtsform von nationalen Vereinen mit internationaler Mitgliedschaft möglich ist. Eine allg. anerkannte Definition der internationalen Organisationen gibt es bisher nicht."
Auch die Richtlinie schweigt sich, ebenso wie der Bundesgesetzgeber, über die Reichweite des Begriffs aus. Aus dem Regelungskontext des Absatzes 1 ergibt sich jedoch, dass nicht öffentliche internationale Organisationen als Datenempfänger ausgeschlossen sind. Für diese wird mit § 52 eine Sonderregelung geschaffen.
Absatz 2 reflektiert die Anforderungen des Bundesverfassungsgerichts im BKAG-Urteil an die Datenübermittlung an Stellen in Drittstaaten oder an internationale Organisationen. Daher ist die Übermittlung unzulässig, wenn im Einzelfall Anlass zur Besorgnis besteht und diese Besorgnis auch nach einer Prüfung durch Vollzugspolizei nicht positiv ausgeräumt ist. Bei der Beurteilung der Zulässigkeit ist insbesondere zu berücksichtigen, ob der Empfänger einen angemessenen Schutz der Daten garantiert. Bei der Beurteilung der Zuverlässigkeit des Empfängers ist auch das tatsächliche Rechtsstaatlichkeitsniveau im Empfängerland mit einzubeziehen.
Absatz 3 regelt den Umgang mit personenbezogenen Daten, die durch eine in § 47 Absatz 1 und 4 genannte Stelle an die Vollzugspolizei übermittelt wurde. Dabei stellt die Regelung darauf ab, dass eine Übermittlung dieser Daten mindestens den gleichen rechtlichen Anforderungen unterliegt. Die Übermittlung an nicht öffentliche Stellen ist nur unter den in § 47 Absatz 3 genannten Voraussetzungen zulässig.
Absatz 4 regelt die Voraussetzungen, unter denen die Weiterübermittlung personenbezogener Daten durch die in Absatz 1 genannten Stellen zulässig ist.

Zu § 50, Datenübermittlung bei geeigneten Garantien:

§ 50 setzt Artikel 37 der Richtlinie um und ist inhaltlich an § 79 BDSG 2018 ausgerichtet. Dabei werden in enger Anlehnung an den Richtlinientext die Voraussetzungen normiert, unter denen eine Datenübermittlung in Drittstaaten zulässig ist, obwohl kein Angemessenheitsbeschluss nach Artikel 36 vorliegt.
Zulässig ist dies nur, wenn nach Absatz 1 Nummer 1 geeignete Garantien für den Schutz personenbezogener Daten durch ein Rechtsinstrument, dies kann eine gesetzliche Regelung oder ein Vertrag sein, vorgesehen sind oder nach Nummer 2 die Vollzugspolizei zu der Auffassung gelangt, dass solche Garantien bestehen. Dabei müssen die die Auffassung begründenden Tatsachen objektiv ausgeschlossen sein. Die Regelung des § 49 Absatz 2 entfaltet bei der Entscheidung über eine Übermittlung nach § 50 Absatz 1 ebenfalls Wirkung.
Absatz 2 regelt die Dokumentationsverpflichtung der Vollzugspolizei und setzt so Artikel 37 Absatz 3 der Richtlinie um.
Absatz 3 regelt die Unterrichtung der oder des Landesbeauftragten für Datenschutz und dient der Umsetzung von Artikel 37 Absatz 2 der Richtlinie.

Zu § 51, Datenübermittlung ohne geeignete Garantien:

§ 51 setzt Artikel 38 der Richtlinie unter Aufgreifen des Wortlauts des § 80 BDSG 2018 um. Dabei werden die in der Praxis seltenen Konstellationen geregelt, unter denen die saarländische Vollzugspolizei personenbezogene Daten in Drittländer übermitteln darf, ohne dass die Voraussetzungen der §§ 49 oder 50 vorliegen.

Zu § 52, Sonstige Datenübermittlung an Empfänger in Drittstaaten:

Die Vorschrift dient der Umsetzung von Artikel 39 der Richtlinie und gibt ebenso wie die §§ 49 bis 51 weitestgehend den Wortlaut der Korrespondenzvorschrift des BDSG 2018, hier § 81, wieder.
Abweichend von den §§ 49 bis 51 regelt § 52 die Übermittlung personenbezogener Daten an öffentliche Stellen, die keine Aufgaben nach § 49 Absatz 1 Satz 1 Nummer 1 erfüllen, und an nicht-öffentliche Stellen. Damit eröffnet die Vorschrift die Möglichkeit, Ersuchen an Finanzinstitutionen oder Telekommunikationsdienstleister in Drittstaaten zu richten, wobei der Umfang der zu übermittelnden personenbezogenen Daten in der Regel auf die zur Identifikation der betroffenen Personen erforderlichen Angaben zu beschränken ist.

## Fünfter Teil
## Besondere Regelungen für die Verarbeitung personenbezogener Daten und die Auftragsverarbeitung

### 1. Abschnitt
### Allgemeine Vorschriften

Zu § 53, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen:

§ 53 setzt Artikel 20 der Richtlinie um und stützt sich dabei auf den Wortlaut des § 71 BDSG 2018. Die Vorschrift macht verbindliche Vorgaben an eine datenschutzfreundliche Gestaltung von Datenverarbeitungssystemen (Privacy by Design) und die Implementierung datenschutzfreundlicher Grundeinstellungen oder Voreinstellungen. Letzter Begriff wird infolge der Umsetzung der Richtlinie neu in das nationale Datenschutzrecht eingeführt und ist unter Zugrundelegung des Erwägungsgrundes 53 so zu verstehen, dass die Polizei nach einer Datenschutz-Folgenabschätzung gemäß der Richtlinie die jeweiligen Ergebnisse bei der Entwicklung von Schutzmaßnahmen berücksichtigt. Nach Erwägungsgrund 53 können solche Maßnahmen oder Voreinstellungen u. a. aus einer möglichst frühen Pseudonymisierung bestehen. Dabei sollte der Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen.
Absatz 2 Satz 1 und 2 regelt die bereits bekannte Forderung nach Datensparsamkeit bei der Verarbeitung, letztlich ein Ausfluss des Erforderlichkeitsprinzips. Satz 3 gibt verbindlich vor, dass die automatisierte umfassende Zugänglichmachung personenbezogener Daten einen bestimmbaren Empfängerkreis voraussetzt. Dies ist in § 46 Absatz 1 Satz 2 entsprechend geregelt.

Zu § 54, Gemeinsam Verantwortliche:

Die Vorschrift setzt Artikel 21 der Richtlinie um und greift den Wortlaut des § 63 BDSG 2018 auf. Sie regelt die nähere Ausgestaltung der Verantwortlichkeiten bei einer kooperativen Verarbeitung personenbezogener Daten.

Zu § 55, Durchführung einer Datenschutz-Folgenabschätzung:

§ 55 dient der Umsetzung von Artikel 27 der Richtlinie und orientiert sich an § 67 BDSG 2018, wobei Absatz 3 dieser Vorschrift als Satz 2 in Absatz 1 einfließt. Da Artikel 27 der Richtlinie keine näheren Vorgaben an die Datenschutz-Folgenabschätzung enthält, greift § 55 - ebenso wie § 67 BDSG 2018 - die Regelungen des Artikels 35 der DSGVO auf.
Generell tritt die Datenschutz-Folgenabschätzung an die Stelle der bisherigen Vorabkontrolle nach § 11 Absatz 1 SDSG (alt).

Zu § 56, Zusammenarbeit mit der oder dem Landesbeauftragten für Datenschutz:

Die Vorschrift regelt die Umsetzung von Artikel 26 der Richtlinie und normiert die Verpflichtung zur Kooperation mit der oder dem Landesbeauftragten für Datenschutz. Der Wortlaut adaptiert § 68 BDSG 2018.

## 2. Abschnitt
## Auftragsverarbeitung

Zu § 57, Auftragsverarbeitung:

§ 57 setzt Artikel 22 der Richtlinie um und greift dabei den Wortlaut des § 62 BDSG 2018 auf. Bislang war die Auftragsdatenverarbeitung in § 5 SDSG (alt) normiert. Der Grundzweck der bisherigen Norm lag in der Festlegung der Kautelen für eine Verarbeitung personenbezogener Daten außerhalb des direkten tatsächlichen Einwirkungsbereichs des Verantwortlichen. Der darin enthaltene Regelungsansatz, wonach es für die Weitergabe personenbezogener Daten an den Auftragsverarbeiter keiner gesonderten Rechtsgrundlage bedarf, wird beibehalten.
Absatz 1 greift die Regelung des § 5 Absatz 1 SDSG (alt) auf.
Absatz 2 setzt Artikel 22 Absatz 1 der Richtlinie um.
Absatz 3 setzt Artikel 22 Absatz 2 der Richtlinie um. Darin werden die Anforderungen an eine zulässige Vergabe von Unterauftragsverarbeitungsverhältnissen normiert.
Absatz 4 regelt detailliert die Anforderungen an Unterauftragsverhältnisse in Anlehnung an die Vorgaben des Artikels 28 Absatz 4 der DSGVO.
Absatz 5 regelt die Inhalte eines Auftragsverarbeitungvertrags. Die Vorschrift greift die Regelungsgedanken aus § 5 Absatz 1 Satz 2ff. SDSG (alt), Artikel 22 Absatz 3 der Richtlinie und Artikel 28 Absatz 3 der DSGVO auf.
Absatz 6 setzt Artikel 22 Absatz 4 der Richtlinie der Richtlinie um und gibt die zulässigen Formen der Vereinbarung abschließend vor.
Absatz 7 dient der Umsetzung von Artikel 22 Absatz 5 der Richtlinie.
Absatz 8 greift die Regelung des § 5 Absatz 3 Satz 1 und 2 SDSG (alt) auf. Satz 3 dient der erleichterten Umsetzung eventueller Ansprüche der Auftragsgeberin im Falle von Verstößen gegen vertragliche Vereinbarungen oder sonstigen Zuwiderhandlungen, etwa gegen Vorschriften zum Schutz personenbezogener Daten. Satz 4 beschränkt die Vergabe von Datenverarbeitungsaufträgen an Auftragsnehmer, die ihren Sitz in einem Mitgliedstaat oder einem Schengen-assoziierten Staat haben.

## 3. Abschnitt
## Sicherheit und Schutz personenbezogener Daten

Zu § 58, Anforderungen an die Sicherheit der Verarbeitung personenbezogener Daten:

§ 58 setzt in Anlehnung an den Wortlaut des § 64 BDSG 2018 Artikel 29 der Richtlinie um. Dabei wird der Regelungsgedanken des § 11 SDSG (alt), insbesondere des Absatzes 2, aufgegriffen, indem der Verantwortliche dazu verpflichtet wird, erforderliche technisch-organisatorische Maßnahmen zum Schutz personenbezogener Daten zu treffen. Der wesentliche Unterschied zu der bisherigen Regelung besteht in der weitergehenden Detaillierung.

Zu § 59, Anhörung der oder des Landesbeauftragten für Datenschutz:

§ 59 dient der Umsetzung von Artikel 28 der Richtlinie und orientiert sich inhaltlich an § 69 BDSG 2018. Materiell wird die Regelung des § 7 SDSG (alt), insbesondere des Absatzes 2, weiterentwickelt. Wie bisher dient die Anhörung der oder des Landesbeauftragten für Datenschutz der Entdeckung besonderer Gefahrenpotentiale beim Einsatz neuer Verfahren beziehungsweise Dateisystemen.
Abweichend von § 69 Absatz 1 BDSG 2018 enthält Absatz 1 Satz 3 eine an den bisherigen § 7 Absatz 2 Satz 2 SDSG (alt) angelehnte Regelung, wobei sich die Beteiligung der zuständigen obersten Landesbehörden auf die reine Information beschränkt. Die sich aus der Rechts- und Fachaufsicht ergebenden Befugnisse bleiben unberührt.
Der bislang auf die Verfahrensbeschreibung beschränkte Umfang von Informationen, die der oder dem Landesbeauftragten für Datenschutz vorzulegen waren, wird ausgeweitet, wobei sich Absatz 2 auf die Vorgaben des Artikel 28 Absatz 4 der Richtlinie und Artikel 36 Absatz 3 der DSGVO, respektive § 69 Absatz 2 BDSG 2018, stützt.
Nach Absatz 3 in Verbindung mit Absatz 1 Satz 1 ist mit der Inbetriebnahme neuer Dateisysteme zuzuwarten, bis das Anhörungsverfahren abgeschlossen ist.
Absatz 4 enthält eine Eilfallregelung, welche es in Abwägung mit polizeifachlichen Erfordernissen zulässt, hiervon abzuweichen und neue Dateisysteme im Vorgriff auf die abschließenden Empfehlungen der oder des Landesbeauftragten für Datenschutz einzusetzen. Das zwingende Prüferfordernis im Hinblick auf die Empfehlungen der oder des Landesbeauftragten für Datenschutz entfällt dadurch nicht.

Zu § 60, Freigabe:

§ 15 SDSG (neu) sieht eine Freigabe für automatisierte Verfahren zur Verarbeitung personenbezogener Daten im Anwendungsbereich der Richtlinie nicht mehr vor. Um den Gedanken aus § 7 Absatz 2 SDSG (alt) weiter zu führen, bedarf es daher einer eigenständigen Regelung. § 60 normiert sowohl die Freigabe selbst als auch deren Umfang. Abweichend von der bisherigen Rechtslage erfolgt die Freigabe durch den Verantwortlichen.
Nach Absatz 2 bedarf es für die dort aufgeführten Kategorien von Verfahren keiner Freigabe. Hierbei handelt es sich um solche, von denen keine oder nur geringe Gefahren für die jeweils Betroffenen ausgehen.

Zu § 61, Verzeichnis von Verarbeitungstätigkeiten:

Die Vorschrift setzt Artikel 24 der Richtlinie um und stellt dabei auf den Wortlaut des § 70 BDSG 2018 ab. Das hier geregelte Verzeichnis entspricht intentionell dem durch den Datenschutzbeauftragten nach § 8 Absatz 2 Nummer 1 in Verbindung mit § 9 Absatz 1 SDSG (alt) bisher zu führenden Verfahrensverzeichnis.
Absatz 1 Satz normiert die Angaben, die zwingend in das durch den Verantwortlichen zu führende Verzeichnis aufzunehmen sind.

Absatz 2 enthält entsprechende Vorgaben für den Auftragsverarbeiter, wenngleich in geringerem Umfang, was wiederum den Vorgaben des Artikels 24 Absatz 2 der Richtlinie geschuldet ist.
Absatz 3 gibt die Form der Verzeichnisse vor. Satz 2 stellt eine saarländische Spezialität dar, welche die Kontrolltätigkeit erleichtern soll. Die Vorschrift richtet sich auch an Auftragsverarbeiter.
Absatz 4 regelt, dass das Verzeichnis und seine Aktualisierungen der oder dem Landesbeauftragten für Datenschutz auf Anfrage zur Verfügung gestellt werden muss.

Zu § 62, Meldung von Verletzungen des Schutzes personenbezogener Daten an die oder den Landesbeauftragten für Datenschutz:

§ 62 dient der Umsetzung von Artikel 30 der Richtlinie und legt den Umfang und das Verfahren der verbindlich vorgeschriebenen Meldung an die oder den Landesbeauftragten für Datenschutz fest. Der Wortlaut orientiert sich an § 65 Absatz 1 bis 6 BDSG 2018
Absatz 3 Satz 1 verpflichtet - insoweit abweichend von § 65 Absatz 3 Satz 1 BDSG 2018 - auch den Auftragsverarbeiter um Mitteilung der in Absatz 3 genannten Angaben. Durch die in § 57 Absatz 8 geforderte Unterwerfungserklärung sind die Absätze 2 und 3 direkt auf Auftragsnehmer anwendbar.

Zu § 63, Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten:

§ 63 setzt Artikel 31 der Richtlinie um. Die Vorschrift ergänzt die Benachrichtigungspflichten des § 10 um die Fallkonstellationen, in denen der Schutz personenbezogener Daten verletzt wurde.
Absatz 1 regelt den Grundsatz, wonach bei erheblichen Gefahren für die Rechtsgüter Betroffener immer und unverzüglich eine Benachrichtigung zu erfolgen hat.
Absatz 2 regelt Art und Mindestumfang der Benachrichtigung.
Absatz 3 enthält enumerativ und abschließend eine Aufzählung der Ausnahmetatbestände von Absatz 1.
Absatz 4 verweist auf die besondere Beurteilungskompetenz der oder des Landesbeauftragten für Datenschutz im Falle der unterbliebenen Benachrichtigung.
Absatz 5 regelt die partielle Anwendbarkeit des § 10 zwecks Aufschiebung, Einschränkung oder Unterlassung der Benachrichtigung.

Zu § 64, Vertrauliche Meldung von Verstößen:

§ 64 setzt Artikel 48 der Richtlinie um; der Wortlaut entspricht § 77 BDSG 2018. Der Verantwortliche hat im Zusammenhang mit der Meldung von Verstößen sowohl interne Meldungen als auch Hinweise der betroffenen Person oder Dritter zu berücksichtigen.

## Sechster Teil
## Schlussvorschriften

Zu § 65, Ordnungswidrigkeiten und Straftaten:

§ 65 setzt Artikel 57 der Richtlinie um, der Wortlaut ist an § 42 BDSG 2018 angelehnt.
Absatz 1 regelt dabei durch die Richtlinie zwar nicht vorgesehenen jedoch auch nicht ausgeschlossenen Ordnungswidrigkeiten; Absätze 2 und 3 regeln die jeweiligen Straftatbestände und die Strafandrohungen.
Nach Absatz 4 Satz 1 stellen die in Absatz 2 und Absatz 3 geregelten Vergehen absolute Antragsdelikte dar; die Antragsberechtigung ist in Satz 2 geregelt.

Absatz 5 dient dem verfassungsrechtlichen garantierten Schutz vor einer Selbstbezichtigung und schützt neben dem Verpflichteten auch dessen in § 52 StPO genannten Angehörigen.

Zu § 66, Berichtspflichten der Landesregierung:

§ 66 greift die bislang in den §§ 28a, b SPolG (alte Fassung) geregelten Berichtspflichten der Landesregierung auf, fasst diese in einer Vorschrift zusammen und erweitert sie auf alle verdeckten oder eingriffsintensiven Maßnahmen sowie auf alle Übermittlungen an Drittstaaten und internationale Organisationen.

Zu § 67, Inkrafttreten:

Die Vorschrift regelt das Inkrafttreten.

**Zu Artikel 3 – Aufhebung der Verordnung über die Zulassung der Übermittlung personenbezogener Daten von der Polizei an ausländische Polizeibehörden**

Durch die Neuregelung der gesamten polizeilichen Datenverarbeitung wird die Übermittlung personenbezogener Daten künftig in einem Parlamentsgesetz geregelt. Daher wird die Verordnung über die Zulassung der Übermittlung personenbezogener Daten von der Polizei an ausländische Polizeibehörden vom 4. Dezember 1996 überflüssig und ist daher aufzuheben.

**Zu Artikel 4 – Einschränkung von Grundrechten**

Artikel 4 trägt dem Zitiergebot Rechnung und nennt die durch dieses Gesetz eingeschränkten Grundrechte.

**Zu Artikel 5 – Übergangsvorschriften**

Absatz 1 räumt der Vollzugspolizei die Möglichkeit ein, von dem in § 22 Absatz 2 SPolDVG normierten Verarbeitungsverbot nicht gekennzeichneter personenbezogener Daten abzuweichen. Damit wird der Erfordernis Rechnung getragen, dass die Informationstechnik der Vollzugspolizei nur sukzessive weiterentwickelt bzw. ersetzt werden kann. Die Regelung unter Nummer 1 orientiert sich an § 91 des Bundeskriminalamtgesetzes.
Auf diese Weise kann die Verarbeitung personenbezogener Daten durch die Vollzugspolizei für eine Übergangsfrist ohne wesentliche Einschränkungen aufrechterhalten werden, auch wenn in den etablierten Dateisystemen keine entsprechende Kennzeichnung gemäß § 22 Absatz 1 SPolDVG technisch möglich ist. In solchen Fällen ist für die Verarbeitung und Übermittlung die Errichtungsanordnung nach § 39 Absatz 2 SPolG (alt) maßgeblich, die für das jeweilige personenbezogene Datum am Inkrafttreten des SPolDVG gilt.
Die Vorschrift bezieht sich sowohl auf „echte Altdaten“, also jene, die bereits vor Inkrafttreten dieses Gesetzes erhoben und gespeichert wurden, als auch auf solche, die nach dem Inkrafttreten dieses Gesetzes erhoben, aber in Dateien und Dateisystem auf Basis des § 39 Absatz 2 SPolG (alt) gespeichert werden. Ein nicht gekennzeichnetes Zuspeichern ist demzufolge ohne die Folge des Datenverwendungsverbotes nach § 22 Absatz 2 SPolDVG möglich. Der Altdatenbestand wird sich aufgrund von Löschfristen und –pflichten von selbst erledigen. Es gibt keine Pflicht zur Nachkennzeichnung. Zu beachten ist, dass Artikel 5 Absatz 1 zeitlich unbefristet ist und die Verarbeitungs- und Übermittlungsbefugnis auf Basis der Errichtungsanordnung nach § 39 Absatz 2 SPolG (alt) so lange gilt, bis eine vollständige technische Kennzeichnung nach § 22 Absatz 1 SPolDVG möglich ist.

Zu beachten ist die Doppelfunktionalität dieser Vorschrift, der nicht nur die Wirkung des § 22 Absatz 1 SPolDVG aussetzt, sondern die Datenverarbeitung ausdrücklich und zusätzlich im Rahmen der bisherigen Errichtungsanordnungen für zulässig erklärt. Solange die Datennutzung im Rahmen der in der Errichtungsanordnung niedergelegten Zwecke erfolgt, ist keine Zweckänderung anzunehmen. Vielmehr richtet sich die Verarbeitung dieser Daten nach den Regeln der jeweiligen Errichtungsanordnung. Im Falle wesentlicher Änderungen der Errichtungsanordnung oder der Überleitung in neue Verfahren tritt die Rechtsfolge des § 22 Absatz 1 ein.
Nicht umfasst von Artikel 5 Absatz 1 Nummer 1 sind die Fälle, in denen Daten nach Inkrafttreten dieses Gesetzes erhoben werden und diese nicht in Dateien bzw. Dateisystemen auf Basis des § 39 Absatz 2 SPolG (alt) gespeichert werden. In diesen Fällen greift das Verwendungsverbot und eine Nutzung von nicht gekennzeichneten Fällen ist nach § 22 Absatz 2 SPolDVG grundsätzlich ausgeschlossen. Da allerdings nicht zu erwarten ist, dass eine vollständige technische Umsetzung nach § 22 Absatz 1 SPolDVG in den Dateisystemen der Vollzugspolizei aufgrund des erheblichen technischen Aufwandes nicht kurzfristig zu realisieren sein wird, wurde die Vollzugspolizei mit der Regelung in § 23 Absatz 10 SPolDVG verpflichtet, bei der Verarbeitung von personenbezogenen Daten durch technische und organisatorische Vorkehrungen und Maßnahmen sicherzustellen, dass Voraussetzungen der hypothetischen Datenneuerhebung zumindest in hohem Maße beachtet werden. Sobald aber Kennzeichnungen technisch möglich sind, greift das Datenverwendungsverbot bei Unterlassen der Pflicht in vollem Umfang.
Absatz 1 Nummer 2 regelt verschiedene weitere Ausnahmen von Kennzeichnungspflicht:
Buchstabe a) regelt mit der ersten Alternative die tatsächliche Unmöglichkeit einer Kennzeichnung etwa, wenn nicht bekannt oder feststellbar ist, woher die Daten stammen oder zu welchem Zweck sie ursprünglich erhoben wurden. Diese dürfen weiter gespeichert werden, soweit nicht die Löschverpflichtung des § 26 Absatz 2 einschlägig wird. Der Fall dürfte in der Praxis regelmäßig dann eintreten, wenn der ursprüngliche Zweck der Datenspeicherung nicht mehr bekannt ist.
Der Fall der technischen Unmöglichkeit als zweite Alternative. Die Regelung betrifft überwiegend solche Auswertemöglichkeiten, die neu geschaffen werden und sich als Datenquellen bereits eingeführter Verfahren und aus deren Datenbeständen bedienen. Soweit diese „Altbestände weder gekennzeichnet noch kennzeichnungsfähig sind, dürfen die Daten weiterhin verarbeitet werden.
Die Regelung unter Buchstabe b) wiederum suspendiert die Kennzeichnungspflicht bei einem damit verbundenen unverhältnismäßigen Aufwand. Der entstehende Aufwand ist jedoch ins Verhältnis zu der Belastung der davon betroffenen Personen zu setzen. Je schwerwiegender der Eingriff, desto stärker überwiegt deren Interesse an einer Löschung ihrer Daten.

Absatz 2 übernimmt die in Artikel 63 Absatz 2 der Richtlinie eingeräumte Übergangsfrist für die in Artikel 25 der Richtlinie geforderte Verarbeitung von Protokolldaten. Erst mit der Einführung neuer Dateisysteme wird es technisch möglich sein, die gesetzlich vorgegebenen Protokolldaten vollumfänglich zu verarbeiten. Solche abweichenden Übergangsregelungen sind nur unter Beteiligung des Ministeriums für Inneres, Bauen und Sport sowie der oder des Landesbeauftragten für Datenschutz möglich.
Absatz 3 regelt das Außerkrafttreten der unter Absatz 1 Nummer 3 und 4 genannten Ausnahmeregelungen. Spätestens zu diesem Zeitpunkt sollten eventuelle alte Datenbestände gekennzeichnet sein und alle neuen gekennzeichnet werden.

**Zu Artikel 6 – Inkrafttreten**

Die Vorschrift regelt das Inkrafttreten.