

GESETZENTWURF

der Regierung des Saarlandes

betr.: Gesetz zum Erlass des Saarländischen Justizvollzugsdatenschutzgesetzes, zur Änderung des Saarländischen Strafvollzugsgesetzes, zur Änderung des Saarländischen Jugendstrafvollzugsgesetzes, zur Änderung des Saarländischen Untersuchungshaftvollzugsgesetzes, zur Änderung des Gesetzes zur ambulanten Resozialisierung und Opferhilfe und zur Änderung des Gesetzes über den Verfassungsgerichtshof

A. Problem und Ziel

Zu Artikel 1:

Das Europäische Parlament und der Rat der Europäischen Union haben am 27. April 2016 zwei Regelwerke zum Schutz bei der Verarbeitung personenbezogener Daten erlassen:

Einerseits die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119 vom 4. Mai 2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23. 5. 2018, S. 2) (Datenschutz-Grundverordnung) und andererseits die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4. Mai 2016, S. 89; L 127 vom 23.5.2018, S. 9) (Richtlinie (EU) 2016/680).

Das vorliegende Gesetz dient der Umsetzung der Richtlinie (EU) 2016/680. Diese findet auch auf den Straf-, Jugendstraf-, Untersuchungshaftvollzug, die Unterbringung in der Sicherungsverwahrung und den Jugendarrestvollzug Anwendung.

Zu Artikel 2:

Das Gesetz modifiziert die bisherigen Regelungen zu den besonderen Sicherungsmaßnahmen im Strafvollzugsgesetz. Es berücksichtigt dabei die im Urteil des Bundesverfassungsgerichts vom 24. Juli 2018 - 2 BvR 309/15, 2 BvR 502/16 - festgelegten verfassungsrechtlichen Anforderungen an die Fixierung von Patienten in der öffentlich-rechtlichen Unterbringung. Diese Entscheidung bezieht sich zwar nicht auf das Saarland und nicht unmittelbar auf den Strafvollzug, gibt aber Veranlassung, die Bestimmungen für die Fixierung von Gefangenen zu präzisieren, da auch im Strafvollzug Fixierungen zur Anwendung kommen.

Ausgegeben:

In der Vollzugspraxis hat sich herausgestellt, dass es sinnvoll ist, den Gefangenen eine strukturierte Möglichkeit zum freiwilligen und pfändungsgeschützten Ansparen von Geld für die Entlassungsvorbereitung und die Zeit nach der Entlassung zu geben. Diese Strukturen sollen geschaffen werden.

Zu Artikel 3:

Das Gesetz modifiziert die bisherigen Regelungen zu den besonderen Sicherungsmaßnahmen im Jugendstrafvollzugsgesetz. Es berücksichtigt dabei die im Urteil des Bundesverfassungsgerichts vom 24. Juli 2018 - 2 BvR 309/15, 2 BvR 502/16 - festgelegten verfassungsrechtlichen Anforderungen an die Fixierung von Patienten in der öffentlich-rechtlichen Unterbringung. Diese Entscheidung bezieht sich zwar nicht auf das Saarland und nicht unmittelbar auf den Jugendstrafvollzug, gibt aber Veranlassung, die Bestimmungen für die Fixierung von Gefangenen zu präzisieren, da auch im Jugendstrafvollzug Fixierungen zur Anwendung kommen.

In der Vollzugspraxis hat sich herausgestellt, dass es sinnvoll ist, den Gefangenen eine strukturierte Möglichkeit zum freiwilligen und pfändungsgeschützten Ansparen von Geld für die Entlassungsvorbereitung und die Zeit nach der Entlassung zu geben. Diese Strukturen sollen geschaffen werden.

Zu Artikel 4:

Das Gesetz modifiziert die bisherigen Regelungen zu den besonderen Sicherungsmaßnahmen im Untersuchungshaftvollzugsgesetz. Es berücksichtigt dabei die im Urteil des Bundesverfassungsgerichts vom 24. Juli 2018 - 2 BvR 309/15, 2 BvR 502/16 - festgelegten verfassungsrechtlichen Anforderungen an die Fixierung von Patienten in der öffentlich-rechtlichen Unterbringung. Diese Entscheidung bezieht sich zwar nicht auf das Saarland und nicht unmittelbar auf den Untersuchungshaftvollzug, gibt aber Veranlassung, die Bestimmungen für die Fixierung von Untersuchungsgefangenen zu präzisieren, da auch im Untersuchungshaftvollzug Fixierungen zur Anwendung kommen.

Zu Artikel 5:

Das Gesetz zur ambulanten Resozialisierung und Opferhilfe ist teilweise ebenfalls von der Richtlinie (EU) 2016/680 betroffen und wird entsprechend angepasst.

Zu Artikel 6:

Das Gesetz über den Verfassungsgerichtshof wird bereichsspezifisch fortentwickelt mit der Zielsetzung, die Regelungen zur gerichtlichen Gewährung von Akteneinsicht an zwischenzeitliche Rechtsänderungen anzupassen und eine flexiblere Gestaltung der Richterwahl in Bezug auf die Besetzung des Gerichts mit Berufsrichterinnen und Berufsrichtern zu eröffnen.

B. Lösung

Zu Artikel 1:

Die Umsetzung der europäischen Vorgaben in das bereichsspezifische Recht des Datenschutzes im Justizvollzug des Saarlandes sieht das vorliegende Justizvollzugsdatenschutzgesetz vor. Das Gesetz beabsichtigt eine weitgehende Vollregelung des für den Justizvollzug geltenden Datenschutzrechts.

Mit dem vorgelegten Gesetz werden die bisherigen datenschutzrechtlichen Standards in den einzelnen saarländischen Vollzugsgesetzen in ein neues eigenständiges Justizvollzugsdatenschutzgesetz überführt und zugleich die Vorgaben der Richtlinie (EU) 2016/680 in Landesrecht umgesetzt. Dadurch wird dem hohen Stellenwert des Datenschutzes im Justizvollzug Rechnung getragen und das eigenständige Gesetz macht die komplexe Materie des Datenschutzes anwendungsfreundlicher.

Zu Artikel 2:

Es werden die Vorgaben des Urteils des Bundesverfassungsgerichts vom 24. Juli 2018 - 2 BvR 309/15, 2 BvR 502/16 – durch die Einführung eines Richtervorbehaltes bei Fixierungen im Strafvollzug umgesetzt.

Es wird ein Eingliederungsgeld eingeführt. Hierbei soll es sich nicht um ein „Zwangsansparen“ wie beim ehemaligen Überbrückungsgeld gemäß § 51 Strafvollzugsgesetz handeln. Das Eingliederungsgeld soll in Eigenverantwortung der Gefangenen angespart werden.

Zu Artikel 3:

Es werden die Vorgaben des Urteils des Bundesverfassungsgerichts vom 24. Juli 2018 - 2 BvR 309/15, 2 BvR 502/16 – durch die Einführung eines Richtervorbehaltes bei Fixierungen im Jugendstrafvollzug umgesetzt.

Es wird ein Eingliederungsgeld eingeführt. Hierbei soll es sich nicht um ein „Zwangsansparen“ wie beim ehemaligen Überbrückungsgeld gemäß § 51 Strafvollzugsgesetz handeln. Das Eingliederungsgeld soll in Eigenverantwortung der Gefangenen angespart werden.

Zu Artikel 4:

Es werden die Vorgaben des Urteils des Bundesverfassungsgerichts vom 24. Juli 2018 - 2 BvR 309/15, 2 BvR 502/16 – durch die Einführung eines Richtervorbehaltes bei Fixierungen im Untersuchungshaftvollzug umgesetzt.

Zu Artikel 5:

Die bisherigen datenschutzrechtlichen Standards im Gesetz zur ambulanten Resozialisierung und Opferhilfe werden im bestehenden Gesetz an die Vorgaben der Richtlinie (EU) 2016/680 angepasst. Durch das einheitliche Gesetz bleibt die komplexe Materie der ambulanten Resozialisierung und Opferhilfe sowie des Datenschutzes für die betroffenen Mitarbeiter anwendungsfreundlicher.

Zu Artikel 6:

In Anlehnung an die einschlägigen Vorschriften des Bundesverfassungsgerichtsgesetzes ist eine entsprechende Anpassung der §§ 14a bis 14c des Gesetzes über den Verfassungsgerichtshof unter Beibehaltung der bisherigen Regulationsstruktur veranlasst. Des Weiteren wird im Interesse einer flexibleren Gestaltung der Richterwahl die Besetzungsregelung in § 2 Absatz 3 Satz 6 des Gesetzes dahingehend geändert, dass der dort vorgeschriebene Berufsrichteranteil nicht mehr an die Zugehörigkeit zu einem oberen Landesgericht geknüpft wird.

C. Alternativen

Keine.

D. Finanzielle Auswirkungen

1. Haushaltsausgaben ohne Vollzugaufwand

Keine.

2. Vollzugaufwand

Das Justizvollzugsdatenschutzgesetz und Artikel 2 - 5 werden zu einem erhöhten Verwaltungsaufwand führen, dessen Kosten jedoch nicht konkret bezifferbar sind. Anfallende Aufwendungen werden aus veranschlagten Haushaltsansätzen finanziert.

E. Sonstige Kosten

Die Pflicht zur Protokollierung von bestimmten Datenverarbeitungs-vorgängen in automatisierten Verarbeitungssystemen in § 42 Justizvollzugsdatenschutzgesetz erfordert eine ergänzende Programmierung des Datenverarbeitungssystems im Justizvollzug BASIS-Web. Das System wird in mehreren Bundesländern eingesetzt und von einem Entwicklerverbund betreut. Dieser ermittelt momentan den Umsetzungsaufwand der Protokollierungspflicht und die daraus resultierenden Kosten. § 42 Justizvollzugsdatenschutzgesetz tritt gemäß Artikel 7 erst am 6. Mai 2023 in Kraft. Vergleichbares gilt für § 32 d des Gesetzes zur ambulanten Resozialisierung und Opferhilfe und das Datenverarbeitungssystem SoPart, welches im Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe zum Einsatz kommt. Anfallende Aufwendungen werden aus veranschlagten Haushaltsansätzen finanziert.

F. Auswirkungen von frauenpolitischer Bedeutung

Keine.

G. Federführende Zuständigkeit

Ministerium der Justiz.

G e s e t z

**zum Erlass des Saarländischen Justizvollzugsdatenschutzgesetzes,
zur Änderung des Saarländischen Strafvollzugsgesetzes,
zur Änderung des Saarländischen Jugendstrafvollzugsgesetzes,
zur Änderung des Saarländischen Untersuchungshaftvollzugsgesetzes,
zur Änderung des Gesetzes zur ambulanten Resozialisierung und Opferhilfe und
zur Änderung des Gesetzes über den Verfassungsgerichtshof**

Der Landtag wolle beschließen:

Artikel 1

Saarländisches Justizvollzugsdatenschutzgesetz

Abschnitt 1

Allgemeine Bestimmungen

- § 1 Anwendungsbereich, Aufsichtsbehörde
- § 2 Begriffsbestimmungen
- § 3 Grundsätze der Datenverarbeitung
- § 4 Rechtmäßigkeit der Datenverarbeitung, Einwilligung
- § 5 Datengeheimnis

Abschnitt 2

Erhebung

- § 6 Rechtmäßigkeit der Datenerhebung
- § 7 Erhebung bei betroffenen Personen
- § 8 Erhebung von Daten über Gefangene bei Dritten
- § 9 Erhebung von Daten über Personen, die nicht Gefangene sind

Abschnitt 3

Speicherung und Nutzung, Aktenführung

- § 10 Speicherung und Nutzung
- § 11 Aktenführung

Abschnitt 4

Übermittlung

- § 12 Übermittlung an öffentliche und nichtöffentliche Stellen, Verfahren zur Feststellung von Vorinhaftierungen
- § 13 Sicherheitsrelevante Erkenntnisse
- § 14 Überprüfung Gefangener
- § 15 Überprüfung anstaltsfremder Personen
- § 16 Fallkonferenzen
- § 17 Weitere Zulässigkeitsvoraussetzungen für die Datenverarbeitung mit den Sicherheitsbehörden
- § 18 Verantwortung für die Datenübermittlung und Verfahren
- § 19 Förmliche Verpflichtung Dritter
- § 20 Mitteilung über Haftverhältnisse
- § 21 Aktenüberlassung
- § 22 Auskunft und Akteneinsicht für wissenschaftliche Zwecke
- § 23 Einsichtnahme in Gefangenenpersonalakten, Gesundheitsakten und Krankenblätter

Abschnitt 5**Besondere Formen der Datenverarbeitung**

- § 24 Datenverarbeitung im Auftrag
- § 25 Datenverarbeitung bei Übertragung von Vollzugsaufgaben
- § 26 Gemeinsame Verantwortung der Justizvollzugsbehörden
- § 27 Erkennungsdienstliche Maßnahmen
- § 28 Erkennungsdienstlicher Datenabgleich
- § 29 Einsatz optisch-elektronischer Einrichtungen und biometrischer Zu- und Ausgangskontrollen
- § 30 Optisch-elektronische Einrichtungen im Umfeld der Anstalt
- § 31 Optisch-elektronische Einrichtungen innerhalb der Anstalt
- § 32 Optisch-elektronische Einrichtungen innerhalb von Hafträumen und Zimmern
- § 33 Speicherung mittels optischer oder akustischer Einrichtungen erhobener Daten, Dokumentation
- § 34 Auslesen von Datenspeichern
- § 35 Identifikation anstaltsfremder Personen
- § 36 Lichtbildausweise

Abschnitt 6**Schutzanforderungen**

- § 37 Zweckbindung
- § 38 Schutzvorkehrungen
- § 39 Verzeichnis von Verarbeitungstätigkeiten
- § 40 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- § 41 Datenschutz-Folgenabschätzung bei hohem Risiko, Konsultationspflicht
- § 42 Protokollierung
- § 43 Kenntlichmachung innerhalb der Anstalt
- § 44 Erkenntnisse aus Beaufsichtigungs-, Überwachungs- und Kontrollmaßnahmen

Abschnitt 7**Besondere Bestimmungen für Geheimnisträgerinnen und Geheimnisträger**

- § 45 Geheimnisträgerinnen und Geheimnisträger
- § 46 Offenbarungspflicht
- § 47 Offenbarungsbefugnis
- § 48 Benachrichtigung der Gefangenen über Offenbarungen
- § 49 Zweckbindung offenbarter personenbezogener Daten, Zulassung von Offenbarungsempfängern
- § 50 Zugriff auf Daten in Notfällen

Abschnitt 8**Rechte der betroffenen Personen**

- § 51 Allgemeine Informationen zur Datenverarbeitung
- § 52 Aufklärungspflicht bei der Datenerhebung mit Kenntnis der betroffenen Personen
- § 53 Benachrichtigung bei Datenerhebung ohne Kenntnis der betroffenen Personen
- § 54 Auskunftsrecht der betroffenen Personen
- § 55 Akteneinsichtsrecht
- § 56 Auskunft und Akteneinsicht in Gesundheitsakten
- § 57 Sperrvermerke
- § 58 Verfahren für die Ausübung der Rechte der betroffenen Personen

Abschnitt 9

Löschung, Einschränkung der Verarbeitung und Berichtigung

§ 59 Löschung

§ 60 Einschränkung der Verarbeitung

§ 61 Berichtigung

§ 62 Rechte der betroffenen Personen auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

§ 63 Mitteilungen

Abschnitt 10

Anwendung weiterer Vorschriften

§ 64 Anwendung weiterer Vorschriften des allgemeinen Datenschutzrechts

Abschnitt 1 Allgemeine Bestimmungen

§ 1 Anwendungsbereich, Aufsichtsbehörde

(1) Dieses Gesetz regelt die Verarbeitung personenbezogener Daten durch Justizvollzugsbehörden im Vollzug von

1. Freiheitsstrafe, Jugendstrafe, Untersuchungshaft, Strafarrrest, Unterbringung in der Sicherungsverwahrung, Jugendarrest und
2. Haft nach § 127b Absatz 2, § 230 Absatz 2, §§ 236, 329 Absatz 3, § 412 Satz 1 und § 453c der Strafprozessordnung sowie der einstweiligen Unterbringung nach § 275a Absatz 6 Strafprozessordnung.

(2) Justizvollzugsbehörden sind Justizvollzugsanstalten, Jugendstrafanstalten, Jugendarrestanstalten und Einrichtungen für den Vollzug der Sicherungsverwahrung (Anstalten) sowie das für den Justizvollzug zuständige Ministerium (Aufsichtsbehörde).

(3) Die oder der Landesbeauftragte für Datenschutz ist Aufsichtsbehörde gemäß Artikel 41 der Richtlinie (EU) 2016/680 bei der Verarbeitung personenbezogener Daten nach diesem Gesetz. Die Justizvollzugsbehörden haben mit der oder dem Landesbeauftragten für Datenschutz bei der Erfüllung ihrer oder seiner Aufgaben zusammenzuarbeiten.

§ 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes sind:

1. „Gefangene“ Personen im Vollzug nach § 1 Absatz 1;
2. „vollzugliche Zwecke“
 - a) die Gefangenen zu befähigen, künftig in sozialer Verantwortung ein Leben ohne Straftaten zu führen,
 - b) die Allgemeinheit vor weiteren Straftaten der Gefangenen zu schützen,
 - c) Leib, Leben, Freiheit und Vermögen der Bediensteten und der Gefangenen sowie das Vermögen des Landes durch die Aufrechterhaltung der Sicherheit und Ordnung innerhalb der Anstalten zu schützen,
 - d) Entweichung und Befreiung von Gefangenen zu verhindern,
 - e) Nichtrückkehr und Missbrauch von Lockerungen zu vermeiden sowie
 - f) die Mitwirkung des Justizvollzugs an den ihm durch Gesetz übertragenen sonstigen Aufgaben, insbesondere an Gefangene betreffenden Entscheidungen der Strafvollstreckungskammern durch vorbereitende Stellungnahmen; an die Stelle des in Nummer 2 Buchstabe a) bestimmten Zwecks tritt für den Vollzug der Untersuchungshaft der Zweck, durch die sichere Unterbringung der Gefangenen die Durchführung eines geordneten Strafverfahrens zu gewährleisten;
3. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann;

4. „Verarbeitung“ jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie
 - a) das Erheben, das Erfassen, die Speicherung, die Veränderung, das Auslesen, das Abfragen, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, das Löschen, die Einschränkung oder die Vernichtung oder
 - b) die Organisation, das Ordnen, die Anpassung, die Verknüpfung oder sonstige Verwendung (Nutzung);
5. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;
6. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;
7. „Pseudonymisierung“ 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;
8. „Anonymisierung“ 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 bestimmbar natürlichen Person zugeordnet werden können;
9. „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;
10. „Verantwortlicher“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;
11. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
12. „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten 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;

13. „Verletzung des Schutzes personenbezogener Daten“ eine 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;
14. „besondere Kategorien personenbezogener Daten“
 - a) Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,
 - b) genetische Daten,
 - c) biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
 - d) Gesundheitsdaten und
 - e) Daten zum Sexualleben oder zur sexuellen Orientierung;
15. „genetische Daten“ 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;
16. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, insbesondere Gesichtsbilder oder daktyloskopische Daten;
17. „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;
18. „internationale Organisation“ eine 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;
19. „Einwilligung“ jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;
20. „anstaltsfremde Personen“ Personen, die zu den Justizvollzugsbehörden nicht in einem Dienst- oder Arbeitsverhältnis stehen und nicht im Auftrag einer anderen Behörde tätig sind oder nicht als Organ der Rechtspflege handeln;

21. „öffentliche Stellen“
- a) die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, der Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform,
 - b) die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes oder sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform und
 - c) die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Mitgliedstaates der Europäischen Union;
22. „nichtöffentliche Stellen“ natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter Nummer 21 fallen; nimmt eine nichtöffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

§ 3

Grundsätze der Datenverarbeitung

- (1) Die Justizvollzugsbehörden wahren das Recht einer jeden Person, grundsätzlich selbst über die Preisgabe und Verwendung ihrer personenbezogenen Daten zu bestimmen (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG) und deren Recht auf Schutz der sie betreffenden personenbezogenen Daten (Artikel 8 Absatz 1 Charta der Grundrechte der Europäischen Union).
- (2) Die Justizvollzugsbehörden sehen vor, dass personenbezogene Daten
- a) auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,
 - b) für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,
 - c) dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sind,
 - d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind; 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,
 - e) 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,
 - f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.
- (3) Bei der Verarbeitung personenbezogener Daten ist so weit wie möglich danach zu unterscheiden, ob diese auf Tatsachen oder auf persönlichen Einschätzungen beruhen.
- (4) Eine ausschließlich auf einer automatisierten Verarbeitung personenbezogener Daten beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffenen Personen verbunden ist oder sie erheblich beeinträchtigt, ist unzulässig. Profiling, das zur Folge hat, dass die betroffenen Personen auf der Grundlage von personenbezogenen Daten besonderer Kategorien diskriminiert werden, ist verboten.

§ 4**Rechtmäßigkeit der Datenverarbeitung, Einwilligung**

(1) Die Justizvollzugsbehörden dürfen personenbezogene Daten nur verarbeiten, wenn dieses Gesetz oder eine andere Rechtsvorschrift dies für den Anwendungsbereich dieses Gesetzes ausdrücklich erlaubt oder anordnet oder die betroffenen Personen eingewilligt haben und der Einwilligung ein gesetzliches Verbot nicht entgegensteht.

(2) Soweit die Verarbeitung personenbezogener Daten auf der Grundlage einer Einwilligung erfolgt, muss die Justizvollzugsbehörde die Einwilligung der betroffenen Personen nachweisen können.

(3) Erfolgt die Einwilligung der betroffenen Personen 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.

(4) Die betroffenen Personen haben das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffenen Personen sind vor Abgabe der Einwilligung hiervon in Kenntnis zu setzen.

(5) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Personen beruhen. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung, etwa die besondere Situation der Freiheitsentziehung, berücksichtigt werden. Die betroffenen Personen sind auf den Zweck der Verarbeitung hinzuweisen. Ist dies nach den Umständen des Einzelfalles erforderlich oder verlangen die betroffenen Personen dies, sind sie auch über die Folgen der Verweigerung der Einwilligung zu belehren.

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

(7) Bei beschränkt geschäftsfähigen Gefangenen bestimmt sich die Einwilligungsfähigkeit nach der tatsächlichen Einsichtsfähigkeit.

(8) Soweit Gefangene nicht die für eine Entscheidung notwendige Einsichtsfähigkeit besitzen und vollzugliche Zwecke nicht gefährdet werden, steht das ihnen nach diesem Gesetz zustehende Recht, informiert und gehört zu werden oder Fragen und Anträge zu stellen, ihren gesetzlichen Vertreterinnen und Vertretern zu. Sind mehrere Personen berechtigt, kann jeder von ihnen die in diesem Gesetz bestimmten Rechte allein ausüben. Sind Mitteilungen vorgeschrieben, genügt es, wenn sie an eine oder einen von ihnen gerichtet werden.

§ 5 Datengeheimnis

(1) Den in Justizvollzugsbehörden tätigen Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Personen, die nicht Amtsträger im Sinne des § 11 Absatz 1 Nummer 2 des Strafgesetzbuchs sind, sind vor der Aufnahme ihrer Tätigkeit über die zu beachtenden Bestimmungen zu unterrichten und auf deren Einhaltung förmlich gemäß § 1 des Verpflichtungsgesetzes vom 2. März 1974 (BGBl. I S. 469, 547), das durch § 1 Nummer 4 des Gesetzes vom 15. August 1974 (BGBl. I S. 1942) geändert worden ist, in der jeweils geltenden Fassung zu verpflichten.

(2) Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

Abschnitt 2 Erhebung

§ 6 Rechtmäßigkeit der Datenerhebung

(1) Die Justizvollzugsbehörden dürfen personenbezogene Daten erheben, soweit dies zu vollzuglichen Zwecken erforderlich ist.

(2) Besondere Kategorien personenbezogener Daten dürfen sie nur erheben, soweit dies zu vollzuglichen Zwecken unbedingt erforderlich ist.

§ 7 Erhebung bei betroffenen Personen

(1) Personenbezogene Daten sind grundsätzlich bei den betroffenen Personen und mit deren Kenntnis und deren Mitwirkung zu erheben.

(2) Eine Erhebung personenbezogener Daten bei den betroffenen Personen ohne deren Kenntnis und deren Mitwirkung ist zulässig, wenn keine Anhaltspunkte dafür vorliegen, dass überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen.

§ 8 Erhebung von Daten über Gefangene bei Dritten

(1) Soweit die Erhebung personenbezogener Daten über Gefangene nach § 6 und § 7 Absatz 2 zulässig ist, dürfen sie auch bei Dritten ohne Kenntnis und Mitwirkung der Gefangenen erhoben werden, wenn

1. dies zur Erreichung des Vollzugsziels oder zur Abwehr einer drohenden Gefahr für die Sicherheit der Anstalt erforderlich ist,
2. eine Rechtsvorschrift dies ausdrücklich erlaubt oder anordnet,
3. Angaben der betroffenen Personen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
4. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist,
5. dies zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist,

6. sich die Erhebung auf Daten aus Akten der gerichtlichen Verfahren bezieht, die der Vollstreckung der gegenwärtigen Freiheitsentziehung zugrunde liegen oder diese Freiheitsentziehung sonst betreffen,
7. die betroffenen Personen einer durch Rechtsvorschrift festgelegten Auskunftspflicht nicht nachgekommen und über die beabsichtigte Erhebung bei Dritten unterrichtet worden sind,
8. die Erhebung bei den betroffenen Personen einen unverhältnismäßigen Aufwand erfordern würde oder
9. die Daten allgemein zugänglich sind.

(2) Soweit die Erhebung personenbezogener Daten über Gefangene nach §§ 6 und 7 Absatz 2 zulässig ist und diese nicht die für eine Einwilligung notwendige Einsichtsfähigkeit besitzen, dürfen personenbezogene Daten auch bei deren gesetzlichen Vertreterinnen und Vertretern erhoben werden.

(3) Werden personenbezogene Daten bei nichtöffentlichen Stellen auf Grund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, ist der Dritte auf die Auskunftspflicht und sonst auf die Freiwilligkeit seiner Angaben hinzuweisen.

§ 9

Erhebung von Daten über Personen, die nicht Gefangene sind

Daten über Personen, die nicht Gefangene sind, können ohne deren Kenntnis und Mitwirkung bei Gefangenen oder sonstigen Dritten erhoben werden, soweit dies zu vollzuglichen Zwecken unbedingt erforderlich ist und schutzwürdige Interessen der betroffenen Personen hierdurch nicht beeinträchtigt werden.

Abschnitt 3

Speicherung und Nutzung, Aktenführung

§ 10

Speicherung und Nutzung

(1) Die Justizvollzugsbehörden dürfen personenbezogene Daten, die sie zulässig erhoben haben, speichern und nutzen, soweit dies zur Aufgabenerfüllung erforderlich ist. Die Daten dürfen nur für Zwecke verarbeitet werden, für die sie erhoben worden sind; zu anderen vollzuglichen Zwecken nur, soweit dies erforderlich und verhältnismäßig ist.

(2) Die Justizvollzugsbehörden dürfen personenbezogene Daten, die sie zulässig erhoben haben, zu anderen nicht-vollzuglichen Zwecken speichern und nutzen, soweit

1. dies erforderlich ist zur Abwehr von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten für eine fremde Macht oder von Bestrebungen in der Bundesrepublik Deutschland, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen
 - a) gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind,
 - b) eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben oder
 - c) auswärtige Belange der Bundesrepublik Deutschland gefährden,
2. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit erforderlich ist,
3. dies zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist,

4. dies zur Verhinderung oder Verfolgung von Straftaten, zur Vollstreckung von Strafen und Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs sowie zur Verhinderung oder Verfolgung von Ordnungswidrigkeiten, durch welche die Sicherheit oder Ordnung der Anstalt gefährdet werden, erforderlich ist oder
5. dies für Maßnahmen der Strafvollstreckung oder strafvollstreckungsrechtliche Entscheidungen hinsichtlich der betroffenen Personen erforderlich ist.

Eine Verarbeitung für andere Zwecke liegt nicht vor, soweit sie dem gerichtlichen Rechtsschutz im Zusammenhang mit diesem Gesetz oder den Vollzugsgesetzen, der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen dient.

(3) Das Speichern oder Nutzen von zulässig erhobenen besonderen Kategorien personenbezogener Daten für Zwecke, zu denen sie nicht erhoben wurden, ist nur zulässig, soweit dies zu den in Absatz 2 genannten Zwecken unbedingt erforderlich ist. Soweit die erhobenen besonderen Kategorien personenbezogener Daten einem Amts- oder Berufsgeheimnis unterliegen und von den zur Verschwiegenheit Verpflichteten in Ausübung ihrer Amts- oder Berufspflicht erlangt wurden, dürfen sie, soweit dieses Gesetz nichts anderes bestimmt, nur für den Zweck gespeichert oder genutzt werden, für den die zur Verschwiegenheit Verpflichteten sie erhalten haben.

(4) Personenbezogene Daten, die nach § 9 über Personen, die nicht Gefangene sind, erhoben wurden, dürfen nur unter den Voraussetzungen des Absatzes 1 oder des Absatzes 2, unter den Voraussetzungen des § 16 oder zur Verhinderung oder Verfolgung von Straftaten von erheblicher Bedeutung gespeichert und genutzt werden.

(5) Sind mit personenbezogenen Daten, die nach Absatz 1 oder Absatz 2 verarbeitet werden dürfen, weitere personenbezogene Daten von betroffenen Personen oder von Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unververtretbarem Aufwand möglich ist, ist die Speicherung auch dieser Daten zulässig, soweit nicht berechnete Interessen von betroffenen Personen oder Dritten an deren Geheimhaltung offensichtlich überwiegen. Eine Nutzung dieser Daten ist unzulässig.

(6) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert oder genutzt werden, dürfen für andere Zwecke nur insoweit genutzt werden, als dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit, insbesondere für Leben, Gesundheit oder Freiheit, sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist. Für die weitere Verarbeitung von Protokolldaten gilt ausschließlich § 42 Absatz 3.

§ 11 Aktenführung

(1) Über Gefangene werden Gefangenenpersonalakten und Gesundheitsakten geführt.

(2) Die Justizvollzugsbehörden können Akten auch elektronisch führen. Das für den Justizvollzug zuständige Ministerium wird ermächtigt, Regelungen für die elektronische Führung von Akten durch Rechtsverordnung zu treffen.

Abschnitt 4 Übermittlung

§ 12

Übermittlung an öffentliche und nichtöffentliche Stellen, Verfahren zur Feststellung von Vorinhaftierungen

(1) Die Justizvollzugsbehörden dürfen personenbezogene Daten, die sie zulässig erhoben haben, übermitteln, soweit dies zur Erfüllung der mit der Erhebung verfolgten vollzuglichen Zwecke erforderlich ist. Für andere vollzugliche Zwecke ist eine Übermittlung zulässig, soweit dies erforderlich und verhältnismäßig ist.

(2) Nichtöffentlichen Stellen dürfen die Justizvollzugsbehörden zulässig erhobene personenbezogene Daten für Zwecke, zu denen sie erhoben wurden, übermitteln, soweit

1. sich die Justizvollzugsbehörden zur Erreichung einzelner vollzuglicher Zwecke in zulässiger Weise der Mitwirkung nichtöffentlicher Stellen bedienen und diese Mitwirkung ohne die Verarbeitung der durch Justizvollzugsbehörden übermittelten personenbezogenen Daten unmöglich oder wesentlich erschwert wäre und
2. es dazu erforderlich ist, Gefangenen insbesondere
 - a) den Besuch von Behandlungs-, Beratungs-, Trainings- und Bildungsmaßnahmen sowie die Beschäftigung innerhalb und außerhalb von Anstalten,
 - b) die Inanspruchnahme von Leistungen der Berufsheimnisträgerinnen und Berufsheimnisträger (§ 45 Absatz 2) und deren Hilfspersonen,
 - c) den Einkauf oder
 - d) die Inanspruchnahme von Telekommunikations- und Mediendienstleistungen,
 - e) die Inanspruchnahme von Maßnahmen der Entlassungsvorbereitung, des Übergangs in die Freiheit, der Schuldenregulierung, der Entlassung, der Wiedereingliederung, der nachgehenden Betreuung oder des freiwilligen Verbleibs zu ermöglichen.

(3) Zuständigen öffentlichen Stellen dürfen die Justizvollzugsbehörden zulässig erhobene personenbezogene Daten für nicht-vollzugliche Zwecke übermitteln, soweit

1. eine andere gesetzliche Bestimmung dies für den Anwendungsbereich dieses Gesetzes ausdrücklich erlaubt oder anordnet oder
2. dies erforderlich ist für
 - a) die Erfüllung der Aufgaben der Gerichtshilfe, Jugendgerichtshilfe, Nachsorge, Bewährungshilfe, Führungsaufsicht oder der forensischen Ambulanzen,
 - b) Entscheidungen in Gnadensachen,
 - c) gesetzlich angeordnete Statistiken der Rechtspflege,
 - d) die Erfüllung von Aufgaben, die den für Sozialleistungen zuständigen Leistungsträgern durch Rechtsvorschrift übertragen worden sind,
 - e) die Einleitung von Hilfsmaßnahmen für Angehörige (§ 11 Absatz 1 Nummer 1 des Strafgesetzbuches) der Gefangenen,
 - f) dienstliche Maßnahmen der Bundeswehr im Zusammenhang mit der Aufnahme und Entlassung von Soldatinnen und Soldaten,
 - g) asyl- oder ausländerrechtliche Maßnahmen,
 - h) die Erfüllung der Aufgaben der Jugendämter,
 - i) die Durchführung der Besteuerung oder
 - j) die Erreichung der in § 10 Absatz 2 oder § 16 genannten Zwecke.

(4) Im Vollzug der Untersuchungshaft und der Freiheitsentziehungen nach 0 Absatz 1 Nummer 2 unterbleiben Übermittlungen nach Absatz 3 Nummer 2, wenn die Gefangenen unter Berücksichtigung der Art der Information und ihrer Rechtsstellung ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben.

(5) Nichtöffentlichen Stellen dürfen die Justizvollzugsbehörden zulässig erhobene personenbezogene Daten für Zwecke, zu denen sie nicht erhoben wurden, ohne Einwilligung der betroffenen Personen nur unter den Voraussetzungen des § 10 Absatz 2 Nummer 1 bis 5 übermitteln.

(6) Die Übermittlung von zulässig erhobenen besonderen Kategorien personenbezogener Daten darf

1. an öffentliche Stellen nur unter den Voraussetzungen des § 10 Absatz 3, § 16 und des § 28,
2. an nichtöffentliche Stellen nur unter den Voraussetzungen, dass dies unbedingt erforderlich ist und
 - a) eine Rechtsvorschrift, dies für den Anwendungsbereich dieses Gesetzes ausdrücklich erlaubt oder anordnet,
 - b) dies der Erreichung vollzuglicher Zwecke dient,
 - c) dies auch unter Berücksichtigung der Interessen der Gefangenen an der Geheimhaltung der personenbezogenen Daten
 - aa) der Abwehr einer Gefahr für das Leben eines Menschen, insbesondere zur Verhütung von Selbsttötungen,
 - bb) der Abwehr einer erheblichen Gefahr für die Gesundheit oder anderer lebenswichtiger Interessen eines Menschen oder
 - cc) der Abwehr der Gefahr erheblicher Straftaten, dient,
 - d) dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder sonst unmittelbar drohender Gefahren für die öffentliche Sicherheit erforderlich ist,
 - e) die Daten von den betroffenen Personen offenkundig öffentlich gemacht wurden.
3. an forensische Ambulanzen und Nachsorgeeinrichtungen zum Zweck von Behandlungsmaßnahmen, der Entlassungsvorbereitung und der Nachsorge, soweit dies unbedingt erforderlich ist, erfolgen.

(7) Personenbezogene Daten, die nach § 9 über Personen, die nicht Gefangene sind, erhoben wurden, dürfen nur unter den Voraussetzungen des Absatzes 1 oder für die in § 10 Absatz 2 oder § 16 aufgeführten Zwecke sowie zur Verhinderung oder Verfolgung von Straftaten von erheblicher Bedeutung übermittelt werden. Sie dürfen auch übermittelt werden, soweit dies für Zwecke der Fahndung und Festnahme der entwichenen oder sich sonst ohne Erlaubnis außerhalb der Anstalt aufhaltenden Gefangenen erforderlich ist.

(8) Sind mit personenbezogenen Daten, die nach den Absätzen 1, 3 oder 4 übermittelt werden dürfen, weitere personenbezogene Daten von betroffenen Personen oder von Dritten in Akten so verbunden, dass eine Trennung, Anonymisierung oder Pseudonymisierung nicht oder nur mit unververtretbarem Aufwand möglich ist, ist die Übermittlung auch dieser Daten zulässig, soweit nicht schutzwürdige Interessen von betroffenen Personen oder Dritten an deren Geheimhaltung offensichtlich überwiegen. Soweit es sich um besondere Kategorien personenbezogener Daten handelt, ist regelmäßig von einem überwiegenden berechtigten Interesse der betroffenen Personen auszugehen. Eine Speicherung, Nutzung und Übermittlung dieser Daten durch den Empfänger ist unzulässig.

(9) Soweit nichts anderes bestimmt ist, unterbleibt die Übermittlung personenbezogener Daten, die

1. den Justizvollzugsbehörden durch Geheimnisträgerinnen und Geheimnisträger im Sinne des § 45 Absatz 1 bekannt wurden oder
2. in ihrer Verarbeitung eingeschränkt oder unrichtig sind.

(10) Zur Feststellung von Vorinhaftierungen und sicherheitsrelevanten Erkenntnissen aus Vorinhaftierungen darf für die Erhebung und Übermittlung personenbezogener Daten gemäß § 14 Absatz 3 ein automatisiertes Verfahren zwischen den Justizvollzugsbehörden eingerichtet werden. Das automatisierte Verfahren darf auch die Angabe umfassen, ob aus der Vorinhaftierung sicherheitsrelevante Erkenntnisse vorliegen.

§ 13

Sicherheitsrelevante Erkenntnisse

(1) Zum Zwecke der Aufrechterhaltung der Sicherheit der Anstalt prüfen die Justizvollzugsbehörden nach Maßgabe der §§ 14 und 15, ob sicherheitsrelevante Erkenntnisse über Gefangene und anstaltsfremde Personen, die Zugang zu den Anstalten begehren, vorliegen.

(2) Sicherheitsrelevant sind Erkenntnisse insbesondere über extremistische, gewaltorientierte Einstellungen oder Kontakte zu derartigen Organisationen, Gruppierungen oder Personen oder Kontakte zur organisierten Kriminalität. Wirken anstaltsfremde Personen an der Eingliederung von Gefangenen mit, können über Satz 1 hinaus auch Erkenntnisse über erhebliche strafrechtliche Verurteilungen, eine bestehende Suchtproblematik oder andere für die Beurteilung der Zuverlässigkeit erhebliche Umstände sicherheitsrelevant sein.

§ 14

Überprüfung Gefangener

(1) Bestehen tatsächliche Anhaltspunkte für eine in einem überschaubaren Zeitraum drohende, einer oder einem Gefangenen zurechenbare Gefahr für die Sicherheit der Anstalt, dürfen die Justizvollzugsbehörden Justiz- und Sicherheitsbehörden um Auskunft ersuchen. Insbesondere dürfen sie dazu

1. eine Auskunft nach § 41 Absatz 1 Nummer 1 des Bundeszentralregistergesetzes in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 I S. 195), das zuletzt durch Gesetz vom 18. Juli 2017 (BGBl. I S. 2732) geändert worden ist, in der jeweils geltenden Fassung einholen,
2. sicherheitsrelevante Erkenntnisse der Polizeibehörden des Bundes und der Länder anfragen und,
3. soweit im Einzelfall erforderlich, sicherheitsrelevante Erkenntnisse des Landesamts für Verfassungsschutz anfragen.

Tatsächliche Anhaltspunkte für eine in einem überschaubaren Zeitraum drohende, den Gefangenen zurechenbare Gefahr können sich insbesondere aus deren Verurteilungen oder deren Verhalten im Vollzug ergeben.

(2) Die Anfrage nach Absatz 1 Satz 2 Nummer 2 erstreckt sich nur auf die personenbezogenen Hinweise und die Erkenntnisse des polizeilichen Staatsschutzes. Bei der Anfrage nach Absatz 1 Satz 2 Nummer 3 erfolgt die Anfrage des nachrichtendienstlichen Informationssystems durch das Landesamt für Verfassungsschutz.

(3) Die Justizvollzugsbehörden übermitteln den angefragten Behörden soweit möglich den Nachnamen, Geburtsnamen, die Vornamen, das Geburtsdatum, das Geschlecht, den Geburtsort, das Geburtsland und die Staatsangehörigkeit der Gefangenen. Über Satz 1 hinaus sollen bekannt gewordene Aliaspersonalien, die voraussichtliche Vollzugsdauer sowie das Aktenzeichen der der Vollstreckung zugrunde liegenden Entscheidung mitgeteilt werden.

(4) Die gemäß Absatz 1 Satz 1 und Satz 2 Nummer 2 und 3 angefragten Behörden teilen den Justizvollzugsbehörden die sicherheitsrelevanten Erkenntnisse über die Gefangenen mit.

(5) Bestehen auf Grund der übermittelten sicherheitsrelevanten Erkenntnisse tatsächliche Anhaltspunkte für eine Gefahr der Sicherheit der Anstalt, dürfen die Justizvollzugsbehörden zusätzliche Auskünfte oder Unterlagen bei Justiz- und Sicherheitsbehörden, einholen.

(6) Im Rahmen der Anfrage mitgeteilte sicherheitsrelevante Erkenntnisse sind in gesonderten Akten oder Dateisystemen zu führen.

(7) Die Verarbeitungs- und Übermittlungsbefugnis für personenbezogene Daten über Gefangene zur Aufrechterhaltung der Sicherheit der Anstalt schließt die Verarbeitungsbefugnis zum Zwecke der Vollzugs- und Eingliederungsplanung der Gefangenen ein.

§ 15

Überprüfung anstaltsfremder Personen

(1) Anstaltsfremde Personen, die in der Anstalt tätig werden sollen, dürfen zu diesen Tätigkeiten nur zugelassen werden, wenn keine Sicherheitsbedenken bestehen. Die Justizvollzugsbehörden sollen zur Aufrechterhaltung der Sicherheit der Anstalt mit vorherigem Einverständnis dieser betroffenen Personen eine Zuverlässigkeitsüberprüfung vornehmen. Insbesondere dürfen sie dazu

1. eine Auskunft nach § 41 Absatz 1 Nummer 1 des Bundeszentralregistergesetzes einholen,
2. sicherheitsrelevante Erkenntnisse der Polizeibehörden des Bundes und der Länder anfragen und,
3. soweit im Einzelfall erforderlich, sicherheitsrelevante Erkenntnisse des Landesamts für Verfassungsschutz anfragen.

Ist eine Überprüfung in Eilfällen, insbesondere bei kurzfristig notwendigen Reparaturarbeiten, nicht möglich, soll eine Beaufsichtigung der Personen bei deren Tätigkeit in der Anstalt erfolgen.

(2) Die Justizvollzugsbehörden sollen von einer Anfrage nach Absatz 1 Satz 3 absehen, wenn aufgrund des Anlasses, der Art, des Umfangs oder der Dauer des Aufenthalts oder der Tätigkeit in der Anstalt eine Gefährdung der Sicherheit der Anstalt fernliegt.

(3) Darüber hinaus dürfen die Justizvollzugsbehörden bei tatsächlichen Anhaltspunkten einer drohenden Gefahr für die Sicherheit der Anstalt auch bei Personen, die die Zulassung zum Besuch von Gefangenen oder zum Besuch der Anstalt begehren, hierfür mit ihrem vorherigen Einverständnis eine Zuverlässigkeitsüberprüfung vornehmen. Absatz 1 Satz 3 gilt entsprechend. In den Fällen des Absatz 1 Satz 3 Nummer 2 und 3 teilen die Justizvollzugsbehörden auch mit, ob und für welche Gefangenen die Zulassung zum Besuch begehrt wird.

(4) Absatz 3 gilt nicht für Besuche von Verteidigerinnen und Verteidigern und Beiständen sowie für Rechtsanwältinnen, Rechtsanwälte sowie Notarinnen und Notare in einer die Gefangenen betreffenden Rechtssache sowie für die im Rahmen der Überwachung des Schriftwechsels der Gefangenen gesetzlich privilegierten Personen und Stellen.

(5) Werden den Justizvollzugsbehörden sicherheitsrelevante Erkenntnisse bekannt, sollen die anstaltsfremden Personen nicht oder nur unter Beschränkungen zu der Tätigkeit oder dem Besuch zugelassen werden. Gleiches gilt, wenn die betroffenen Personen eine Einwilligung in eine Zuverlässigkeitsüberprüfung verweigert.

(6) Eine erneute Zuverlässigkeitsüberprüfung soll erfolgen, wenn neue sicherheitsrelevante Erkenntnisse nach § 13 Absatz 2 vorliegen, spätestens jedoch nach Ablauf von fünf Jahren, sofern ihre Erforderlichkeit nach Absatz 1 Satz 1 und 2 und Absatz 3 weiter besteht.

§ 16

Fallkonferenzen

(1) Im Rahmen von Fallkonferenzen dürfen die Justizvollzugsbehörden personenbezogene Daten, einschließlich solcher besonderer Kategorien, die sie zulässig erhoben haben, insbesondere den voraussichtlichen Entlassungszeitpunkt, die voraussichtliche Entlassungsadresse sowie die Vollzugs- und Eingliederungspläne, den Polizeibehörden des Bundes und der Länder übermitteln, sofern

1. tatsächliche Anhaltspunkte für die fortdauernde Gefährlichkeit von Gefangenen für die Allgemeinheit vorliegen,
2. die Entlassung von Gefangenen aller Voraussicht nach in einem Zeitraum von nicht mehr als einem Jahr bevorsteht und
3. dies zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist.

Fallkonferenzen dürfen auch zur Vorbereitung von Ausführungen, Vorführungen, Ausantwortungen, Überstellungen und Verlegungen bei tatsächlichen Anhaltspunkten für eine Gefahr der Entweichung, von Gewalttätigkeiten gegen Personen oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, und der Selbstverletzung oder Selbsttötung von Gefangenen stattfinden. An den Fallkonferenzen nach Satz 1 sollen die Nachsorge, die Bewährungshilfe und die Führungsaufsichtsstellen beteiligt werden. Im Zuge der Fallkonferenzen nach den Sätzen 1 und 2 dürfen die Justizvollzugsbehörden personenbezogene Daten, einschließlich solcher besonderer Kategorien, bei den Polizeibehörden auch abfragen und erheben.

(2) Im Rahmen von Fallkonferenzen dürfen die Justizvollzugsbehörden personenbezogene Daten, einschließlich solcher besonderer Kategorien, die sie zulässig erhoben haben, insbesondere den voraussichtlichen Entlassungszeitpunkt, die voraussichtliche Entlassungsadresse sowie die Vollzugs- und Eingliederungspläne den Verfassungsschutzbehörden des Bundes und der Länder übermitteln, sofern

1. bestimmte Tatsachen den Verdacht von Tätigkeiten oder Bestrebungen nach § 10 Absatz 2 Nummer 1 begründen,
2. eine damit im Zusammenhang stehende Gefahr für die Sicherheit der Anstalt oder die Erreichung des Vollzugsziels in einem überschaubaren Zeitraum einzutreten droht und
3. dies zur Verhütung der in Nummer 2 genannten Gefahren unbedingt erforderlich ist.

An den Fallkonferenzen sollen die Nachsorge, die Bewährungshilfe und die Führungsaufsichtsstellen beteiligt werden, sofern die Entlassung der Gefangenen in voraussichtlich nicht mehr als einem Jahr bevorsteht. Im Zuge dieser Fallkonferenzen dürfen die Justizvollzugsbehörden personenbezogene Daten, einschließlich solcher besonde-

rer Kategorien, bei den Verfassungsschutzbehörden des Bundes und der Länder auch abfragen und erheben.

(3) Fallkonferenzen dürfen zwischen den Justizvollzugsbehörden, den Polizeibehörden des Bundes und der Länder und den Verfassungsschutzbehörden des Bundes und der Länder stattfinden, sofern

1. bestimmte Tatsachen die Annahme einer gegenwärtigen Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, begründen,
2. bestimmte Tatsachen den Verdacht von Tätigkeiten oder Bestrebungen nach § 10 Absatz 2 Nummer 1 begründen und
3. dies zur Abwehr der in Nummer 1 genannten Gefahren unbedingt erforderlich ist.

Absatz 2 Satz 2 gilt entsprechend. Im Zuge dieser Fallkonferenzen dürfen die Justizvollzugsbehörden personenbezogene Daten, einschließlich solcher besonderer Kategorien, bei den Polizeibehörden des Bundes und der Länder sowie den Verfassungsschutzbehörden des Bundes und der Länder auch abfragen und erheben.

(4) Die wesentlichen Ergebnisse der stattgefundenen Fallkonferenzen sind zu dokumentieren.

(5) Die Vollzugs- und Eingliederungsplanung bleibt den Justizvollzugsbehörden vorbehalten.

§ 17

Weitere Zulässigkeitsvoraussetzungen für die Datenverarbeitung mit den Sicherheitsbehörden

(1) Die Übermittlung personenbezogener Daten an Sicherheitsbehörden zum Zwecke der Gefahrenverhütung, zum Zwecke der Gefahrenabwehr, zur Verhinderung oder Verfolgung von Straftaten, zur Verhinderung oder Verfolgung von Ordnungswidrigkeiten oder zu den in § 10 Absatz 2 Nummer 1 genannten Zwecken ist nur zulässig, wenn 1. sich im Einzelfall konkrete Ansätze ergeben

- a) zur Verhütung, Aufdeckung oder Verfolgung der Straftaten oder Ordnungswidrigkeiten oder
 - b) zur Abwehr von in einem überschaubaren Zeitraum drohenden Gefahren
- und

2. mindestens

- a) der Schutz solch bedeutsamer Rechtsgüter oder
- b) die Verhütung, Aufdeckung oder Verfolgung solch schwerwiegender Straftaten oder Ordnungswidrigkeiten verwirklicht werden soll, dass ein im Vergleich zur Datenerhebung gleichwertiger Rechtsgüterschutz sichergestellt ist.

(2) Absatz 1 gilt für die Erhebung von personenbezogenen Daten über Gefangene, anstaltsfremde oder sonstige Personen durch die Justizvollzugsbehörden bei den Sicherheitsbehörden zum Zwecke der Gefahrenverhütung, zum Zwecke der Gefahrenabwehr, zur Verhinderung oder Verfolgung von Straftaten oder zur Verhinderung oder Verfolgung von Ordnungswidrigkeiten entsprechend.

(3) Für die Übermittlung und Erhebung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen oder verdeckten Eingriff in informationstechnische Systeme erlangt wurden, gilt Absatz 1 Nummer 1 Buchstabe b mit der Maßgabe entsprechend, dass 1. bei personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen erlangt wurden, im Einzelfall eine dringende Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes für Leib,

Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, vorliegen muss und 2. bei personenbezogenen Daten, die durch einen verdeckten Eingriff in informationstechnische Systeme erlangt wurden, im Einzelfall bestimmte Tatsachen jedenfalls die Annahme rechtfertigen, dass innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Schädigung von Leib, Leben oder Freiheit einer Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt, eintritt.

(4) Die Befugnis zum erkenntnisdienlichen Datenabgleich zum Zwecke der Identifikation von Gefangenen (§ 28) und anstaltsfremden Personen (§ 35 Absatz 4) bleibt hiervon unberührt.

§ 18

Verantwortung für die Datenübermittlung und Verfahren

(1) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Justizvollzugsbehörde.

(2) Erfolgt die Übermittlung auf Ersuchen einer öffentlichen Stelle, trägt diese die Verantwortung. In diesem Fall prüfen die Justizvollzugsbehörden nur, ob das Ersuchen im Rahmen der Aufgaben der empfangenden öffentlichen Stelle liegt und dieses Gesetz der Übermittlung nicht entgegensteht, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht.

(3) Soll die Übermittlung auf Ersuchen einer nichtöffentlichen Stelle erfolgen, hat diese die hierfür erforderlichen Angaben zu machen, insbesondere die Rechtsgrundlage für die Übermittlung anzugeben.

(4) Soweit dies mit angemessenem Aufwand möglich ist, sind die personenbezogenen Daten vor ihrer Übermittlung auf Richtigkeit, Vollständigkeit und Aktualität zu überprüfen.

(5) Bei der Übermittlung personenbezogener Daten zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit werden nach Möglichkeit die erforderlichen Informationen beigefügt, die es den empfangenden öffentlichen Stellen ermöglichen, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der personenbezogenen Daten sowie deren Aktualitätsgrad zu beurteilen.

(6) Personenbezogene Daten, die an nichtöffentliche Stellen übermittelt werden sollen, sind vor der Übermittlung zu pseudonymisieren, soweit nicht der Personenbezug für die Erfüllung des Übermittlungszweckes erforderlich ist. Dabei ist die Gefangenenbuchungsnummer als Pseudonym zu verwenden, wenn nicht besondere Gründe entgegenstehen.

§ 19

Förmliche Verpflichtung Dritter

(1) Personen, die für eine nichtöffentliche Stelle Kenntnis von personenbezogenen Daten erlangen sollen, die von Justizvollzugsbehörden übermittelt wurden, sind vor Aufnahme ihrer Tätigkeit gemäß § 1 des Verpflichtungsgesetzes in der jeweils geltenden Fassung förmlich zu verpflichten.

(2) Personen, die nicht nach Absatz 1 förmlich verpflichtet wurden, dürfen von personenbezogenen Daten nur Kenntnis erlangen, wenn 1. die übermittelten Daten vor ihrer Übermittlung pseudonymisiert wurden, 2. die förmliche Verpflichtung vor Kenntniserlangung Leib oder Leben eines Menschen oder bedeutende Sachwerte gefährden würde und die Verpflichtung veranlasst und unverzüglich nachgeholt wird; erfolgt die Übermittlung der Daten nicht durch die Justizvollzugsbehörden, sind sie unverzüglich unter Angabe der Personalien der Kenntniserlangenden von der Übermittlung zu unterrichten oder 3. sie Amtsträger im Sinne des § 11 Absatz 1 Nummer 2 des Strafgesetzbuchs sind.

(3) Die Justizvollzugsbehörden stellen auf geeignete Weise sicher, dass bei nichtöffentlichen Stellen nur solche Personen Kenntnis von übermittelten personenbezogenen Daten erlangen, die zuvor nach Absatz 1 verpflichtet wurden oder die nach Absatz 2 auch ohne förmliche Verpflichtung Kenntnis von übermittelten personenbezogenen Daten erlangen dürfen.

§ 20

Mitteilung über Haftverhältnisse

(1) Die Justizvollzugsbehörden dürfen auf schriftlichen Antrag mitteilen, ob und gegebenenfalls in welcher Anstalt sich eine Person in Haft befindet, ob ihre Entlassung voraussichtlich innerhalb eines Jahres bevorsteht sowie, falls die Entlassung innerhalb eines Jahres bevorsteht, den vorgesehenen Entlassungstermin, soweit

1. die Mitteilung zur Erfüllung der in der Zuständigkeit der anfragenden öffentlichen Stelle liegenden Aufgaben erforderlich ist oder
2. von nichtöffentlichen Stellen ein berechtigtes Interesse an dieser Mitteilung glaubhaft dargelegt wird und die betroffenen Gefangenen kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben.

(2) Verletzten einer Straftat sowie deren Rechtsnachfolgerinnen und Rechtsnachfolgern können über Absatz 1 hinaus auf schriftlichen Antrag Auskünfte erteilt werden über

1. die Entlassungsadresse oder die Vermögensverhältnisse von Gefangenen, wenn die Erteilung zur Feststellung oder Durchsetzung von Rechtsansprüchen im Zusammenhang mit der Straftat erforderlich ist,
2. die Gewährung erstmaliger Lockerungen, wenn sie ein berechtigtes Interesse darlegen und kein überwiegendes schutzwürdiges Interesse der Gefangenen am Ausschluss der Mitteilung vorliegt, oder
3. den Gefangenen erneut gewährte Lockerungen, wenn dafür ein berechtigtes Interesse dargelegt oder ersichtlich ist und kein überwiegendes schutzwürdiges Interesse der Gefangenen am Ausschluss der Mitteilung besteht.

(3) In den Fällen des Absatzes 2 Nummer 2 bedarf es der Darlegung eines berechtigten Interesses nicht, wenn die Antragstellerin oder der Antragsteller Verletzte oder Verletzter einer Straftat nach

1. §§ 174 bis 182, 184i und 184j des Strafgesetzbuchs,
2. §§ 211 und 212 des Strafgesetzbuchs, die versucht wurde,
3. §§ 221, 223 bis 226 und 340 des Strafgesetzbuchs,
4. §§ 232 bis 238, § 239 Absatz 3 und §§ 239a, 239b und § 240 Absatz 4 des Strafgesetzbuchs oder
5. § 4 des Gewaltschutzgesetzes vom 11. Dezember 2001 (BGBl. I S.3513), zuletzt geändert durch Artikel 4 des Gesetzes vom 1. März 2017 (BGBl. I S. 386),

ist. Satz 1 gilt entsprechend in den Fällen des § 395 Absatz 3 der Strafprozessordnung, wenn die Antragstellerin oder der Antragsteller zur Nebenklage zugelassen wurde.

(4) Zuständigen öffentlichen Stellen können über Absatz 1 hinaus auf schriftlichen Antrag Auskünfte über die Entlassungsadresse oder die Vermögensverhältnisse von Gefangenen erteilt werden, wenn dies zur Feststellung oder Durchsetzung öffentlich-rechtlicher Forderungen erforderlich ist.

(5) Im Vollzug der Untersuchungshaft und der Freiheitsentziehungen nach § 1 Absatz 1 Nummer 2 besteht die zulässige Mitteilung nach den Absätzen 1 und 2 in der Angabe, ob sich eine Person in der Anstalt in Untersuchungshaft oder der Freiheitsentziehung befindet. Eine Übermittlung unterbleibt, wenn die Gefangenen unter Berücksichtigung der Art der Information und ihrer Rechtsstellung ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben.

(6) Die betroffenen Gefangenen werden vor der Mitteilung gehört, es sei denn, es ist zu besorgen, dass dadurch die Interessen der Antragstellerin oder des Antragstellers vereitelt oder wesentlich erschwert werden würden, und eine Abwägung ergibt, dass diese Interessen das Interesse der Gefangenen an ihrer vorherigen Anhörung überwiegen. Ist die Anhörung unterblieben, werden die betroffenen Gefangenen über die Mitteilung unter Angabe des Inhalts nachträglich unterrichtet.

7) Bei Anhörung und Unterrichtung Gefangener nach Absatz 6 ist auf die berechtigten Interessen nichtöffentlicher Empfänger an der Geheimhaltung ihrer Lebensumstände in besonderer Weise Rücksicht zu nehmen. Die Anschrift der Empfänger darf den Gefangenen nicht übermittelt werden.

(8) Erfolgte Mitteilungen sind in den Gefangenenpersonalakten der betroffenen Gefangenen zu dokumentieren.

§ 21 Aktenüberlassung

(1) Soweit die Übermittlung der darin enthaltenen Daten zulässig ist, dürfen Akten mit personenbezogenen Daten nur

1. Justizvollzugsbehörden,
2. Stellen der Gerichtshilfe, Jugendgerichtshilfe, Nachsorge, Bewährungshilfe oder Führungsaufsicht,
3. den für strafvollzugs-, strafvollstreckungs- und strafrechtliche Entscheidungen zuständigen Gerichten,
4. den Strafvollstreckungs- und Strafverfolgungsbehörden,
5. den von Justizvollzugs-, Strafverfolgungs- oder Strafvollstreckungsbehörden oder von einem Gericht mit Gutachten beauftragten Stellen sowie
6. sonstigen öffentlichen Stellen, wenn die Erteilung einer Auskunft entweder einen unverhältnismäßigen Aufwand erfordern würde oder nach Darlegung der die Akteneinsicht begehrenden Stelle die Erteilung einer Auskunft für die Erfüllung ihrer Aufgaben nicht ausreicht, überlassen oder im Falle elektronischer Aktenführung in Form von Duplikaten übermittelt werden.

(2) Sind mit personenbezogenen Daten, die nach § 12 Absatz 1, 3 oder 5 übermittelt werden dürfen, weitere personenbezogene Daten von betroffenen Personen oder von Dritten in Akten so verbunden, dass eine Trennung, Anonymisierung oder Pseudonymisierung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, ist die Übermittlung nach Absatz 1 zulässig,

soweit nicht berechnigte Interessen von betroffenen Personen oder Dritten an deren Geheimhaltung offensichtlich überwiegen. Soweit es sich um besondere Kategorien personenbezogener Daten handelt, ist regelmäßig von einem überwiegenden berechtigten Interesse der betroffenen Personen auszugehen. Eine Speicherung, Nutzung und Übermittlung der weiteren personenbezogenen Daten nach Satz 1 durch die empfangende öffentliche Stelle ist unzulässig.

§ 22

Auskunft und Akteneinsicht für wissenschaftliche Zwecke

(1) Für die Übermittlung personenbezogener Daten in Akten an Hochschulen, andere Einrichtungen, die wissenschaftliche Forschung betreiben, und öffentliche Stellen für wissenschaftliche Zwecke gilt § 476 der Strafprozessordnung entsprechend mit der Maßgabe, dass auch elektronisch gespeicherte personenbezogene Daten übermittelt werden können. Die Übermittlung kann auch auf elektronischem Wege erfolgen.

(2) Im Vollzug der Untersuchungshaft und der Freiheitsentziehungen nach § 1 Absatz 1 Nummer 2 unterbleiben Übermittlungen nach Absatz 1, wenn für die übermittelnde Stelle erkennbar ist, dass die Gefangenen unter Berücksichtigung der Art der Information und ihrer Rechtsstellung ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben.

§ 23

Einsichtnahme in Gefangenenpersonalakten, Gesundheitsakten und Krankenblätter

Die Mitglieder einer Delegation des Europäischen Ausschusses zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe erhalten während des Besuchs in der Anstalt Einsicht in die Gefangenenpersonalakten, Gesundheitsakten und Krankenblätter im Justizvollzugskrankenhaus, soweit dies zur Wahrnehmung der Aufgaben des Ausschusses unbedingt erforderlich ist.

Abschnitt 5

Besondere Formen der Datenverarbeitung

§ 24

Datenverarbeitung im Auftrag

(1) Die Justizvollzugsbehörden dürfen personenbezogene Daten durch andere Personen oder Stellen im Auftrag verarbeiten lassen. Dies gilt auch für Test- und Freigabeverfahren, Prüfungs- und Wartungsarbeiten und vergleichbare Hilfstätigkeiten einschließlich der Fernwartung.

(2) In den Fällen des Absatz 1 bleiben die Justizvollzugsbehörden für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Schadensersatz sind in diesem Fall gegenüber den Justizvollzugsbehörden geltend zu machen.

(3) Die Justizvollzugsbehörden dürfen 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 Personen gewährleistet wird.

(4) Auftragsverarbeiter dürfen weitere Auftragsverarbeiter ohne gesonderte vorherige schriftliche Genehmigung der Justizvollzugsbehörden nicht in Anspruch nehmen.

(5) Zieht ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter hinzu, so legt er diesem dieselben Verpflichtungen aus seinem Vertrag mit den Justizvollzugsbehörden oder einem anderen Rechtsinstrument nach Absatz 6 auf, die auch für ihn gelten, soweit diese Pflichten für den weiteren Auftragsverarbeiter nicht schon aufgrund anderer Vorschriften verbindlich sind. Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber den Justizvollzugsbehörden für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.

(6) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines schriftlichen Vertrags oder eines anderen Rechtsinstruments, der oder das den Auftragsverarbeiter an die Justizvollzugsbehörden 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 Justizvollzugsbehörden festlegt. Der Vertrag oder das andere Rechtsinstrument enthalten insbesondere, dass der Auftragsverarbeiter 1. nur auf dokumentierte Weisung der Justizvollzugsbehörden handelt; ist der Auftragsverarbeiter der Auffassung, dass eine Weisung rechtswidrig ist, hat er die Justizvollzugsbehörden 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 Justizvollzugsbehörden mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Personen zu gewährleisten, 4. alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl der Justizvollzugsbehörden zurückgibt oder löscht und bestehende Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht, 5. den Justizvollzugsbehörden alle erforderlichen Informationen, insbesondere die gemäß § 42 erstellten Protokolle, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt, 6. Überprüfungen, die von den Justizvollzugsbehörden oder einem von diesen hierzu Beauftragten durchgeführt werden, ermöglicht und dazu beiträgt, 7. die in den Absätzen 4 und 5 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält, 8. alle gemäß § 40 erforderlichen Maßnahmen ergreift und 9. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Justizvollzugsbehörden bei der Einhaltung der in den §§ 40, 41 und 64 Absatz 1 Nummer 1 und 5 genannten Pflichten unterstützt.

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

(8) § 18 Absatz 6 und § 19 gelten entsprechend.

§ 25

Datenverarbeitung bei Übertragung von Vollzugsaufgaben

(1) Werden Aufgaben zu vollzuglichen Zwecken in zulässiger Weise öffentlichen oder nicht-öffentlichen Stellen zur Erledigung übertragen, dürfen personenbezogene Daten übermittelt

werden, soweit dies für die Erfüllung der Aufgaben erforderlich ist. Besondere Kategorien personenbezogener Daten dürfen nur übermittelt werden, soweit dies für die Erfüllung der Aufgaben unbedingt erforderlich ist. Ist die Übermittlung nach Satz 1 oder 2 zulässig, dürfen Akten und Dateisysteme überlassen werden, soweit dies zur Aufgabenerfüllung unbedingt erforderlich ist.

(2) Die Auftragnehmer nach Absatz 1 Satz 1 sind sorgfältig auszuwählen. Dabei ist auch zu berücksichtigen, ob die Auftragnehmer ausreichend Gewähr dafür bieten, dass sie die für eine datenschutzgerechte Datenverarbeitung erforderlichen technischen und organisatorischen Maßnahmen zu treffen in der Lage sind. Der Auftrag ist schriftlich oder im elektronischen Format zu erteilen. Er enthält Angaben zum Gegenstand und zum Umfang der Aufgabenübertragung, zur Erforderlichkeit der Verarbeitung von personenbezogenen Daten zur Erfüllung übertragener Aufgaben und die förmliche Verpflichtung des hierfür einzusetzenden Personals nach § 1 des Verpflichtungsgesetzes in der jeweils gültigen Fassung. Die Justizvollzugsbehörden sind verpflichtet, die Einhaltung der von den Auftragnehmern getroffenen datenschutzrechtlichen Maßnahmen regelmäßig zu überprüfen und dies zu dokumentieren.

(3) Soweit die Auftragnehmer zur Erfüllung der übertragenen Aufgaben personenbezogene Daten verarbeiten, finden die Vorschriften dieses Gesetzes entsprechende Anwendung.

§ 26

Gemeinsame Verantwortung der Justizvollzugsbehörden

Legen zwei oder mehrere Justizvollzugsbehörden gemeinsam die Zwecke und die Mittel der Verarbeitung fest, gelten sie als gemeinsam verantwortlich. Sie haben ihre jeweiligen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten in transparenter Form in einer Vereinbarung festzulegen, soweit diese nicht bereits in Rechtsvorschriften festgelegt sind. Aus der Vereinbarung muss insbesondere hervorgehen, wer welchen Informationspflichten nachzukommen hat und wie und gegenüber wem betroffene Personen ihre Rechte wahrnehmen können.

§ 27

Erkennungsdienstliche Maßnahmen

(1) Zur Identitätsfeststellung und zur Gewährleistung der Sicherheit der Anstalt sind mit Kenntnis der Gefangenen zulässig:

1. die Aufnahme von Lichtbildern,
2. die Abnahme von Finger- und Handflächenabdrücken,
3. die Feststellung äußerlicher körperlicher Merkmale,
4. Messungen,
 5. die Erfassung biometrischer Merkmale von Fingern, Händen, Gesicht, Augen, der Stimme und
6. die Erfassung der Unterschrift.

(2) Die nach Absatz 1 gewonnenen erkennungsdienstlichen Daten werden zu den Gefangenenpersonalakten genommen oder in personenbezogenen Dateisystemen gespeichert. Sie sind so zu sichern, dass eine Kenntnisnahme nur zu den in den Absätzen 3 und 4 genannten Zwecken sowie zu den Zwecken der §§ 16 und § 28 möglich ist.

(3) Nach Absatz 1 erhobene Daten dürfen nur genutzt werden

1. für die Zwecke, zu denen sie erhoben wurden,

2. zur Identifikation Gefangener, soweit dies für Zwecke der Fahndung und Festnahme der entwichenen oder sich sonst ohne Erlaubnis außerhalb der Anstalt aufhaltenden Gefangenen erforderlich ist oder
3. für die in § 10 Absatz 2 Nummer 5, § 16 und § 28 genannten Zwecke.

(4) Nach Absatz 1 erhobene Daten dürfen nur übermittelt werden an

1. Vollstreckungs- und Strafverfolgungsbehörden, soweit dies für Zwecke der Fahndung nach und Festnahme von entwichenen oder sich sonst ohne Erlaubnis außerhalb der Anstalt aufhaltenden Gefangenen erforderlich ist,
2. Polizeibehörden des Bundes und der Länder, soweit dies zur Abwehr einer gegenwärtigen in der Anstalt drohenden Gefahr für Leib, Leben oder Freiheit von Personen oder für erhebliche Sachwerte erforderlich ist,
3. die in § 16 und § 28 genannten öffentlichen Stellen unter den dort genannten Voraussetzungen sowie
4. öffentliche Stellen auf deren Ersuchen, soweit die betroffenen Personen verpflichtet wären, eine unmittelbare Erhebung der zu übermittelnden Daten durch diese zu dulden oder an einer solchen Erhebung mitzuwirken; die ersuchende öffentliche Stelle hat in ihrem Ersuchen die Rechtsgrundlage der Mitwirkungs- oder Duldungspflicht mitzuteilen; beruht diese Pflicht auf einer Anordnung gegenüber den betroffenen Personen im Einzelfall, weist die ersuchende Stelle zugleich nach, dass eine entsprechende Anordnung ergangen und vollziehbar ist.

(5) Nach Absatz 1 erhobene Daten sind nach der Entlassung der Gefangenen unverzüglich zu löschen; §§ 59, 60 bleiben unberührt. Die Löschung ist in den Gefangenenpersonalakten zu dokumentieren.

§ 28

Erkennungsdienstlicher Datenabgleich

(1) Bestehen Zweifel an der Identität von Gefangenen, übermitteln die Justizvollzugsbehörden die von ihnen erhobenen oder anderweitig bei ihnen vorliegenden erkennungsdienstlichen Daten im Sinne des § 27 Absatz 1 sowie die bei ihnen im Sinne des § 14 Absatz 3 vorliegenden Daten unverzüglich dem Landeskriminalamt, soweit dies zur Identitätsfeststellung erforderlich ist. Das Landeskriminalamt veranlasst einen Abgleich der übermittelten Daten mit den dort vorliegenden Daten zum Zwecke der Identifizierung der Gefangenen und teilt das Ergebnis den Justizvollzugsbehörden mit.

(2) Unter den Voraussetzungen des Absatzes 1 Satz 1 dürfen die Justizvollzugsbehörden auch das Bundeskriminalamt sowie das Bundesamt für Migration und Flüchtlinge um einen Abgleich der erkennungsdienstlichen Daten und Identitätsdaten ersuchen.

(3) Die nach Absatz 1 übermittelten Daten dürfen beim Empfänger nur für Zwecke des Abgleichs verwendet werden und nicht über den Zeitpunkt der Mitteilung des Ergebnisses hinaus, dort gespeichert werden.

§ 29

Einsatz optisch-elektronischer Einrichtungen und biometrischer Zu- und Ausgangskontrollen

(1) Die Anstalten dürfen Räume und Freiflächen mittels optisch-elektronischer Einrichtungen nur beobachten, soweit eine gesetzliche Bestimmung dies aus Gründen der Sicherheit gestattet.

(2) Jede Anstalt, die optisch-elektronische Einrichtungen einsetzt, erstellt ein einheitliches Konzept zur optisch-elektronischen Beobachtung der baulichen Anlagen. Das Konzept hat alle betriebsfähigen Einrichtungen sowie die von ihnen erfassten Bereiche in kartenmäßiger Darstellung zu enthalten und ist laufend fortzuschreiben.

(3) Bei der Planung optisch-elektronischer Einrichtungen ist sicherzustellen, dass

1. die Beobachtung nur insoweit erfolgt, als dies aus Gründen der Sicherheit erforderlich ist, insbesondere um das Betreten bestimmter Zonen durch Unbefugte zu verhindern und
2. den Gefangenen in den Anstalten angemessene Bereiche verbleiben, in denen sie nicht mittels optisch-elektronischer Einrichtungen beobachtet werden.

(4) Die Beobachtung mittels optisch-elektronischer Einrichtungen von Räumen und Freiflächen ist durch sprachliche und nicht sprachliche Zeichen auf eine Weise kenntlich zu machen, die die Tatsache und die Reichweite der Beobachtung jederzeit eindeutig erkennbar macht.

(5) Bei Gefangenentransporten ist in den vom Justizvollzug genutzten Fahrzeugen die Beobachtung von Gefangenen mittels optisch-elektronischer Einrichtungen zulässig; Absatz 4 und § 32 Absatz 4 gelten entsprechend.

(6) Soweit es zur Sicherung der Anstalten erforderlich ist, sind mit Kenntnis und unter Mitwirkung der Bediensteten im Rahmen von Zu- und Ausgangskontrollen die elektronische Erfassung biometrischer Merkmale (physiologische und physische Merkmale) und Messungen zulässig. Die Verarbeitung der nach Satz 1 erhobenen Daten durch die Anstalten ist zulässig, wenn es zur Sicherung der Anstalten erforderlich ist. Die Daten nach Satz 1 dürfen nur für die Zwecke verarbeitet werden, für die sie erhoben worden sind. Sie sind unverzüglich zu löschen, sobald die betroffenen Bediensteten aus dem Dienst ausscheiden.

§ 30

Optisch-elektronische Einrichtungen im Umfeld der Anstalt

Die Beobachtung öffentlich frei zugänglichen Raumes außerhalb der Grenzen der Anstalt mittels optisch-elektronischer Einrichtungen ist nur und soweit zulässig, wie dies aufgrund der örtlichen Gegebenheiten zur Wahrnehmung des Hausrechts oder zur Sicherheit der Anstalt auch unter Berücksichtigung der Belange Dritter unbedingt erforderlich ist, insbesondere um Entweichungen, Befreiungen und Überwürfe von Gegenständen auf das Anstaltsgelände zu verhindern.

§ 31

Optisch-elektronische Einrichtungen innerhalb der Anstalt

Die Beobachtung von Räumen und Freiflächen innerhalb der Anstalt mittels optisch-elektronischer Einrichtungen ist zulässig, soweit dies aus Gründen der Sicherheit erforderlich ist, insbesondere um die Gefangenen zu beaufsichtigen und das Betreten bestimmter Zonen durch Unbefugte zu verhindern, und § 32 nichts anderes bestimmt.

§ 32

Optisch-elektronische Einrichtungen innerhalb von Hafträumen und Zimmern

(1) Die Beobachtung innerhalb von Hafträumen und Zimmern mittels optisch-elektronischer Einrichtungen ist nicht zulässig, soweit nachfolgend nichts anderes bestimmt ist.

(2) Im Rahmen einer Beobachtung als besonderer Sicherungsmaßnahme ist die optisch-elektronische Beobachtung zulässig, soweit dies zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben erforderlich ist. Soweit die Erforderlichkeit entfällt, ist die optisch-elektronische Beobachtung unverzüglich zu beenden. Die optisch-elektronische Beobachtung ist im Rahmen der Anordnung der Beobachtung schriftlich anzuordnen und zu begründen; in der Anordnung ist der Umfang der Beobachtung zu bestimmen.

(3) Während der Dauer der optisch-elektronischen Beobachtung ist diese für die Gefangenen kenntlich zu machen.

(4) Bei der Gestaltung und Beobachtung optisch-elektronisch beobachteter Hafträume und Zimmer ist grundsätzlich auf die elementaren Bedürfnisse der Gefangenen nach Wahrung ihrer Intimsphäre angemessen Rücksicht zu nehmen, insbesondere sind sanitäre Einrichtungen von der Beobachtung auszunehmen; hilfsweise ist die Erkennbarkeit dieser Bereiche durch technische Maßnahmen auszuschließen. Bei akuter Selbstverletzungs- oder Selbsttötungsgefahr ist im Einzelfall eine uneingeschränkte Überwachung zulässig. Die Beobachtung weiblicher Gefangener soll durch weibliche Bedienstete, die Beobachtung männlicher Gefangener durch männliche Bedienstete erfolgen.

(5) Die optisch-elektronische Beobachtung ist zu unterbrechen, wenn sie im Einzelfall vorübergehend nicht erforderlich oder die Beaufsichtigung gesetzlich ausgeschlossen ist.

§ 33

Speicherung mittels optischer oder akustischer Einrichtungen erhobener Daten, Dokumentation

(1) Die mittels optisch-elektronischer Einrichtungen zulässig erhobenen Daten dürfen nur gespeichert werden, wenn dies zur Erreichung des die Erhebung gestattenden Zwecks erforderlich ist. Sobald dieser Zweck entfällt, sind die Daten unverzüglich, spätestens nach 4 Wochen zu löschen. § 60 Absatz 1 Nummer 1 bis 3 und 5 bleibt unberührt.

(2) Für die Speicherung der mittels akustisch-elektronischer Einrichtungen zulässig erhobenen Daten gilt Absatz 1 entsprechend. Darüber hinaus ist eine Speicherung auch zulässig, soweit und solange dies zur Übermittlung der erhobenen Daten an das Gericht, das die inhaltliche Überwachung der Gespräche angeordnet hat, erforderlich ist.

(3) Mittels akustisch-elektronischer Einrichtungen erhobene Daten dürfen nicht weiter verarbeitet werden, soweit sie dem Kernbereich der privaten Lebensgestaltung unterfallen. Durch geeignete Maßnahmen und Prüfungen ist sicherzustellen, dass keine weitere Verarbeitung dieser Daten erfolgt. Dennoch gespeicherte Daten sind unverzüglich zu löschen. Nicht vom Kernbereich der privaten Lebensgestaltung erfasst sind in der Regel Gespräche über Straftaten oder Gespräche, durch die Straftaten begangen werden.

(4) Die Verarbeitung der mittels optisch-elektronischer oder akustisch-elektronischer Einrichtungen erhobenen Daten ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese

Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

§ 34

Auslesen von Datenspeichern

(1) Elektronische Datenspeicher sowie elektronische Geräte mit Datenspeicher, die sich ohne Erlaubnis in der Anstalt befinden, dürfen auf Anordnung der Anstaltsleiterin oder des Anstaltsleiters ausgelesen werden, soweit konkrete Anhaltspunkte die Annahme rechtfertigen, dass dies zur Abwehr von Gefahren für die Sicherheit und Ordnung der Anstalt erforderlich ist. Die Gründe sind in der Anordnung festzuhalten. Sind die betroffenen Personen bekannt, sind ihnen die Gründe vor dem Auslesen mitzuteilen. Beim Auslesen sind die schutzwürdigen Interessen der betroffenen Personen, insbesondere der Kernbereich privater Lebensgestaltung, zu berücksichtigen. Das Auslesen ist möglichst auf die Inhalte zu beschränken, die zur Erreichung der die Anordnung begründenden Zwecke erforderlich sind.

(2) Die nach Absatz 1 erhobenen Daten dürfen zu den Zwecken, zu denen sie erhoben wurden, verarbeitet werden, soweit dies erforderlich ist. Darüber hinaus ist die Verarbeitung zu den in §§ 10 Absatz 2 und Absatz 3, § 12 Absatz 3 und Absatz 6 unter Beachtung von § 17 genannten Zwecken zulässig, soweit dies erforderlich ist und schutzwürdige Interessen der betroffenen Personen dem nicht entgegenstehen.

(3) Die Verarbeitung der nach Absatz 1 erhobenen Daten ist unzulässig, soweit sie dem Kernbereich der privaten Lebensgestaltung unterfallen. Diese Daten sind unverzüglich zu löschen. Die Erhebung und die Löschung der Daten sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist. § 42 Absatz 4 gilt entsprechend.

(4) Die Gefangenen sind bei der Aufnahme über die Möglichkeit des Auslesens von nicht gestatteten Datenspeichern zu belehren.

§ 35

Identifikation anstaltsfremder Personen

(1) Das Betreten der Anstalt durch anstaltsfremde Personen kann davon abhängig gemacht werden, dass diese zur Identitätsfeststellung

1. ihre Vornamen, ihren Namen und ihre Anschrift angeben und durch amtliche Ausweise nachweisen und

2. die Erhebung von eindeutigen Identifikationsmerkmalen des Gesichts, der Augen, der Hände, der Stimme oder der Unterschrift dulden, soweit dies erforderlich oder, wenn es sich um biometrische Daten handelt, unbedingt erforderlich ist, um Entweichungen von Gefangenen durch verwechselungsbedingtes Verlassen der Anstalt zu verhindern.

(2) Eine Verarbeitung der nach Absatz 1 erhobenen Identifikationsmerkmale ist nur zulässig, soweit dies erforderlich ist zur

1. Identitätsüberprüfung vor dem Verlassen der Anstalt oder

2. Verfolgung von Straftaten, bei denen der Verdacht besteht, dass sie während des Aufenthalts in der Anstalt begangen wurden; die zur Strafverfolgung erforderlichen Daten können hierzu der zuständigen Strafverfolgungsbehörde übermittelt werden; dies gilt auch für die

Verfolgung von Ordnungswidrigkeiten gemäß § 115 des Gesetzes über Ordnungswidrigkeiten.

(3) Die nach Absatz 1 Nr. 2 erhobenen Identifikationsmerkmale sind spätestens 24 Stunden nach ihrer Erhebung zu löschen, soweit sie nicht nach Absatz 2 Nummer 2 übermittelt werden dürfen; in diesem Fall sind sie unverzüglich zu übermitteln und danach zu löschen.

(4) § 28 gilt entsprechend.

§ 36 Lichtbildausweise

(1) Die Anstalt kann die Gefangenen verpflichten, einen Lichtbildausweis mit sich zu führen, wenn dies aus Gründen der Sicherheit oder Ordnung der Anstalt erforderlich ist. Dabei ist sicherzustellen, dass der Ausweis nur die zur Erreichung dieser Zwecke notwendigen Daten enthält.

(2) Der Ausweis ist bei der Entlassung oder bei der Verlegung in eine andere Anstalt einzuziehen und unverzüglich zu vernichten.

Abschnitt 6 Schutzanforderungen

§ 37 Zweckbindung

Empfänger dürfen personenbezogene Daten nur zu dem Zweck speichern, nutzen und übermitteln, zu dessen Erfüllung sie übermittelt wurden. Für andere Zwecke dürfen sie diese Daten nur speichern, nutzen und übermitteln, soweit sie ihnen auch für diese Zwecke hätten überlassen werden dürfen und wenn im Fall einer Übermittlung an eine nichtöffentliche Stelle die Justizvollzugsbehörde zugestimmt hat. Die Justizvollzugsbehörden weisen die Empfänger auf die Zweckbindung nach den Sätzen 1 und 2 hin.

§ 38 Schutzvorkehrungen

(1) Personenbezogene Daten in Akten und Dateisystem sind gegen unbefugten Zugang, unbefugte Offenlegung und unbefugten Gebrauch, sowie vor Vernichtung, Verlust und Veränderung, ob unbeabsichtigt oder unrechtmäßig, zu schützen. Für Art und Umfang der hierzu erforderlichen technischen und organisatorischen Maßnahmen gelten §§ 39 bis 41.

(2) Soweit nichts anderes geregelt ist, dürfen sich die Bediensteten von personenbezogenen Daten nur Kenntnis verschaffen, wenn dies zur Erfüllung der ihnen obliegenden Aufgaben oder zugewiesenen Tätigkeiten erforderlich ist.

(3) Gesundheitsakten sind getrennt von anderen Unterlagen zu führen und besonders zu sichern.

§ 39

Verzeichnis von Verarbeitungstätigkeiten

(1) Die Justizvollzugsbehörden haben ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die in ihre Zuständigkeit fallen. Dieses Verzeichnis hat die folgenden Angaben zu enthalten:

1. den Namen und die Kontaktdaten der jeweiligen Justizvollzugsbehörde und den Namen sowie die Kontaktdaten der oder des behördlichen Datenschutzbeauftragten,
2. die Zwecke der Verarbeitung,
3. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
4. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen,
5. die Kategorien von Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,
6. die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten,
7. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 40,
8. die Rechtsgrundlage der Verarbeitung und
9. die Verwendung von Profiling.

(2) Der Auftragsverarbeiter hat ein Verzeichnis aller Kategorien von Verarbeitungen zu führen, die er im Auftrag der Justizvollzugsbehörden durchführt, das folgende Angaben zu enthalten hat:

1. den Namen und die Kontaktdaten des Auftragsverarbeiters, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie der oder des behördlichen Datenschutzbeauftragten,
2. 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 § 40.

(3) Die in den Absätzen 1 und 2 genannten Verzeichnisse sind schriftlich oder in einem elektronischen Format zu führen.

(4) Die Justizvollzugsbehörden und Auftragsverarbeiter stellen ihre Verzeichnisse der oder dem Landesbeauftragten für Datenschutz auf Anforderung zur Verfügung.

§ 40

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Die Justizvollzugsbehörden und der Auftragsverarbeiter treffen unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen, 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 von den Justizvollzugsbehörden zu treffenden technischen und organisatorischen Maßnahmen gewährleisten, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
4. personenbezogene Daten jederzeit ihrem Ursprung zugeordnet werden können (Authentizität),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz),
7. personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck verarbeitet werden können, sofern nicht eine Rechtsvorschrift dies erlaubt oder anordnet (Nicht-Verkettbarkeit), und
8. Verfahren so gestaltet werden, dass sie den betroffenen Personen die Ausübung der in den Abschnitten 8 und 9 genannten Rechte wirksam ermöglichen (Intervenierbarkeit).

(3) Zur Umsetzung der Maßnahmen nach Absatz 2 ergreifen die Justizvollzugsbehörden oder der Auftragsverarbeiter im Fall einer automatisierten Verarbeitung nach einer Risikobewertung Maßnahmen, 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 Störfall 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) und

14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).

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

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

(5) Die zu treffenden technischen und organisatorischen Maßnahmen sind auf der Grundlage eines zu dokumentierenden Sicherheitskonzepts zu ermitteln, zu dessen Bestandteilen die Abschätzung von Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für das Recht auf informationelle Selbstbestimmung gehört. Die Wirksamkeit der Maßnahmen ist unter Berücksichtigung sich verändernder Rahmenbedingungen und Entwicklungen der Technik zu überprüfen. Die sich daraus ergebenden notwendigen Anpassungen sind zeitnah umzusetzen, soweit dies mit einem angemessenen Aufwand möglich ist. § 41 bleibt unberührt.

§ 41

Datenschutz-Folgenabschätzung bei hohem Risiko, Konsultationspflicht

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge, führen die Justizvollzugsbehörden vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen durch.

(2) Für mehrere ähnliche Verarbeitungsvorgänge mit ähnlich hohem Gefahrenpotential kann eine gemeinsame Datenschutz-Folgenabschätzung vorgenommen werden.

(3) Die Justizvollzugsbehörden beteiligen die behördlichen Datenschutzbeauftragten an der Durchführung der Datenschutz-Folgenabschätzung.

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

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

(5) Die Justizvollzugsbehörden haben vor der Inbetriebnahme von neu anzulegenden Dateisystemen die Landesbeauftragte oder den Landesbeauftragten für Datenschutz anzuhören,

1. wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge hätte, wenn die Justizvollzugsbehörden keine Abhilfemaßnahmen treffen würden, oder
2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge hat.

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

(6) Der oder dem Landesbeauftragten für Datenschutz sind im Fall des Absatzes 5 vorzulegen:

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

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

(7) Falls die oder Landesbeauftragte für Datenschutz der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstoßen würde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder keine ausreichenden Abhilfemaßnahmen getroffen hat, kann sie oder er dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von sechs Wochen nach Einleitung der Anhörung schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergriffen werden sollten. Die oder der Landesbeauftragte für Datenschutz kann diese Frist um einen Monat verlängern, wenn die geplante Verarbeitung besonders komplex ist. 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.

(8) Hat die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung des Verantwortlichen und ist sie daher besonders dringlich, kann er mit der Verarbeitung nach Beginn der Anhörung, aber vor Ablauf der in Absatz 7 Satz 1 genannten Frist beginnen. 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.

§ 42 Protokollierung

(1) In automatisierten Verarbeitungssystemen sind die folgenden Verarbeitungsvorgänge zu protokollieren:

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

6. Löschung oder Einschränkung der Verarbeitung.

(2) Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen. Aus der Identität der Person muss sich auch die Begründung für eine Abfrage oder Offenlegung ableiten lassen.

(3) Die Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die behördlichen Datenschutzbeauftragten, die Landesbeauftragte für Datenschutz oder den Landesbeauftragten für Datenschutz sowie für die Eigenüberwachung und für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten verwendet werden. Die Protokolldaten dürfen auch zur Verfolgung von Straftaten und Ordnungswidrigkeiten oder für beamtenrechtliche oder disziplinarrechtliche Maßnahmen im Zusammenhang mit einer Verletzung des Datengeheimnisses sowie zur Verfolgung von Straftaten von erheblicher Bedeutung verarbeitet werden.

(4) Die Protokolldaten sind zwei Jahre nach ihrer Erstellung zu löschen.

(5) Die Protokolle sind der oder dem Landesbeauftragten für Datenschutz auf Anforderung zur Verfügung zu stellen.

§ 43

Kenntlichmachung innerhalb der Anstalt

(1) Personenbezogene Daten von Gefangenen dürfen innerhalb der Anstalt nur kenntlich gemacht werden, soweit dies für ein geordnetes Zusammenleben in der Anstalt erforderlich ist und Bestimmungen dieses Gesetzes nicht entgegenstehen.

(2) Besondere Kategorien personenbezogener Daten von Gefangenen dürfen in der Anstalt nicht allgemein kenntlich gemacht werden.

§ 44

Erkenntnisse aus Beaufsichtigungs-, Überwachungs- und Kontrollmaßnahmen

(1) Die bei der Beaufsichtigung oder der Überwachung der Besuche, der Überwachung der Telekommunikation, der Sichtkontrolle oder der Überwachung des Schriftwechsels oder der Kontrolle des Inhalts von Paketen in zulässiger Weise bekannt gewordenen personenbezogenen Daten sind in Akten und Dateisystemen des Vollzuges sowie bei einer Übermittlung eindeutig als solche zu kennzeichnen. Sie dürfen nur verarbeitet werden

1. mit Einwilligung der Gefangenen,
2. für die Maßnahmen der Vollzugs- und Eingliederungsplanung,
3. zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt oder
4. für die in § 10 Absatz 2 und § 16 genannten Zwecke.

(2) Die nach Absatz 1 Satz 1 zulässig bekannt gewordenen Daten dürfen im Vollzug der Untersuchungshaft und der Freiheitsentziehungen nach § 1 Absatz 1 Nummer 2 über die in Absatz 1 Satz 2 bezeichneten Zwecke hinaus auch verarbeitet werden zur

1. Abwehr von Gefährdungen der Aufgabe des Vollzuges der Untersuchungshaft oder
2. Umsetzung einer Anordnung nach § 119 der Strafprozessordnung.

(3) Soweit die in Absatz 1 bezeichneten Daten dem Kernbereich der privaten Lebensgestaltung unterfallen, dürfen sie nicht aufgezeichnet, protokolliert oder sonst gespeichert und nicht auf andere Art verarbeitet werden. Nicht erfasst vom Kernbereich der privaten Lebensgestaltung sind in der Regel Gespräche über Straftaten oder Gespräche, durch die Straftaten begangen werden. Abweichend von Satz 1 gespeicherte Daten sind unverzüglich zu löschen. Die Tatsachen der Erfassung und der Löschung der Daten sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist. § 42 Absatz 4 gilt entsprechend.

Abschnitt 7

Besondere Bestimmungen für Geheimnisträgerinnen und Geheimnisträger

§ 45

Geheimnisträgerinnen und Geheimnisträger

(1) Die im Justizvollzug tätigen oder außerhalb des Justizvollzuges mit der Untersuchung, Behandlung oder Beratung von Gefangenen beauftragten

1. Ärztinnen und Ärzte, Zahnärztinnen und Zahnärzte, Apothekerinnen und Apotheker oder Angehörige eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

2. Diplom-Psychologinnen und Diplom-Psychologen,

3. staatlich anerkannten Sozialarbeiterinnen und Sozialarbeiter oder staatlich anerkannten Sozialpädagoginnen und Sozialpädagogen sowie

4. Seelsorgerinnen und Seelsorger

unterliegen hinsichtlich der ihnen in der ausgeübten Funktion von Gefangenen anvertrauten oder sonst über Gefangene bekannt gewordenen Geheimnisse untereinander sowie gegenüber der Anstalt und der Aufsichtsbehörde der Schweigepflicht, soweit nichts anderes bestimmt ist. Dies gilt entsprechend für ihre berufsmäßig tätigen Gehilfinnen und Gehilfen und die Personen, die bei ihnen zur Vorbereitung auf den Beruf tätig sind, nicht aber gegenüber der Berufsgeheimnisträgerin oder dem Berufsgeheimnisträger.

(2) Die Anstalt weist externe Geheimnisträgerinnen und Geheimnisträger nach Absatz 1 Satz 1 Nummer 1 bis 3 (Berufsgeheimnisträgerinnen und Berufsgeheimnisträger) auf die Offenbarungspflichten und -befugnisse hin.

§ 46

Offenbarungspflicht

(1) Berufsgeheimnisträgerinnen und Berufsgeheimnisträger haben der Anstaltsleiterin oder dem Anstaltsleiter ihnen bekannte personenbezogene Daten von sich aus oder auf Befragen zu offenbaren, auch wenn sie ihnen im Rahmen des beruflichen Vertrauensverhältnisses anvertraut wurden oder sonst bekannt geworden sind, soweit dies auch unter Berücksichtigung der Interessen der Gefangenen an der Geheimhaltung der personenbezogenen Daten erforderlich ist zur Abwehr

1. einer Gefahr für das Leben eines Menschen, insbesondere zur Verhütung von Selbsttötungen,

2. einer erheblichen Gefahr für Körper oder Gesundheit eines Menschen oder

3. der Gefahr der Begehung von Straftaten von erheblicher Bedeutung.

(2) Staatlich anerkannte Sozialarbeiterinnen und Sozialarbeiter sowie staatlich anerkannte Sozialpädagoginnen und Sozialpädagogen, die als Bedienstete im Justizvollzug tätig sind, haben der Anstaltsleiterin oder dem Anstaltsleiter ihnen bekannte personenbezogene Daten von sich aus oder auf Befragen zu offenbaren, soweit dies zu vollzuglichen Zwecken erforderlich ist. Soweit sie im Rahmen von besonderen Behandlungsangeboten tätig sind, gilt Absatz 1.

(3) Berufsheimnisträgerinnen und Berufsheimnisträger außerhalb des Justizvollzuges können die Verpflichtung nach Absatz 1 auch gegenüber in der Anstalt beschäftigten Berufsheimnisträgerinnen oder Berufsheimnisträgern erfüllen.

§ 47

Offenbarungsbefugnis

(1) Die Berufsheimnisträgerinnen und Berufsheimnisträger sind befugt, die ihnen im Rahmen des beruflichen Vertrauensverhältnisses anvertrauten oder sonst bekannt gewordenen personenbezogenen Daten gegenüber der Anstaltsleiterin oder dem Anstaltsleiter zu offenbaren, soweit

1. die Gefangenen einwilligen oder
2. dies aus ihrer Sicht zu vollzuglichen Zwecken unbedingt erforderlich ist und das Interesse der Gefangenen an der Geheimhaltung nicht überwiegt.

(2) Behandeln Berufsheimnisträgerinnen oder Berufsheimnisträger gleichzeitig oder nacheinander dieselben Gefangenen, unterliegen sie im Verhältnis zueinander nicht der Schweigepflicht und sind zur umfassenden gegenseitigen Information und Auskunft befugt, wenn eine wirksame Einwilligung der Gefangenen vorliegt, dies zum Zwecke einer zielgerichteten gemeinsamen Behandlung erforderlich ist und sie in Bezug auf die betreffenden Gefangenen nicht mit anderen Aufgaben im Justizvollzug betraut sind.

§ 48

Benachrichtigung der Gefangenen über Offenbarungen

(1) Vor der Erhebung personenbezogener Daten sind die Gefangenen durch die Berufsheimnisträgerinnen oder Berufsheimnisträger schriftlich über die nach diesem Gesetz bestehenden Offenbarungspflichten und Offenbarungsbefugnisse zu unterrichten. Bei Einschaltung von Berufsheimnisträgerinnen oder Berufsheimnisträgern außerhalb der Anstalt erfolgt die Unterrichtung nach Satz 1 durch die Anstalt.

(2) Die Gefangenen sind von einer Offenbarung gemäß § 46 Absatz 1 Nummer 2 und Absatz 3 und § 47 zu benachrichtigen. Eine Pflicht zur Benachrichtigung besteht nicht, sofern die Gefangenen auf andere Weise Kenntnis von der Offenbarung erlangt haben. Die Benachrichtigung kann unterbleiben, solange hierdurch der Zweck der Maßnahme vereitelt würde. Die Benachrichtigung ist unverzüglich nachzuholen, sobald der Zweck der Maßnahme entfallen ist.

§ 49

Zweckbindung offenbarter personenbezogener Daten, Zulassung von Offenbarungsempfängern

(1) Die nach den §§ 46 und 47 offenbarten personenbezogenen Daten dürfen nur für den Zweck, für den sie offenbart wurden oder für den eine Offenbarung zulässig gewesen wäre, und nur unter denselben Voraussetzungen gespeichert, genutzt und übermittelt werden, unter denen Berufsgeheimnisträgerinnen und Berufsgeheimnisträger selbst hierzu befugt wären.

(2) Die Anstaltsleiterin oder der Anstaltsleiter kann unter diesen Voraussetzungen die unmittelbare Offenbarung gegenüber bestimmten Bediensteten allgemein zulassen.

§ 50

Zugriff auf Daten in Notfällen

(1) Alle im Justizvollzug tätigen Personen dürfen sich Kenntnis auch von besonderen Kategorien personenbezogener Daten zu dem Zweck verschaffen, diese Daten unmittelbar und unverzüglich den zur Notfallrettung eingesetzten Personen zu übermitteln, soweit die Gefangene oder der Gefangene

1. einwilligt oder

2. zur Einwilligung unfähig ist und die Kenntnisverschaffung zur Abwehr einer gegenwärtigen Gefahr für das Leben eines Menschen oder einer gegenwärtigen erheblichen Gefahr für die Gesundheit eines Menschen unbedingt erforderlich ist.

(2) Soweit dies zur Abwehr einer gegenwärtigen Gefahr für das Leben oder einer gegenwärtigen erheblichen Gefahr für die Gesundheit eines Menschen erforderlich ist, dürfen sich im Justizvollzug tätige Personen Kenntnis von personenbezogenen Daten verschaffen, die von Berufsgeheimnisträgerinnen oder Berufsgeheimnisträgern erhoben worden sind.

(3) Die anderweitige Verarbeitung der so erlangten Daten ist unzulässig. Die Kenntnisnahme ist in den Gefangenenpersonalakten zu dokumentieren.

Abschnitt 8

Rechte der betroffenen Personen

§ 51

Allgemeine Informationen zur Datenverarbeitung

Die verantwortlichen Justizvollzugsbehörden stellen den Gefangenen und anderen betroffenen Personen Informationen in allgemeiner und verständlicher Form zur Verfügung über

1. die Zwecke, für die die personenbezogenen Daten verarbeitet werden,

2. die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung,

3. ihre Namen und ihre Kontaktdaten und die Kontaktdaten ihrer behördlichen Datenschutzbeauftragten,

4. das Recht, die Landesbeauftragte für Datenschutz oder den Landesbeauftragten für Datenschutz anzurufen, und deren oder dessen Kontaktdaten.

§ 52

Aufklärungspflicht bei der Datenerhebung mit Kenntnis und Mitwirkung der betroffenen Personen

Werden personenbezogene Daten bei betroffenen Personen mit deren Kenntnis und Mitwirkung erhoben, sind sie in geeigneter Weise über den Zweck der Datenerhebung und das Bestehen von Auskunfts- und Berichtigungsrechten aufzuklären. Werden die personenbezogenen Daten aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, sind die betroffenen Personen hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen. Sind die Angaben für die Gewährung einer Leistung erforderlich, sind die betroffenen Personen über die möglichen Folgen einer Nichtbeantwortung aufzuklären.

§ 53

Benachrichtigung bei Datenverarbeitung ohne Kenntnis und Mitwirkung der betroffenen Personen

(1) Über eine ohne ihre Kenntnis und Mitwirkung vorgenommene Erhebung personenbezogener Daten oder eine Übermittlung von Daten zu Zwecken, zu denen sie nicht erhoben worden sind, werden die Gefangenen und andere betroffene Personen unter Angabe dieser Daten benachrichtigt. Diese Benachrichtigung enthält neben den in § 51 aufgeführten allgemeinen Informationen insbesondere die folgenden Angaben:

1. die Rechtsgrundlage der Verarbeitung,
2. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer und
3. die Empfänger der personenbezogenen Daten und
4. in den Fällen einer Erhebung Angaben zur Herkunft der personenbezogenen Daten.

(2) In den Fällen des Absatzes 1 dürfen die Justizvollzugsbehörden die Benachrichtigung aufschieben, einschränken oder unterlassen, soweit und solange andernfalls

1. die Erreichung der vollzuglichen Zwecke nach § 2 Nummer 2 gefährdet würde,
 2. Verfahren zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten oder der Strafvollstreckung gefährdet würden,
 3. die öffentliche Sicherheit gefährdet würde,
 4. dem Wohl des Bundes oder eines Landes Nachteile bereitet würden oder
 5. die Rechte einer anderen Person gefährdet oder beeinträchtigt würden,
- und das Interesse an der Vermeidung dieser Gefahren und Nachteile das Interesse der betroffenen Personen an der Benachrichtigung überwiegt.

(3) Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an Behörden der Staatsanwaltschaft, Polizeibehörden, Landesfinanzbehörden, soweit diese personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, Verfassungsschutzbehörden des Bundes und der Länder, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig. Dies gilt für die Erhebung von personenbezogenen Daten bei den in Satz 1 genannten Behörden entsprechend.

(4) Im Fall der eingeschränkten Benachrichtigung gemäß Absatz 2 gilt § 54 Absatz 6 entsprechend. Die Justizvollzugsbehörden dokumentieren die Gründe für die Entscheidung nach Absatz 2.

§ 54**Auskunftsrecht der betroffenen Personen**

(1) Die Justizvollzugsbehörden erteilen den betroffenen Personen auf Antrag Auskunft darüber, ob sie diese Personen betreffende personenbezogene Daten verarbeiten. Bei einer Datenverarbeitung nach Satz 1 haben betroffene Personen 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 zur 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,
5. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
6. das Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung der Daten durch die Justizvollzugsbehörden,
7. das Recht, die Landesbeauftragte für Datenschutz oder den Landesbeauftragten für Datenschutz anzurufen, sowie
8. Angaben zu den Kontaktdaten 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 betroffenen Personen keine Angaben machen, die das Auffinden der Daten ermöglichen, obwohl ihnen das möglich und zumutbar wäre, und deshalb der für die Erteilung der Auskunft erforderliche Aufwand, insbesondere bei nicht-automatisierten Verfahren, außer Verhältnis zu dem von den betroffenen Personen geltend gemachten Informationsinteresse steht.

(4) Die Justizvollzugsbehörden dürfen unter den Voraussetzungen des § 53 Absatz 2 und 3 von einer Auskunft absehen, diese aufschieben oder einschränken.

(5) Die Justizvollzugsbehörden unterrichten die betroffenen Personen unverzüglich schriftlich über das Absehen von oder die Einschränkung einer Auskunft. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung, einen Nachteil oder eine Beeinträchtigung im Sinne des § 53 Absatz 2 mit sich bringen würde. 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.

(6) Werden die betroffenen Personen nach Absatz 5 über das Absehen von oder die Einschränkung der Auskunft unterrichtet, können sie ihr Auskunftsrecht auch über die Landesbeauftragte für Datenschutz oder den Landesbeauftragten für Datenschutz ausüben. Die Justizvollzugsbehörden unterrichten die betroffenen Personen über diese Möglichkeit sowie darüber, dass sie die Landesbeauftragte für Datenschutz oder den Landesbeauftragten für Datenschutz anrufen oder gerichtlichen Rechtsschutz suchen können. Machen die betroffenen Personen von ihrem Recht nach Satz 1 Gebrauch, ist die Auskunft auf ihr Verlangen der oder dem Landesbeauftragten für Datenschutz zu erteilen. Die oder der Landesbeauftragte für Datenschutz unterrichtet die betroffenen Personen darüber, dass alle erforderlichen Prüfungen erfolgt sind oder eine Überprüfung durch sie oder ihn stattgefunden hat. Diese Mitteilung kann die Information enthalten, dass datenschutzrechtliche Verstöße festgestellt wur-

den, darf jedoch Rückschlüsse auf den Erkenntnisstand der Justizvollzugsbehörden nicht zulassen, soweit diese keiner weitergehenden Auskunft zustimmen. Die Justizvollzugsbehörden dürfen die Zustimmung nur soweit und solange verweigern, wie sie nach Absatz 4 von einer Auskunft absehen oder sie einschränken können. Die oder der Landesbeauftragte für Datenschutz unterrichtet zudem die betroffenen Personen über ihr Recht auf gerichtlichen Rechtsschutz.

(7) Die Auskunft kann auch durch die Gewährung von Akteneinsicht oder die Aushändigung von Kopien oder Ausdrucken erteilt werden. Dabei ist das Interesse der Gefangenen und anderer betroffener Personen an einer bestimmten Form der Auskunftserteilung zu berücksichtigen.

(8) Die Justizvollzugsbehörden dokumentieren die Gründe für die Entscheidung.

§ 55 Akteneinsichtsrecht

(1) Betroffene Personen erhalten auf Antrag Akteneinsicht, soweit eine Auskunft für die Wahrnehmung ihrer rechtlichen Interessen nicht ausreicht, die Einsichtnahme hierfür unbedingt erforderlich ist und überwiegende berechnigte Interessen Dritter nicht entgegenstehen. Soweit Aktenbestandteile mit einem Sperrvermerk versehen sind, unterliegen sie nicht der Akteneinsicht.

(2) Betroffene Personen können auf eigene Kosten bei einer Einsicht hinzuziehen

1. eine Person aus dem Kreis

a) der Rechtsanwältinnen und Rechtsanwälte,

b) der Notarinnen und Notare,

c) der gewählten Verteidigerinnen und Verteidiger (§ 138 Absatz 1 und 2 der Strafprozessordnung),

d) der durch richterliche Entscheidung nach § 149 Absatz 1 oder 3 der Strafprozessordnung zugelassenen Beistände oder

e) der Beistände nach § 69 des Jugendgerichtsgesetzes,

2. Personensorgeberechnigte sowie

3. eine allgemein beedigte Dolmetscherin oder einen allgemein beedigten Dolmetscher.

Die betroffenen Personen können ihr Akteneinsichtsrecht auch durch eine Person aus dem in Satz 1 Nummer 1 und 2 genannten Personenkreis allein ausüben lassen (Akteneinsicht durch Beauftragte). Eine Hinzuziehung oder Beauftragung anderer Gefangener ist unzulässig, auch wenn diese zu dem in Satz 1 genannten Personenkreis gehören.

(3) Bei einer Einsichtnahme haben die betroffenen Personen das Recht, sich aus den Akten Notizen zu machen.

(4) Den betroffenen Personen sind aus den über sie geführten Akten oder Dateisystemen auf schriftlichen Antrag Ablichtungen oder Ausdrücke einzelner Dokumente zu überlassen, soweit ein berechnigtes Interesse vorliegt. Ein solches Interesse ist insbesondere anzunehmen, wenn die betroffenen Personen zur Geltendmachung von Rechten gegenüber Gerichten und Behörden auf Ablichtungen oder Ausdrücke angewiesen sind.

(5) Die Akteneinsicht ist unentgeltlich. Die Fertigung von Ablichtungen und Ausdrucken ist gebührenpflichtig. Die betroffenen Personen entrichten die zu erwartenden Kosten im Voraus. Sind die Gefangenen dazu nicht in der Lage, können die Justizvollzugsbehörden die Kosten in begründeten Fällen in angemessenem Umfang übernehmen.

§ 56

Auskunft und Akteneinsicht in Gesundheitsakten

Die Gefangenen erhalten auf Antrag Auskunft aus ihren oder Einsicht in ihre Gesundheitsakten. Für das Recht auf Akteneinsicht gilt § 55 Absatz 1 Satz 2, Absatz 2, 3 und 5 entsprechend.

§ 57

Sperrvermerke

(1) Sperrvermerke dürfen nur angebracht werden, soweit dies

1. aus medizinischen Gründen allein zum Wohl der Gefangenen,
2. zum Schutz überwiegender schutzwürdiger Interessen sowie von Leib oder Leben Dritter oder
3. aufgrund einer Rechtsvorschrift, die zur Geheimhaltung verpflichtet, und auch unter Berücksichtigung des Informationsinteresses der betroffenen Personen zwingend erforderlich ist. Der Sperrvermerk gemäß Satz 1 Nummer 1 wird von den Berufsheimlichkeitsgeheimnisträgerinnen und Berufsheimlichkeitsgeheimnistägern angebracht, die die zu sperrenden Aktenbestandteile zur Akte verfügt haben; die übrigen Sperrvermerke bringt die Anstaltsleiterin oder der Anstaltsleiter an.

(2) Der Grund und der Umfang der Sperrung sind in der Akte zu vermerken. Dieser Vermerk nimmt an der Sperrung teil. Gesperrte Aktenbestandteile sind gesondert von den übrigen Akten zu verwahren, soweit die Akten in Papierform geführt werden; im Übrigen sind sie besonders zu sichern.

§ 58

Verfahren für die Ausübung der Rechte der betroffenen Personen

(1) Die Justizvollzugsbehörden kommunizieren mit den betroffenen Personen in präziser, verständlicher und leicht zugänglicher Form und verwenden hierbei eine klare und einfache Sprache. Unbeschadet besonderer Formvorschriften sollen sie bei der Beantwortung von Anträgen die für den Antrag gewählte Form verwenden.

(2) Die Justizvollzugsbehörden informieren die betroffenen Personen unverzüglich schriftlich darüber, wie mit ihrem Antrag verfahren wurde. § 54 Absatz 5 und § 62 Absatz 3 bleiben unberührt.

(3) Die Erteilung von allgemeinen Informationen nach § 51, die Aufklärungspflicht bei der Datenerhebung nach § 52, die Benachrichtigungen nach den §§ 53 und 64 Absatz 1 Satz 2 Nummer 1 zweiter Teilsatz und die Bearbeitung von Anträgen nach den §§ 54 und 62 erfolgen gebührenfrei. Bei offenkundig unbegründeten oder exzessiven Anträgen nach den §§ 54, 55 und 62 können die Justizvollzugsbehörden es ablehnen, aufgrund des Antrags tätig zu werden. In diesem Fall müssen die Justizvollzugsbehörden den offenkundig unbegründeten oder exzessiven Charakter des Antrags belegen können.

(4) Haben die Justizvollzugsbehörden begründete Zweifel an der Identität einer betroffenen Person, die einen Antrag nach den §§ 54 oder 62 gestellt hat, können sie von ihr zusätzliche Informationen anfordern, die zur Bestätigung ihrer Identität erforderlich sind.

Abschnitt 9

Löschung, Einschränkung der Verarbeitung und Berichtigung

§ 59

Löschung

(1) Personenbezogene Daten sind zu löschen, soweit ihre weitere Verarbeitung nicht mehr zulässig oder aus anderem Grund

1. für die Erfüllung vollzuglicher Zwecke oder
 2. für die Durchführung wissenschaftlicher Forschungsvorhaben gemäß § 22 oder statistische Zwecke
- nicht erforderlich ist.

(2) Die Erforderlichkeit der Löschung ist jährlich oder aus Anlass einer Einzelfallbearbeitung zu kontrollieren. Die Frist zur Kontrolle personenbezogener Daten nach Satz 1 beginnt mit der Entlassung oder Verlegung der Gefangenen in eine andere Anstalt oder jede andere dauerhafte Unterbringung, in sonstigen Fällen mit Erhebung der personenbezogenen Daten. Unrechtmäßig verarbeitete Daten sind unverzüglich zu löschen.

(3) Personenbezogene Daten sind spätestens fünf Jahre nach der Entlassung oder der Verlegung der Gefangenen zu löschen; im Vollzug der Jugendstrafe beträgt die Frist drei Jahre und beim Jugendarrest zwei Jahre. Hiervon können bis zum Ablauf der Aufbewahrungsfrist für die Gefangenenpersonalakte die Angaben über Familienname, Vorname, Geburtsname, Geburtstag, Geburtsort, Eintritts- und Austrittsdatum der Gefangenen ausgenommen werden, soweit dies für das Auffinden der Gefangenenpersonalakte erforderlich ist.

(4) Soweit die Justizvollzugsbehörden im Vollzug der Untersuchungshaft und einer der Freiheitsentziehungen nach § 1 Absatz 1 Nummer 2 von einer nicht nur vorläufigen Einstellung des Verfahrens, einer unanfechtbaren Ablehnung der Eröffnung des Hauptverfahrens oder einem rechtskräftigen Freispruch Kenntnis erlangen, haben sie die personenbezogenen Daten unverzüglich zu löschen. Darüber hinaus sind in diesen Fällen auf Antrag der Gefangenen die Stellen, die eine Mitteilung nach § 20 erhalten haben, über den Verfahrensausgang in Kenntnis zu setzen. Die Gefangenen sind auf ihr Antragsrecht bei der Anhörung oder der nachträglichen Unterrichtung (§ 20 Absatz 6) hinzuweisen.

§ 60

Einschränkung der Verarbeitung

(1) Statt die gespeicherten personenbezogenen Daten zu löschen, ist deren Verarbeitung einzuschränken, wenn dies erforderlich ist,

1. weil tatsächliche Anhaltspunkte zur Gefahrenverhütung, zur Gefahrenabwehr, zur Verhinderung und Verfolgung von Straftaten oder zur Erreichung der in § 10 Absatz 2 Nummer 1 genannten Zwecke bestehen,
2. zur Feststellung, Durchsetzung oder Abwehr von Rechtsansprüchen im Zusammenhang mit dem Justizvollzug,
3. weil Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen betroffener Personen beeinträchtigt werden können,
4. zu sonstigen Beweis Zwecken oder
5. weil einer Löschung nach § 59 die Aufbewahrungsfrist einer anderen Rechtsnorm entgegensteht.

Der Zweck der Einschränkung der Verarbeitung ist zu dokumentieren.

(2) In ihrer Verarbeitung nach Absatz 1 eingeschränkte Daten dürfen nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand; sie dürfen auch verarbeitet werden, soweit dies zur Behebung einer Beweisnot oder zur Verfolgung von Straftaten unerlässlich ist oder die betroffenen Personen einwilligen. 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. Der Verarbeitungszweck ist zu dokumentieren sowie im Fall der Übermittlung der Empfänger.

(3) Die Verarbeitung personenbezogener Daten ist abweichend von Absatz 2 wieder uneingeschränkt möglich und die Einschränkung der Verarbeitung ist aufzuheben, wenn

1. die betroffenen Personen eingewilligt haben oder
2. die Gefangenen erneut in den Justizvollzug aufgenommen werden.

(4) Nach Absatz 1 in der Verarbeitung eingeschränkte Daten dürfen nicht über zehn Jahre hinaus aufbewahrt werden. Dies gilt nicht, wenn konkrete Anhaltspunkte dafür vorliegen, dass die Aufbewahrung für die in Absatz 1 genannten Zwecke weiterhin erforderlich ist. Die Aufbewahrungsfrist beginnt mit dem auf das Jahr der Weglegung folgenden Kalenderjahr. Die Bestimmungen des Landesarchivgesetzes bleiben unberührt. Für die Aufbewahrung von Akten mit nach den Vorschriften dieses Gesetzes in der Verarbeitung eingeschränkten Daten gelten die Regelungen der Schriftgutaufbewahrungsverordnung der Justiz des Saarlandes.

§ 61 Berichtigung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig, unvollständig oder nicht mehr aktuell sind. Bei Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder Beurteilung. Soweit dies mit angemessenem Aufwand möglich ist, sind die personenbezogenen Daten vor ihrer Verarbeitung auf Richtigkeit, Vollständigkeit und Aktualität zu überprüfen. In Akten genügt es, in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt oder aus welchem Grund sie unrichtig waren oder unrichtig geworden sind. Eine Vervollständigung personenbezogener Daten kann auch mittels einer ergänzenden Erklärung erfolgen.

(2) Kann die Richtigkeit oder Unrichtigkeit der personenbezogenen Daten nicht festgestellt werden, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. Vor der Aufhebung der Einschränkung sind die betroffenen Personen zu unterrichten.

§ 62 Rechte der betroffenen Personen auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

(1) Die betroffenen Personen haben das Recht, von den Justizvollzugsbehörden unverzüglich die Berichtigung sie betreffender unrichtiger Daten gemäß § 61 zu verlangen. Die betroffenen Personen können zudem die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist.

(2) Die betroffenen Personen können unter den Voraussetzungen von § 59 die Löschung der Daten verlangen.

(3) Die Justizvollzugsbehörden unterrichten die betroffenen Personen schriftlich über ein Absehen von der Berichtigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 53 Absatz 2 mit sich bringen würde. 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. § 54 Absatz 6 und 8 gilt entsprechend.

§ 63 Mitteilungen

(1) Die Justizvollzugsbehörden teilen die Berichtigung personenbezogener Daten der Stelle mit, die sie ihnen zuvor übermittelt hat. Gleiches gilt in den Fällen der Löschung oder Einschränkung der Verarbeitung wegen unzulässiger Verarbeitung oder der Berichtigung der Daten für die Empfänger von Daten. Die Empfänger haben die Daten in eigener Verantwortung zu löschen, ihre Verarbeitung einzuschränken oder zu berichtigen.

(2) Die Einhaltung der vorgenannten Maßgaben ist durch geeignete technische oder organisatorische Vorkehrungen sicherzustellen.

Abschnitt 10 Anwendung weiterer Vorschriften

§ 64 Anwendung weiterer Vorschriften des allgemeinen Datenschutzrechts

(1) Soweit in diesem Gesetz nicht etwas Abweichendes geregelt ist, gilt das allgemeine Datenschutzrecht. Insbesondere finden die Vorschriften für

1. die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (§ 3 Absatz 1 des Saarländischen Datenschutzgesetzes vom 16. Mai 2018 (Amtsblatt S. 254); Artikel 33 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) und die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen (§§ 3 Absatz 1, 12 Saarländisches Datenschutzgesetz; Artikel 34 Datenschutz-Grundverordnung),
2. die Benennung, Bestellung und die Aufgaben der behördlichen Datenschutzbeauftragten (§ 3 Absatz 1 Saarländisches Datenschutzgesetz; Artikel 37 bis 39 Datenschutz-Grundverordnung),
3. die Übermittlung von personenbezogenen Daten an Stellen in Drittstaaten oder an internationale Organisationen (§ 3 Absatz 1 Saarländisches Datenschutzgesetz; Artikel 44 bis 50 Datenschutz-Grundverordnung),
4. die datenschutzrechtliche Aufsicht über die Justizvollzugsbehörden durch die oder den Landesbeauftragten für Datenschutz (§§ 16 bis 20 Saarländisches Datenschutzgesetz),
5. den Anspruch auf Schadensersatz, Entschädigung (§ 3 Absatz 1 Saarländisches Datenschutzgesetz; Artikel 82 Datenschutz-Grundverordnung) und die Sanktionen (§ 27 Saarländisches Datenschutzgesetz),
6. die Anrufung der oder des Landesbeauftragten für Datenschutz (§ 3 Absatz 1 Saarländisches Datenschutzgesetz; Artikel 77 Datenschutz-Grundverordnung) und den Rechtsschutz

gegen deren oder dessen Entscheidungen (§§ 3 Absatz 1, 26 Saarländisches Datenschutzgesetz; Artikel 78 Datenschutz-Grundverordnung) entsprechende Anwendung.

(2) Für die Verarbeitung personenbezogener Daten durch Justizvollzugsbehörden im sachlichen Anwendungsbereich der Datenschutz-Grundverordnung gelten deren Bestimmungen und die hierzu erlassenen Vorschriften, soweit dieses Gesetz keine spezielleren Vorschriften enthält.

Artikel 2

Änderung des Saarländischen Strafvollzugsgesetzes

Das Saarländische Strafvollzugsgesetz in der Fassung der Bekanntmachung vom 24. April 2013 (Amtsbl. I S. 116), geändert durch das Gesetz vom 21. Januar 2015 (Amtsbl. I S. 187) wird wie folgt geändert:

1. Die Inhaltsangabe zu § 60 wird wie folgt gefasst:

„§ 60 Zweckgebundene Einzahlungen, Eingliederungsgeld“

2. § 60 wird wie folgt geändert:

a) In der Überschrift wird „, Eingliederungsgeld“ angefügt.

b) Es wird folgender Absatz 2 angefügt:

„(2) Die Gefangenen dürfen für Zwecke der Vorbereitung der Eingliederung ein Guthaben in angemessener Höhe bilden (Eingliederungsgeld). Sie dürfen auch bereits vor der Entlassung über das Eingliederungsgeld verfügen. Das Geld darf nur für Zwecke der Vorbereitung der Eingliederung verwendet werden. Der Anspruch auf Auszahlung ist nicht übertragbar.“

3. Dem § 78 Absatz 2 werden folgende Sätze angefügt:

„Eine Fesselung, durch die die Bewegungsfreiheit weitgehend aufgehoben wird (Fixierung), ist nur zulässig, soweit und solange die gegenwärtige erhebliche Gefahr von Gewalttätigkeiten gegen Personen, der Selbsttötung oder der Selbstverletzung besteht und die Fixierung zur Abwehr dieser Gefahr unerlässlich ist. Für die Fixierung ist ein Gurtsystem zu verwenden.“

4. Dem § 79 Absatz 1 werden folgende Sätze angefügt:

„Eine Fixierung, die nicht nur kurzfristig ist, ist auf Antrag der Anstaltsleitung nur aufgrund vorheriger richterlicher Anordnung zulässig. Bei Gefahr im Verzug können auch die Anstaltsleitung oder andere Bedienstete die Fixierung vorläufig anordnen; die richterliche Entscheidung ist unverzüglich einzuholen. Wurde die Fixierung vor Erlangung einer richterlichen Entscheidung beendet, so ist dies dem Gericht unverzüglich mitzuteilen.“

5. Dem § 79 Absatz 3 wird folgender Satz angefügt:

„Bei einer Fixierung sind die Anordnung und die dafür maßgeblichen Gründe sowie der Verlauf, die Art der Überwachung und die Beendigung umfassend zu dokumentieren.“

6. In § 79 Absatz 5 wird folgender Satz 1 vorangestellt:

„Eine Fixierung ist unverzüglich mitzuteilen.“

7. § 79 Absatz 6 wird wie folgt neu gefasst:

„(6) Während der Absonderung, der Unterbringung im besonders gesicherten Haftraum und der Fixierung sind die Gefangenen in besonderem Maße zu betreuen. Sind die Gefangenen fixiert, sind sie durch eine geschulte Bedienstete oder einen geschulten Bediensteten ständig und in unmittelbarem Sichtkontakt zu beobachten.“

8. § 79 wird folgender Absatz 7 angefügt:

„(7) Nach Beendigung der Fixierung sind die Gefangenen auf ihr Recht hinzuweisen, die Rechtmäßigkeit der durchgeführten Fixierung gerichtlich überprüfen zu lassen. Der Hinweis ist aktenkundig zu machen.“

Artikel 3

Änderung des Saarländischen Jugendstrafvollzugsgesetzes

Das Saarländische Jugendstrafvollzugsgesetz vom 30. Oktober 2007 (Amtsbl. S. 2370), zuletzt geändert durch das Gesetz vom 24. April 2013 (Amtsbl. I S. 116) wird wie folgt geändert:

1. Die Inhaltsangabe zu § 61 wird wie folgt gefasst:

„§ 61 Eigengeld, Zweckgebundene Einzahlungen, Eingliederungsgeld“

2. § 61 wird wie folgt geändert:

a) In der Überschrift wird „, Eingliederungsgeld“ angefügt.

b) Es wird folgender Absatz 4 angefügt:

„(4) Die Gefangenen dürfen für Zwecke der Vorbereitung der Eingliederung ein Guthaben in angemessener Höhe bilden (Eingliederungsgeld). Sie dürfen auch bereits vor der Entlassung über das Eingliederungsgeld verfügen. Das Geld darf nur für Zwecke der Vorbereitung der Eingliederung verwendet werden. Der Anspruch auf Auszahlung ist nicht übertragbar.“

3. Dem § 70 Absatz 2 werden folgende Sätze angefügt:

„Eine Fesselung, durch die die Bewegungsfreiheit weitgehend aufgehoben wird (Fixierung), ist nur zulässig, soweit und solange die gegenwärtige erhebliche Gefahr von Gewalttätigkeiten gegen Personen, der Selbsttötung oder der Selbstverletzung besteht und die Fixierung zur Abwehr dieser Gefahr unerlässlich ist. Für die Fixierung ist ein Gurtsystem zu verwenden.“

4. In § 71 wird Satz 4 wie folgt gefasst:

„Sind die Gefangenen fixiert, sind sie durch eine geschulte Bedienstete oder einen geschulten Bediensteten ständig und in unmittelbarem Sichtkontakt zu beobachten.“

5. Dem § 73 Absatz 1 werden folgende Sätze angefügt:

„Eine Fixierung, die nicht nur kurzfristig ist, ist auf Antrag der Anstaltsleitung nur aufgrund vorheriger richterlicher Anordnung zulässig. Bei Gefahr im Verzug können auch die Anstaltsleitung oder andere Bedienstete die Fixierung vorläufig anordnen; die richterliche Entscheidung ist unverzüglich einzuholen. Wurde die Fixierung vor Erlangung einer richterlichen Entscheidung beendet, so ist dies dem Gericht unverzüglich mitzuteilen.“

6. Dem § 73 Absatz 3 wird folgender Satz angefügt:

„Bei einer Fixierung sind die Anordnung und die dafür maßgeblichen Gründe sowie der Verlauf, die Art der Überwachung und die Beendigung umfassend zu dokumentieren.“

7. In § 73 Absatz 5 wird folgender Satz 2 angefügt:

„Eine Fixierung ist unverzüglich mitzuteilen.“

8. § 73 wird folgender Absatz 6 angefügt:

„(6) Nach Beendigung der Fixierung sind die Gefangenen auf ihr Recht hinzuweisen, die Rechtmäßigkeit der durchgeführten Fixierung gerichtlich überprüfen zu lassen. Der Hinweis ist aktenkundig zu machen.“

Artikel 4

Änderung des Saarländischen Untersuchungshaftvollzugsgesetzes

Das Saarländische Untersuchungshaftvollzugsgesetz vom 1. Juli 2009 (Amtsbl. S. 1219), zuletzt geändert durch das Gesetz vom 13. Oktober 2015 (Amtsbl. I S. 790) wird wie folgt geändert:

1. Dem § 49 Absatz 2 werden folgende Sätze angefügt:

„Eine Fesselung, durch die die Bewegungsfreiheit weitgehend aufgehoben wird (Fixierung), ist nur zulässig, soweit und solange die gegenwärtige erhebliche Gefahr von Gewalttätigkeiten gegen Personen, der Selbsttötung oder der Selbstverletzung besteht und die Fixierung zur Abwehr dieser Gefahr unerlässlich ist. Für die Fixierung ist ein Gurtsystem zu verwenden.“

2. In § 50 wird Satz 4 wie folgt gefasst:

„Sind die Untersuchungsgefangenen fixiert, sind sie durch eine geschulte Bedienstete oder einen geschulten Bediensteten ständig und in unmittelbarem Sichtkontakt zu beobachten.“

3. Dem § 52 Absatz 1 werden folgende Sätze angefügt:

„Eine Fixierung, die nicht nur kurzfristig ist, ist auf Antrag der Anstaltsleitung nur aufgrund vorheriger richterlicher Anordnung zulässig. Bei Gefahr im Verzug können auch die Anstaltsleitung oder andere Bedienstete die Fixierung vorläufig anordnen; die richterliche Entscheidung ist unverzüglich einzuholen. Wurde die Fixierung vor Erlangung einer richterlichen Entscheidung beendet, so ist dies dem Gericht unverzüglich mitzuteilen.“

4. Dem § 52 Absatz 3 wird folgender Satz angefügt:

„Bei einer Fixierung sind die Anordnung und die dafür maßgeblichen Gründe sowie der Verlauf, die Art der Überwachung und die Beendigung umfassend zu dokumentieren.“

5. In § 52 Absatz 5 wird folgender Satz 3 angefügt:

„Eine Fixierung ist unverzüglich der Aufsichtsbehörde, dem Gericht und der Staatsanwaltschaft mitzuteilen. Absatz 1 Satz 3 bis 4 bleibt unberührt.“

6. § 52 wird folgender Absatz 6 angefügt:

„(6) Nach Beendigung der Fixierung sind die Untersuchungsgefangenen auf ihr Recht hinzuweisen, die Rechtmäßigkeit der durchgeführten Fixierung gerichtlich überprüfen zu lassen. Der Hinweis ist aktenkundig zu machen.“

Artikel 5

Änderung des Gesetzes zur ambulanten Resozialisierung und Opferhilfe

Das Gesetz zur ambulanten Resozialisierung und Opferhilfe vom 21. Januar 2015 (Amtsbl. I S. 187) wird wie folgt geändert:

1. § 26 wird wie folgt gefasst:

„§ 26

Vorrang des Bundesrechts; Anwendung des Saarländischen Datenschutzgesetzes und des Saarländischen Justizvollzugsdatenschutzgesetzes

Die Vorschriften dieses Abschnitts kommen zur Anwendung, soweit die Verarbeitung von Daten durch die ambulanten sozialen Dienste der Justiz nicht durch Bundesrecht ausdrücklich im Einzelnen geregelt ist. Durch Bundesrecht begründete Kompetenzen zur Verarbeitung von Daten bleiben ebenso unberührt wie das Gesetz über die Zustimmung zum Beitritt zum Staatsvertrag der Länder Baden-Württemberg, Bayern, Hessen und Nordrhein-Westfalen über die Einrichtung einer Gemeinsamen Überwachungsstelle der Länder vom 20. Juni 2012 (Amtsbl. S. 338). Die Bestimmungen des Saarländischen Justizvollzugsdatenschutzgesetzes finden entsprechende Anwendung, insbesondere im Hinblick auf die Begriffsbestimmungen, die Rechte der betroffenen Personen und die Anwendung weiterer Vorschriften des allgemeinen Datenschutzrechts, soweit nicht die nachfolgenden Regelungen Abweichendes bestimmen.“

2. § 27 wird wie folgt gefasst:

„§ 27

Zulässigkeit der Datenverarbeitung; Einwilligung

(1) Das Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe und das Ministerium der Justiz als für die Dienst- und Fachaufsicht zuständige Behörde dürfen personenbezogene Daten verarbeiten, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies für den Anwendungsbereich dieses Gesetzes ausdrücklich erlaubt oder anordnet oder soweit die betroffenen Personen wirksam eingewilligt haben und der Datenverarbeitung kein ausdrückliches gesetzliches Verbot entgegensteht.

(2) Die Einwilligung gemäß Absatz 1 ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Personen beruht. Sie bedarf der Schriftform, soweit nicht ausnahmsweise der Umstände halber eine andere Form angemessen ist. Die betroffenen Personen sind

über den vorgesehenen Zweck der Verarbeitung zu unterrichten, bei beabsichtigten Übermittlungen auch über die beabsichtigten Empfänger sowie den Zweck der Übermittlung. Soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen sind sie auf die Folgen einer Verweigerung der Einwilligung hinzuweisen. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, so ist sie in der Gestaltung der Erklärung besonders hervorzuheben. Die betroffenen Personen haben das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffenen Personen sind vor Abgabe der Einwilligung hiervon in Kenntnis zu setzen. Soweit besondere Kategorien personenbezogener Daten (Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten und Daten zum Sexualleben oder zur sexuellen Orientierung) verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen. Bei beschränkt geschäftsfähigen Probandinnen und Probanden bestimmt sich die Einwilligungsfähigkeit nach der tatsächlichen Einsichtsfähigkeit.“

3. § 28 wird wie folgt gefasst:

„§ 28

Erhebung personenbezogener Daten

(1) Das Kompetenzzentrum für ambulante Resozialisierung und Opferhilfe und das Ministerium der Justiz als für die Dienst- und Fachaufsicht zuständige Behörde dürfen personenbezogene Daten erheben, soweit dies zur Erfüllung der ihnen durch dieses Gesetz oder durch Verordnung zugewiesenen Aufgaben erforderlich ist. Besondere Kategorien personenbezogener Daten dürfen sie nur erheben, soweit dies zur Aufgabenerfüllung unbedingt erforderlich ist.

(2) Personenbezogene Daten sind grundsätzlich bei den betroffenen Personen und mit deren Kenntnis und Mitwirkung zu erheben. Eine Erhebung personenbezogener Daten bei den betroffenen Personen ohne deren Kenntnis und Mitwirkung ist zulässig, wenn keine Anhaltspunkte dafür vorliegen, dass überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen.

(3) Soweit die Erhebung personenbezogener Daten nach Absatz 1 und 2 zulässig ist, dürfen sie auch bei Dritten erhoben werden, wenn

1. dies zur Aufgabenerfüllung nach Absatz 1 erforderlich ist,
2. eine Rechtsvorschrift dies ausdrücklich erlaubt oder anordnet,
3. Angaben der betroffenen Personen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
4. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist,
5. dies zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist,
6. sich die Erhebung auf Daten aus Akten der gerichtlichen Verfahren bezieht, die der Unterstellung der Bewährungshilfe oder Führungsaufsicht zugrunde liegen oder
7. keine Anhaltspunkte dafür vorliegen, dass überwiegende schutzwürdige Interessen der betroffenen Personen einer Erhebung ohne ihre Kenntnis entgegenstehen und
 - a) die betroffenen Personen einer durch Rechtsvorschrift festgelegten Auskunftspflicht nicht nachgekommen und über die beabsichtigte Erhebung bei Dritten unterrichtet worden sind,
 - b) die Erhebung bei den betroffenen Personen einen unverhältnismäßigen Aufwand erfordern würde oder
 - c) die Daten allgemein zugänglich sind.

(4) Soweit die Erhebung personenbezogener Daten über Probandinnen und Probanden nach Absatz 1 und 2 zulässig ist und diese nicht die für eine Einwilligung notwendige Einsichtsfähigkeit besitzen, dürfen personenbezogene Daten auch bei deren gesetzlichen Vertreterinnen und Vertretern erhoben werden.

(5) Nichtöffentliche Stellen sind auf die Rechtsvorschrift, die zur Auskunft verpflichtet, ansonsten auf die Freiwilligkeit ihrer Angaben hinzuweisen.“

4. § 29 wird wie folgt gefasst:

„§ 29

Verarbeitung personenbezogener Daten

(1) Das Kompetenzzentrum für ambulante Resozialisierung und Opferhilfe und das Ministerium der Justiz als für die Dienst- und Fachaufsicht zuständige Behörde dürfen personenbezogene Daten, die sie zulässig erhoben haben, für die erhobenen Zwecke verarbeiten, soweit dies zur Aufgabenerfüllung erforderlich ist.

(2) Das Kompetenzzentrum für ambulante Resozialisierung und Opferhilfe und das Ministerium der Justiz als für die Dienst- und Fachaufsicht zuständige Behörde dürfen personenbezogene Daten, die sie zulässig erhoben haben zu Zwecken, zu denen sie nicht erhoben wurden, nur verarbeiten, soweit

1. die Voraussetzungen vorliegen, die eine Erhebung von Daten nach § 28 Absatz 3 bei Dritten zulassen,
2. eine Rechtsvorschrift dies ausdrücklich erlaubt oder anordnet,
3. dies dem gerichtlichen Rechtsschutz, der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Automatisierung des Berichtswesens, der Rechnungsprüfung, der Durchführung von Organisationsuntersuchungen oder statistischen Zwecken dient und überwiegende schutzwürdige Interessen der betroffenen Personen nicht entgegenstehen,
4. dies erforderlich ist zur Abwehr von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten für eine fremde Macht oder von Bestrebungen in der Bundesrepublik Deutschland, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen
 - a) gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind,
 - b) eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben oder
 - c) auswärtige Belange der Bundesrepublik Deutschland gefährden,
5. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit erforderlich ist,
6. dies zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist,
7. dies zur Verhinderung oder Verfolgung von Straftaten, zur Vollstreckung von Strafen und Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs sowie zur Verhinderung oder Verfolgung von Ordnungswidrigkeiten, durch welche die Aufgabenerfüllung des Kompetenzzentrums für ambulante Resozialisierung und Opferhilfe gefährdet werden, erforderlich ist oder
8. dies für Maßnahmen der Strafvollstreckung oder strafvollstreckungsrechtliche Entscheidungen hinsichtlich der betroffenen Personen erforderlich ist.

(3) Das Verarbeiten von zulässig erhobenen besonderen Kategorien personenbezogener Daten für Zwecke, zu denen sie nicht erhoben wurden, ist nur zulässig, soweit dies zu den in Absatz 2 genannten Zwecken unbedingt erforderlich ist. Soweit die erhobenen besonderen Kategorien personenbezogener Daten einem Amts- oder Berufsgeheimnis unterliegen und von den zur Verschwiegenheit Verpflichteten in Ausübung ihrer Amts- oder Berufspflicht er-

langt wurden, dürfen sie, soweit dieses Gesetz nichts anderes bestimmt, nur für den Zweck gespeichert oder genutzt werden, für den die zur Verschwiegenheit Verpflichteten sie erhalten haben.

(4) Sind mit personenbezogenen Daten, die nach Absatz 1 oder Absatz 2 verarbeitet werden dürfen, weitere personenbezogene Daten von betroffenen Personen oder von Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unververtretbarem Aufwand möglich ist, ist die Speicherung auch dieser Daten zulässig, soweit nicht berechnete Interessen von betroffenen Personen oder Dritten an deren Geheimhaltung offensichtlich überwiegen. Eine Nutzung dieser Daten ist unzulässig.

(5) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert oder genutzt werden, dürfen für andere Zwecke nur insoweit genutzt werden, als dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit, insbesondere für Leben, Gesundheit oder Freiheit, sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist. Für die weitere Verarbeitung von Protokolldaten gilt § 32d Absatz 3.“

5. § 31 wird wie folgt gefasst:

„§ 31
Zweckbindung

Empfänger dürfen personenbezogene Daten nur zu dem Zweck speichern, nutzen und übermitteln, zu dessen Erfüllung sie übermittelt wurden. Für andere Zwecke dürfen sie diese Daten nur speichern, nutzen und übermitteln, soweit sie ihnen auch für diese Zwecke hätten überlassen werden dürfen und wenn im Fall einer Übermittlung an eine nichtöffentliche Stelle das Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe zugestimmt hat. Dieses hat die Empfänger auf die Zweckbindung nach den Sätzen 1 und 2 hinzuweisen.“

6. § 32 wird wie folgt gefasst:

„§ 32
Schutzvorkehrungen

(1) Personenbezogene Daten in Akten und Dateien sind gegen unbefugten Zugang, unbefugte Offenlegung und unbefugten Gebrauch, sowie vor Vernichtung, Verlust und Veränderung, ob unbeabsichtigt oder unrechtmäßig, zu schützen. Für Art und Umfang der hierzu erforderlichen technischen und organisatorischen Maßnahmen gelten §§ 32a bis 32c.

(2) Soweit nichts anderes geregelt ist, dürfen sich die Bediensteten von personenbezogenen Daten nur Kenntnis verschaffen, wenn dies zur Erfüllung der ihnen obliegenden Aufgaben erforderlich ist.“

7. Nach § 32 werden die folgenden §§ 32 a bis 32 i eingefügt:

„§ 32a
Verzeichnis von Verarbeitungstätigkeiten

(1) Das Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe hat ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die in seine Zuständigkeit fallen. Dieses Verzeichnis hat die folgenden Angaben zu enthalten:

1. die Kontaktdaten des Kompetenzzentrums der Justiz für ambulante Re-sozialisierung und Opferhilfe und den Namen sowie die Kontaktdaten der oder des Datenschutzbeauftragten,

2. die Zwecke der Verarbeitung,
3. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
4. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen,
5. die Kategorien von Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,
6. die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten,
7. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 32b,
8. die Rechtsgrundlage der Verarbeitung und
9. die Verwendung von Profiling.

(2) Das in Absatz 1 genannte Verzeichnis ist schriftlich oder in einem elektronischen Format zu führen. Auf Anforderung ist es der Landesbeauftragten für Datenschutz oder dem Landesbeauftragten für Datenschutz zur Verfügung zu stellen.

§ 32b

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Das Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen, 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 vom Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe zu treffenden technischen und organisatorischen Maßnahmen gewährleisten, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
4. personenbezogene Daten jederzeit ihrem Ursprung zugeordnet werden können (Authentizität),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz),
7. personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck verarbeitet werden können, sofern nicht eine Rechtsvorschrift dies erlaubt oder anordnet, (Nicht-Verkettbarkeit) und
8. Verfahren so gestaltet werden, dass sie den betroffenen Personen die Ausübung der in den §§ 32h genannten Rechte wirksam ermöglichen (Intervenierbarkeit).

(3) Zur Umsetzung der Maßnahmen nach Absatz 2 ergreift das Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe im Fall einer automatisierten Verarbeitung nach einer Risikobewertung Maßnahmen, 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 Störfall 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) und
 14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).
- Ein Zweck nach Satz 1 Nummer 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

(4) Das Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden können, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Dies betrifft die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Die Maßnahmen müssen insbesondere gewährleisten, dass die Daten durch Voreinstellungen nicht automatisch einer unbestimmten Anzahl von Personen zugänglich gemacht werden können.

(5) Die zu treffenden technischen und organisatorischen Maßnahmen sind auf der Grundlage eines zu dokumentierenden Sicherheitskonzepts zu ermitteln, zu dessen Bestandteilen die Abschätzung von Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für das Recht auf informationelle Selbstbestimmung gehört. Die Wirksamkeit der Maßnahmen ist unter Berücksichtigung sich verändernder Rahmenbedingungen und Entwicklungen der Technik zu überprüfen. Die sich daraus ergebenden notwendigen Anpassungen sind zeitnah umzusetzen, soweit dies mit einem angemessenen Aufwand möglich ist. § 32c bleibt unberührt.

§ 32c

Datenschutz-Folgenabschätzung bei hohem Risiko, Konsultationspflicht

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge, führt das Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen durch.

(2) Für mehrere ähnliche Verarbeitungsvorgänge mit ähnlich hohem Gefahrenpotential kann eine gemeinsame Datenschutz-Folgenabschätzung vorgenommen werden. Die behördlichen Datenschutzbeauftragten sind an der Durchführung der Datenschutz-Folgenabschätzung zu beteiligen.

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

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,
2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck,
3. eine Bewertung der Gefahren für die Rechtsgüter der betroffenen Personen und
4. die Maßnahmen, mit denen Gefahren abgewendet werden sollen, 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) Das Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe hat vor der Inbetriebnahme von neu anzulegenden Dateisystemen die Landesbeauftragte oder den Landesbeauftragten für Datenschutz anzuhören,

1. wenn aus einer Datenschutz Folgenabschätzung hervorgeht, dass die Verarbeitung eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge hätte, wenn das Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe 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 Personen zur Folge hat.

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

(5) Der oder dem Landesbeauftragten für Datenschutz sind im Fall des Absatzes 4 vorzulegen:

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

Auf Anforderung sind ihr oder ihm zudem alle sonstigen Informationen zu übermitteln, die sie oder er benötigt, um die Rechtmäßigkeit der Verarbeitung sowie insbesondere die in Bezug

auf den Schutz der personenbezogenen Daten der betroffenen Personen bestehenden Gefahren und die diesbezüglichen Garantien bewerten zu können.

(6) Falls die oder Landesbeauftragte für Datenschutz der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstoßen würde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder keine ausreichenden Abhilfemaßnahmen getroffen hat, kann sie oder er dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von sechs Wochen nach Einleitung der Anhörung schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergriffen werden sollten. Die oder der Landesbeauftragte für Datenschutz kann diese Frist um einen Monat verlängern, wenn die geplante Verarbeitung besonders komplex ist. 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.

(7) Hat die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung des Verantwortlichen und ist sie daher besonders dringlich, kann er mit der Verarbeitung nach Beginn der Anhörung, aber vor Ablauf der in Absatz 6 Satz 1 genannten Frist beginnen. 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.

§ 32d Protokollierung

(1) In automatisierten Verarbeitungssystemen sind die folgenden Verarbeitungsvorgänge zu protokollieren:

1. Erhebung und Speicherung,
2. Veränderung,
3. Abfrage,
4. Offenlegung einschließlich Übermittlung,
5. Kombination und
6. Löschung oder Einschränkung der Verarbeitung.

(2) Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen. Aus der Identität der Person muss sich auch die Begründung für eine Abfrage oder Offenlegung ableiten lassen.

(3) Die Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die behördlichen Datenschutzbeauftragten, die Landesbeauftragte für Datenschutz oder den Landesbeauftragten für Datenschutz sowie für die Eigenüberwachung und für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten verwendet werden. Die Protokolldaten dürfen auch zur Verfolgung von Straftaten oder für beamtenrechtliche oder disziplinarrechtliche Maßnahmen im Zusammenhang mit einer Verletzung des Datengeheimnisses sowie zur Verfolgung von Straftaten von erheblicher Bedeutung verarbeitet werden.

(4) Die Protokolldaten sind zwei Jahre nach ihrer Erstellung zu löschen.

(5) Die Protokolle sind der Landesbeauftragten für Datenschutz oder dem Landesbeauftragten für Datenschutz auf Anforderung zur Verfügung zu stellen.

§ 32e

Löschung

(1) Personenbezogene Daten sind zu löschen, soweit ihre weitere Verarbeitung nicht mehr zulässig oder aus anderem Grund

1. für die Erfüllung der Aufgaben des Kompetenzzentrums für ambulante Resozialisierung und Opferhilfe oder
2. für die Durchführung wissenschaftlicher Forschungsvorhaben oder statistische Zwecke nicht erforderlich ist.

(2) Die Erforderlichkeit der Löschung ist jährlich oder aus Anlass einer Einzelfallbearbeitung zu kontrollieren. Die Frist zur Kontrolle personenbezogener Daten nach Satz 1 beginnt mit dem Ende des Jahres, das auf das Jahr folgt, in dem

1. die letzte zur Bewährung ausgesetzte Freiheitsstrafe erlassen wird,
2. der Widerruf der Bewährung Rechtskraft erlangt oder
3. die Führungsaufsicht endet.

Im Übrigen mit dem Ende des Jahres in dem das Verfahren abgeschlossen worden ist. Unrechtmäßig verarbeitete Daten sind unverzüglich zu löschen.

(3) Personenbezogene Daten über Probandinnen und Probanden sind mit Ablauf des fünften Jahres zu löschen, das auf das Jahr folgt, in das das letzte der in Absatz 1 Nummer 1 bis 3 genannten Ereignisse fällt. Im Übrigen sind personenbezogene Daten über Probandinnen und Probanden mit Ablauf des zweiten Jahres zu löschen, das auf das Jahr folgt, in dem das Verfahren abgeschlossen worden ist. Dies gilt nicht soweit und solange die Probandinnen und Probanden in anderer Sache unter Bewährungsaufsicht oder Führungsaufsicht stehen oder soweit und solange gegen sie eine Freiheitsstrafe oder eine freiheitsentziehende Maßregel der Besserung und Sicherung vollzogen wird. Hiervon können bis zum Ablauf der Aufbewahrungsfrist für die Akte der Probandinnen und Probanden die Angaben über Familienname, Vorname, Geburtsname, Geburtstag, und Geburtsort ausgenommen werden, soweit dies für das Auffinden der Akte erforderlich ist.

§ 32f

Einschränkung der Verarbeitung

(1) Statt die gespeicherten personenbezogenen Daten zu löschen, ist deren Verarbeitung einzuschränken, wenn dies erforderlich ist,

1. weil tatsächliche Anhaltspunkte zur Gefahrenverhütung, zur Gefahrenabwehr, zur Verhinderung und Verfolgung von Straftaten oder zur Erreichung der in § 29 Absatz 2 Nummer 4 genannten Zwecke bestehen,
2. zur Feststellung, Durchsetzung oder Abwehr von Rechtsansprüchen im Zusammenhang mit den Aufgaben des Kompetenzzentrums für ambulante Resozialisierung und Opferhilfe ,
3. weil Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen betroffener Personen beeinträchtigt werden können,
4. zu sonstigen Beweis Zwecken,
5. weil einer Löschung nach § 32e die Aufbewahrungsfrist eine andere Rechtsnorm entgegensteht.

Der Zweck der Einschränkung der Verarbeitung ist zu dokumentieren.

(2) In ihrer Verarbeitung nach Absatz 1 eingeschränkte Daten dürfen nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand; sie dürfen auch verarbeitet werden, soweit dies zur Behebung einer Beweisnot oder zur Verfolgung von Straftaten unerlässlich ist oder die betroffenen Personen einwilligen. 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. Der Verarbeitungszweck ist zu dokumentieren sowie im Fall der Übermittlung der Empfänger.

(3) Die Verarbeitung personenbezogener Daten ist abweichend von Absatz 2 wieder uneingeschränkt möglich und die Einschränkung der Verarbeitung ist aufzuheben, wenn

1. die betroffenen Personen eingewilligt haben oder
2. die Probandinnen und Probanden erneut in den Zuständigkeitsbereich des Kompetenzzentrums für ambulante Resozialisierung und Opferhilfe aufgenommen werden.

(4) Nach Absatz 1 in der Verarbeitung eingeschränkte Daten dürfen nicht über zehn Jahre hinaus aufbewahrt werden. Dies gilt nicht, wenn konkrete Anhaltspunkte dafür vorliegen, dass die Aufbewahrung für die in Absatz 1 genannten Zwecke weiterhin erforderlich ist. Die Aufbewahrungsfrist beginnt mit dem auf das Jahr der Weglegung folgenden Kalenderjahr. Die Bestimmungen des Landesarchivgesetzes bleiben unberührt. Für die Aufbewahrung von Akten mit nach den Vorschriften dieses Gesetzes in der Verarbeitung eingeschränkten Daten gelten die Regelungen der Schriftgutaufbewahrungsverordnung der Justiz des Saarlandes.

§ 32g

Berichtigung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig, unvollständig oder nicht mehr aktuell sind. Bei Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder Beurteilung. Soweit dies mit angemessenem Aufwand möglich ist, sind die personenbezogenen Daten vor ihrer Verarbeitung auf Richtigkeit, Vollständigkeit und Aktualität zu überprüfen. In Akten genügt es, in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt oder aus welchem Grund sie unrichtig waren oder unrichtig geworden sind. Eine Vervollständigung personenbezogener Daten kann auch mittels einer ergänzenden Erklärung erfolgen.

(2) Kann die Richtigkeit oder Unrichtigkeit der personenbezogenen Daten nicht festgestellt werden, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. Vor der Aufhebung der Einschränkung sind die betroffenen Personen zu unterrichten.

§ 32h

Rechte der betroffenen Personen auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

(1) Die betroffenen Personen haben das Recht, vom Kompetenzzentrum für ambulante Resozialisierung und Opferhilfe unverzüglich die Berichtigung sie betreffender unrichtiger Daten gemäß § 32g zu verlangen. Die betroffenen Personen können zudem die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist.

(2) Die betroffenen Personen können unter den Voraussetzungen von § 32e die Löschung der Daten verlangen.

(3) Das Kompetenzzentrum für ambulante Resozialisierung und Opferhilfe unterrichtet die betroffenen Personen schriftlich über ein Absehen von der Berichtigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 53 Absatz 2 Justizvollzugsdatenschutzgesetz mit sich bringen würde. 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. § 54 Absatz 6 und 8 Justizvollzugsdatenschutzgesetz gilt entsprechend.

§ 32i Mitteilungen

(1) Das Kompetenzzentrum für ambulante Resozialisierung und Opferhilfe teilt die Berichtigung personenbezogener Daten der Stelle mit, die sie ihnen zuvor übermittelt hat. Gleiches gilt in den Fällen der Löschung oder Einschränkung der Verarbeitung wegen unzulässiger Verarbeitung oder der Berichtigung der Daten für die Empfänger von Daten. Die Empfänger haben die Daten in eigener Verantwortung zu löschen, ihre Verarbeitung einzuschränken oder zu berichtigen.

(2) Die Einhaltung der vorgenannten Maßgaben ist durch geeignete technische oder organisatorische Vorkehrungen sicherzustellen.“

Artikel 6

Änderung des Gesetzes über den Verfassungsgerichtshof

Das Gesetz über den Verfassungsgerichtshof in der Fassung der Bekanntmachung vom 6. Februar 2001 (Amtsbl. S. 582), zuletzt geändert durch das Gesetz vom 16. Juli 2014 (Amtsbl. I S. 358), wird wie folgt geändert:

1. In § 2 Absatz 3 Satz 6 werden die Wörter „und einem oberen Landesgericht angehören“ gestrichen.

2. In § 14a werden die Wörter „die Vorschriften des Saarländischen Datenschutzgesetzes“ durch die Wörter „die allgemeinen datenschutzrechtlichen Vorschriften“ ersetzt.

3. § 14b Absatz 1 Satz 1 wird wie folgt gefasst:

„Auskunft aus oder Einsicht in Akten des Verfassungsgerichtshofs kann gewährt werden

1. öffentlichen Stellen, soweit

a) dies für Zwecke der Rechtspflege erforderlich ist oder

b) eine der in § 7 Absatz 2 des Saarländischen Datenschutzgesetzes genannten Voraussetzungen vorliegt oder

c) dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann,

2. Privatpersonen und anderen nicht öffentlichen Stellen, soweit die in § 4 Absatz 3 Nummer 2 des Saarländischen Datenschutzgesetzes genannten Voraussetzungen vorliegen. Einer Unterrichtung des Betroffenen von der Übermittlung seiner Daten bedarf es nicht; die Erteilung der Auskunft und die Gewährung der Akteneinsicht sind in der Akte zu vermerken.“

4. § 14c wird wie folgt geändert:

a) In der Überschrift wird das Wort „Nutzung“ durch das Wort „Verarbeitung“ ersetzt.

b) Im Wortlaut wird das Wort „nutzen“ durch das Wort „verarbeiten“ ersetzt.

Artikel 7

Inkrafttreten, Außerkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am Tag nach der Verkündung in Kraft. Gleichzeitig treten der Gesetzestext und das Inhaltsverzeichnis zu Abschnitt 21 des Saarländischen Strafvollzugsgesetzes, der Gesetzestext und das Inhaltsverzeichnis zum 13. Abschnitt des Saarländischen Jugendstrafvollzugsgesetzes, der Gesetzestext und das Inhaltsverzeichnis zu Abschnitt 14 des Saarländischen Untersuchungshaftvollzugsgesetzes, der Gesetzestext und das Inhaltsverzeichnis zu Titel 14 des Saarländischen Jugendarrestvollzugsgesetzes und der Gesetzestext und das Inhaltsverzeichnis zu Abschnitt 4 des Saarländischen Sicherungsverwahrungsvollzugsgesetzes außer Kraft.

(2) § 42 des Saarländischen Justizvollzugsdatenschutzgesetzes tritt am 6. Mai 2023 in Kraft. § 32 d des Gesetzes zur ambulanten Resozialisierung und Opferhilfe tritt am 6. Mai 2023 in Kraft.

Begründung

Allgemeines

Zu Artikel 1:

Das Europäische Parlament und der Rat der Europäischen Union haben am 27. April 2016 zwei Regelungswerke zum Schutz bei der Verarbeitung personenbezogener Daten erlassen:

Einerseits die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119 vom 4. Mai 2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23. 5. 2018, S. 2) (Datenschutz-Grundverordnung) und andererseits die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4. Mai 2016, S. 89; L 127 vom 23.5.2018, S. 9) (Richtlinie (EU) 2016/680).

Das vorliegende Gesetz dient der Umsetzung der Richtlinie (EU) 2016/680.

Die Richtlinie (EU) 2016/680 findet auch auf den Straf-, Jugendstraf-, Untersuchungshaftvollzug, die Unterbringung in der Sicherungsverwahrung und den Jugendarrestvollzug (Justizvollzug) Anwendung; der Justizvollzug ist ein Teil der Strafvollstreckung beziehungsweise fällt zumindest unter den Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Im Wesentlichen sprechen folgende Argumente für diese Bewertung:

Die Einordnung des Justizvollzugs unter den Begriff der Strafvollstreckung ist dem deutschen Rechtssystem nicht fremd. So wird in der Kommentarliteratur zu den §§ 449 ff. der Strafprozessordnung vorwiegend zwischen der Strafvollstreckung im weiteren und der Strafvollstreckung im engeren Sinne unterschieden (vgl. Meyer-Goßner/Schmitt, 60. Auflage 2017, StPO, vor § 449 Rn. 2). Der Begriff der Strafvollstreckung im weiteren Sinne ist dabei gleichbedeutend mit dem Begriff der Strafverwirklichung zu verstehen und umfasst neben der Strafvollstreckung im engeren Sinne auch den Strafvollzug (vgl. Appl, in: Karlsruher Kommentar zur StPO, 7. Auflage 2013, vor § 449 Rn. 3; Pollähne, in: Gercke/Julius/Temming u.a., StPO, 5. Auflage 2012, vor § 449 Rn. 1).

Auch eine europarechtliche Betrachtung führt zu einer Einordnung des Justizvollzugs unter den Begriff der Strafvollstreckung im Sinne der Richtlinie (EU) 2016/680. Dafür spricht zunächst, dass in zahlreichen europäischen Ländern eine begriffliche Unterscheidung nicht vorgenommen wird und beide Materien in einheitlichen Gesetzen geregelt sind. Zudem führt eine an Sinn und Zweck orientierte Betrachtung zu dieser Bewertung: Der sensible Bereich der Strafrechtspflege soll der Richtlinie (EU) 2016/680 – und nicht der unmittelbar seit 25. Mai 2018 geltenden Verordnung (EU) 2016/679 – unterfallen, um den Mitgliedstaaten bei der Umsetzung größere Handlungsspielräume zu eröffnen. Es ist daher naheliegend, dass dies auch für den Justizvollzug gilt, der als zeitlich letzter Abschnitt eines Strafverfahrens oder Maßnahme zur sicheren Durchführung eines Strafverfahrens ein Teil der Strafrechtspflege ist.

Diese Betrachtungen gelten auch für den Vollzug der Sicherungsverwahrung und des Jugendarrests, die zwar keine Strafen im eigentlichen Sinne darstellen, aber Maßnahmen sind, die als staatliche Reaktion auf Verstöße gegen strafrechtliche Bestimmungen erfolgen. Die Untersuchungshaft und ihr gleichgestellte Haftarten knüpfen an den dringenden Verdacht eines Verstoßes gegen strafrechtliche Bestimmungen an und dienen der geordneten Durchführung eines Strafverfahrens oder der Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung. Insgesamt ist somit für den Bereich des Justizvollzugs der Anwendungsbereich der Richtlinie (EU) 2016/680 eröffnet.

Soweit der Anwendungsbereich der Richtlinie (EU) 2016/680 eröffnet ist, schließt sie in der Regel die Geltung der am 25. Mai 2018 in Kraft getretenen Verordnung (EU) 2016/679 aus. Allerdings folgt aus Artikel 9 Absatz 1 Satz 2 und Absatz 2 der Richtlinie (EU) 2016/680, dass auch bei grundsätzlicher Eröffnung ihres Anwendungsbereichs in einigen Fällen die Verordnung (EU) 2016/679 in Verbindungen mit den jeweiligen landesrechtlichen Datenschutzbestimmungen Anwendung finden kann. Wenn etwa personenbezogene Daten, die ursprünglich für einen der Zwecke der Richtlinie (EU) 2016/680 erhoben wurden, zu anderen Zwecken (weiter)verarbeitet werden, gilt hierfür die Verordnung (EU) 2016/679 (Erwägungsgrund 34 der Richtlinie (EU) 2016/680).

Anders als die Richtlinie (EU) 2016/680 ist die Verordnung (EU) 2016/679 in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat; sie bedarf gemäß Artikel 288 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) keiner Umsetzung in das mitgliedstaatliche Recht. Ziel der Verordnung (EU) 2016/679 ist ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen und die Beseitigung von Hemmnissen für den Verkehr personenbezogener Daten innerhalb der gesamten Union zu erreichen (Erwägungsgrund 10 und 13 der Verordnung (EU) 2016/679). Nichtsdestotrotz enthält die Verordnung (EU) 2016/679 Öffnungsklauseln für den nationalen Gesetzgeber mit Regelungsoptionen und konkreten Regelungsaufträgen, damit das allgemeine und das bereichsspezifische Datenschutzrecht soweit wie nötig angepasst werden kann. Dieser sich ergebende Anpassungsbedarf findet sich in den jeweiligen Landesgesetzen, vornehmlich den Landesdatenschutzgesetzen, aber auch in speziellen landesrechtlichen oder auch bundesgesetzlichen Fachgesetzen, die eigene Rechtsgrundlagen für die Datenverarbeitung beinhalten; diese Rechtsgrundlagen sind dann stets in Verbindung mit der unmittelbar geltenden Verordnung (EU) 2016/679 für die Datenverarbeitung zu anderen Zwecken als denjenigen der Richtlinie (EU) 2016/680 heranzuziehen.

Der Anwendungsbereich der Verordnung (EU) 2016/679 ist gemäß Artikel 9 Absatz 2 der Richtlinie (EU) 2016/680 etwa eröffnet, wenn die Datenverarbeitung von Anfang an nicht dem Anwendungsbereich des Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 unterfällt, weil sie der Verwaltung von Personaldaten der Bediensteten im Justizvollzug dient. Ferner kann die Verordnung (EU) 2016/679 in Verbindung mit bereichsspezifischen nationalen Datenschutzbestimmungen zur Anwendung kommen, weil personenbezogene Daten, die für Zwecke des Justizvollzugs erhoben wurden, für andere Zwecke als diejenigen der Richtlinie (EU) 2016/680 weiterverarbeitet werden, etwa bei der Übermittlung personenbezogener Daten an die für Sozialleistungen zuständigen Behörden gemäß § 12 Absatz 3 Nummer 2 Buchstabe d) oder die Ausländerbehörde für asyl- oder ausländerrechtlicher Maßnahmen gemäß § 12 Absatz 3 Nummer 2 Buchstaben g).

Aufgrund der Richtlinie (EU) 2016/680 ergibt sich für den Bereich des Justizvollzugs und den dort normierten bereichsspezifischen Datenschutzbestimmungen ein entsprechender zielverbindlicher Umsetzungsbedarf. Denn wie jede Richtlinie gemäß Artikel 288 AEUV ist auch die Richtlinie (EU) 2016/680 für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich. Die Rechtsform der Richtlinie überlässt allerdings den innerstaatlichen Stellen die Wahl der Form und der Mittel für die Umsetzung in das nationale Recht.

Der Bund hat weiterhin die Gesetzgebungskompetenz für den Datenschutz im Vollzug der Ordnungs-, Sicherungs-, Zwangs- und Erzwingungshaft (Zivilhaft). Daher gilt für die Zivilgefangenen die Verordnung (EU) 2016/679 in Verbindung mit den angepassten Bestimmungen des Strafvollzugsgesetzes des Bundes.

Die Umsetzung der europäischen Vorgaben in das bereichsspezifische Recht des Datenschutzes im Justizvollzug des Saarlandes sieht das vorliegende Justizvollzugsdatenschutzgesetz vor. Das Gesetz beabsichtigt eine weitgehende Vollregelung des für den Justizvollzug geltenden Datenschutzrechts.

Mit dem vorgelegten Gesetz werden die bisherigen datenschutzrechtlichen Standards in den einzelnen saarländischen Vollzugsgesetzen in ein neues eigenständiges Justizvollzugsdatenschutzgesetz überführt und zugleich die Vorgaben der Richtlinie (EU) 2016/680 in Landesrecht umgesetzt. Dadurch wird dem hohen Stellenwert des Datenschutzes im Justizvollzug Rechnung getragen und das eigenständige Gesetz macht die komplexe Materie des Datenschutzes anwendungsfreundlicher.

Der Strafvollzugausschuss der Länder hat auf seiner 125. Tagung vom 10. bis 12. Mai 2017 in Potsdam beschlossen, eine länderübergreifende Arbeitsgruppe zur Erarbeitung eines Mustergesetzentwurfs zur Umsetzung der Richtlinie (EU) 2016/680 für den Justizvollzug einzurichten, in der Brandenburg, Berlin, Nordrhein-Westfalen und Schleswig-Holstein die Federführung übernommen haben. Der Musterentwurf berücksichtigt neben den Ergebnissen der Arbeitsgruppe auch die während der Erarbeitungsphase bereits weiter vorangeschrittenen Entwürfe der Länder zum bereichsspezifischen Datenschutz im Justizvollzug. Bei der Erarbeitung des Musterentwurfs wurden zudem die Regelungen des neuen Bundesdatenschutzgesetzes vom 30. Juni 2017 (BGBl. I S. 2097) herangezogen.

Als Vorlage für den Musterentwurf diente das Justizvollzugsdatenschutzgesetz Schleswig-Holstein vom 21. Juli 2016 (GVObI. S. 618, 644) als das jüngste, vollzugsform übergreifende, eigenständige Datenschutzgesetz. Bestehende bereits richtlinienkonforme Regelungen haben neben wenigen sprachlichen Änderungen keine erforderlichen Neuregelungen im Hinblick auf die Umsetzung der Richtlinie (EU) 2016/680 erfahren (z.B. die besonderen Bestimmungen für Geheimnisträgerinnen und Geheimnisträger).

Der Musterentwurf enthält Bestimmungen über allgemeine Grundsätze der Datenverarbeitung, die Rechtsgrundlagen einzelner Verarbeitungsformen (Erhebung, Speicherung, Nutzung und Übermittlung), besondere Formen der Datenverarbeitung (etwa die Datenverarbeitung im Auftrag), die Schutzanforderungen an die Datenverarbeitung als weitere Pflichten der Justizvollzugsbehörden (z.B. Zweckbindung oder Verzeichnis von Verarbeitungstätigkeiten) und die mit der Richtlinienumsetzung erweiterten Rechte der betroffenen Personen.

Um das bisherige hohe datenschutzrechtliche Schutzniveau beizubehalten und eine möglichst hohe Anwenderfreundlichkeit zu erzielen, greift das Gesetz zwar auf den neuen zentralen Begriff der Verarbeitung der Richtlinie (EU) 2016/680 zurück, setzt aber dennoch die im Justizvollzug bewährte begriffliche Unterscheidung zwischen Erhebung, Speicherung, Nutzung und Übermittlung fort. Dadurch wird die Datenverarbeitung in ihren einzelnen Schritten mit den daran geknüpften Voraussetzungen weiterhin nachvollziehbar im Gesetz verortet, d.h. erst werden die Daten erhoben, dann werden sie gespeichert und genutzt, dann gegebenenfalls übermittelt und nach Entlassung der Gefangenen gelöscht.

Die Richtlinie (EU) 2016/680 verlangt Garantien, mit denen die Datenschutzgrundsätze zum Schutz der Rechte der Gefangenen umgesetzt werden. Das Gesetz sieht daher in Anlehnung an die bisherige Rechtslage eine Umsetzung des Standard-Datenschutzmodells vor, das um weitere technische Schutzstandards ergänzt wird.

Neu aufgenommen werden Regelungen zum Datenabgleich mit den Sicherheitsbehörden unabhängig von der erforderlichen Umsetzung der Richtlinie (EU) 2016/680. Diese Regelungen (Sicherheitsrelevante Erkenntnisse, Überprüfung Gefangener, Überprüfung anstaltsfremder Personen, Fallkonferenzen, Weitere Zulässigkeitsvoraussetzungen für die Datenverarbeitung mit den Sicherheitsbehörden und der erkennungsdienstliche Datenabgleich) gehen ebenfalls auf eine Beschlussfassung des Strafvollzugausschusses aus der Frühjahrstagung im Jahr 2017 zurück.

Der vorgelegte Entwurf für ein Saarländisches Vollzugsdatenschutzgesetz beruht auf dem Musterentwurf und weicht nur in einigen wenigen Punkten inhaltlich von dem gemeinsam erarbeiteten Entwurf ab, unter Berücksichtigung von bisherigen saarländischen Datenschutzregelungen.

Zu Artikel 2,3 und 4:

Das Gesetz modifiziert die bisherigen Regelungen zu den besonderen Sicherungsmaßnahmen in den Landesjustizvollzugsgesetzen. Es berücksichtigt dabei die im Urteil des Bundesverfassungsgerichts vom 24. Juli 2018 - 2 BvR 309/15, 2 BvR 502/16 - festgelegten verfassungsrechtlichen Anforderungen an die Fixierung von Patienten in der öffentlich-rechtlichen Unterbringung. Diese Entscheidung bezieht sich zwar nicht auf das Saarland und nicht unmittelbar auf den Justizvollzug, gibt aber im Hinblick auf Art. 104 Abs. 2 Satz 2 GG Veranlassung, die Bestimmungen für die Fixierung von Gefangenen zu präzisieren, da auch im Justizvollzug Fixierungen zur Anwendung kommen. Aufgrund des vorbezeichneten Urteils wird aktuell bundesweit die Auffassung vertreten, dass die besonderen Anforderungen auch auf Fixierungen im Rahmen des Justizvollzuges anzuwenden sind. Die oben genannte Entscheidung steht im Kontext einer zivilrechtlichen Unterbringung, die aufgrund einer psychischen Erkrankung angeordnet wird, im amtlichen Leitsatz hingegen ist generell auf eine richterliche Unterbringungsentscheidung abgestellt, welche die Fixierung nicht abdeckt. Dies gilt auch für den Justizvollzug.

Das Urteil unterscheidet drei Zeiträume der Fixierung:

- Absehbar kurzfristige Fixierung bis zu einer halben Stunde

Für diese Maßnahme von kurzfristiger Dauer besteht nach Auffassung des Bundesverfassungsgerichts kein Richtervorbehalt. In der Vollzugspraxis dürfte eine solche Maßnahme eher die Ausnahme sein.

- Fixierung nach 21.00 Uhr bis 6.00 Uhr

Aus der Beschränkung des richterlichen Bereitschaftsdienstes auf den Zeitraum von 6.00 Uhr bis 21.00 Uhr entnimmt das Bundesverfassungsgericht, dass der Richtervorbehalt für Fixierungen, die im Zeitraum von 21.00 Uhr bis 6.00 Uhr angeordnet werden müssen, nicht greift.

- Fixierung zwischen 6.00 Uhr und 21.00 Uhr

In dieser Zeit erfordert die Fixierung nach Auffassung des Bundesverfassungsgerichts grundsätzlich eine vorherige richterliche Anordnung.

Eine nachträglich richterliche Entscheidung genügt nur dann, wenn der mit der Fixierung verfolgte verfassungsrechtlich zulässige Zweck nicht erreichbar wäre, wenn dieser Maßnahme eine richterliche Entscheidung vorausgehen müsste. Das Bundesverfassungsgericht weist ausdrücklich darauf hin, dass dies regelmäßig der Fall ist, wenn die Fixierung zur Abwehr einer von der betroffenen Person ausgehenden akuten Selbst- oder Fremdgefährdung angeordnet wird. Diese Situation dürfte im Justizvollzug regelmäßig gegeben sein. Nach den Vorgaben des Bundesverfassungsgerichts müsste aber auch in diesen Fällen unverzüglich eine richterliche Entscheidung herbeigeführt werden, wenn nicht bereits eindeutig absehbar ist, dass die Fixierung vor Erlangung eines richterlichen Beschlusses oder innerhalb einer halben Stunde beendet sein wird.

Aus der verfassungsrechtlichen Garantie des effektiven Rechtsschutzes ergibt sich nach dem Bundesverfassungsgericht die Notwendigkeit, die maßgeblichen Gründe für die Fixierung, ihre Durchsetzung, Dauer und Art der Maßnahme schriftlich zu dokumentieren. Zudem verlangt das Bundesverfassungsgericht während der gesamten Dauer der Fixierung grundsätzlich eine 1:1-Betreuung durch therapeutisches oder pflegerisches Personal. Im Justizvollzug dürfte dies durch die bereits praktizierten Sitzwachen erfüllt sein. In allen Fällen der Fixierung ist die betroffene Person ausdrücklich auf die Möglichkeit hinzuweisen, die Zulässigkeit der durchgeführten Maßnahme gerichtlich überprüfen zu lassen.

Das Bundesverfassungsgericht hat sich zu der gerichtlichen Zuständigkeit für die Anordnung der Fixierung und die nachträgliche Überprüfung nicht geäußert. Die Festlegung dieser Zuständigkeit wird durch Bundesgesetz geregelt, kann daher nicht Gegenstand dieses Gesetzes sein.

Zu Artikel 5:

Das Gesetz zur ambulanten Resozialisierung und Opferhilfe ist teilweise ebenfalls von der Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4. Mai 2016, S. 89; L 127 vom 23.5.2018, S. 9) (Richtlinie (EU) 2016/680) betroffen und wird entsprechend angepasst.

Zu Artikel 6:

Die vorgesehene Änderung des Gesetzes über den Verfassungsgerichtshof ist wie folgt veranlasst:

Mit Gesetz vom 8. November 2000 (Amtsbl. 2001 S. 94) wurden im Gesetz über den Verfassungsgerichtshof die §§ 14a ff zur Auskunft aus oder Einsicht in Akten des Verfassungsgerichtshofs eingeführt. Dies erfolgte unter weitgehender Übernahme der mit Gesetz vom 16. Juli 1998 (BGBl. I S. 1823) diesbezüglich eingefügten Parallelregelungen des Zweiten Abschnitts des Bundesverfassungsgerichtsgesetzes (§§ 35a bis 35c BVerfGG).

Im Rahmen des Entwurfs eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 ist auf Bundesebene eine Anpassung der §§ 35a bis 35c des Bundesverfassungsgerichtsgesetzes an die neue EU - Datenschutz-Grundverordnung und die hierauf Bezug nehmende Neuregelung des Bundesdatenschutzgesetzes vorgesehen.

In Anlehnung hieran ist deshalb auch eine entsprechende Anpassung der §§ 14a bis 14c des Gesetzes über den Verfassungsgerichtshof veranlasst unter Beibehaltung der bisherigen Regelungsstruktur und unter Übernahme der vorgesehenen einschlägigen Vorschriften des Bundesverfassungsgerichtsgesetzes.

Des Weiteren wird im Interesse einer flexibleren Gestaltung der Richterwahl die Besetzungsregelung in § 2 Absatz 3 Satz 6 des Gesetzes dahingehend geändert, dass der dort vorgeschriebene Berufsrichteranteil nicht mehr an die Zugehörigkeit zu einem oberen Landesgericht geknüpft wird.

Im Einzelnen

Zu Artikel 1

Abschnitt 1

Allgemeine Bestimmungen

Zu § 1 Anwendungsbereich, Aufsichtsbehörde

Die Bestimmung regelt den Anwendungsbereich des Gesetzes und definiert wesentliche vollzugliche Begriffe. Sie greift § 1 Absatz 1 und 2 JVollzDSG SH in der bisherigen Fassung auf.

Nach Absatz 1 umfasst der Anwendungsbereich des Gesetzes die Verarbeitung personenbezogener Daten im gesamten der Gesetzgebungskompetenz der Länder unterfallenden Justizvollzug. So regelt dieses Gesetz die gesamte Materie des Datenschutzes für den Justizvollzug in Umsetzung der Richtlinie (EU) 2016/680 bereichsspezifisch abschließend und einheitlich. § 64 sieht ergänzend die Anwendung weiterer Bestimmungen des allgemeinen Datenschutzrechts vor. Nummer 1 benennt die klassischen Haft- und Unterbringungsarten im Justizvollzug, Nummer 2 enthält eine Aufzählung der Haftarten, die dem Vollzug der Untersuchungshaft entsprechen. Auf die Zivilhaft ist dieses Gesetz wegen der fehlenden Gesetzgebungsbefugnis der Länder für diese Materie nicht anwendbar. Für diese Haft nach § 171 StVollzG gelten die datenschutzrechtlichen Regelungen des Strafvollzugsgesetzes des Bundes ergänzt um die Bestimmungen des Bundesdatenschutzgesetzes und der Verordnung (EU) 2016/679.

Absatz 2 definiert den in Absatz 1 verwendeten Begriff der Justizvollzugsbehörden und führt aus Gründen der besseren Lesbarkeit des Gesetzestextes die verkürzten Begriffe „Anstalten“ und „Aufsichtsbehörde“ ein. Das für den Justizvollzug zuständige Ministerium ist – der Terminologie der Justizvollzugsgesetze des Landes folgend und damit abweichend von der Definition des Artikels 3 Nummer 15 der Richtlinie (EU) 2016/680 – hier weiterhin „Aufsichtsbehörde“.

Absatz 3 Satz 1 definiert die oder den Landesbeauftragten für Datenschutz als die nach Artikel 41 der Richtlinie einzurichtende Aufsichtsbehörde. Satz 2 regelt die Umsetzung von Artikel 26 der Richtlinie und normiert die Verpflichtung zur Kooperation mit der oder dem Landesbeauftragten für Datenschutz.

Zu § 2 **Begriffsbestimmungen**

Die Bestimmung definiert wesentliche vollzugliche und datenschutzrechtliche Begriffe, um die Lesbarkeit des Gesetzes und die einheitliche Handhabung der Bestimmungen zu erleichtern. Einige Begriffsbestimmungen dienen der Umsetzung von Artikel 3 der Richtlinie (EU) 2016/680. In den Nummern 3, 5 bis 7, 9 bis 13 und 15 bis 18 werden die Begriffsbestimmungen der Richtlinie (EU) 2016/680 unverändert übernommen.

Nummer 1 definiert den Begriff „Gefangene“ als alle Personen, die sich im Vollzug der in § 1 Absatz 1 genannten Vollzugsarten befinden. Diese Personen sind unter dem Begriff „Gefangene“ zusammengefasst, weil sie eine Vielzahl von Regelungen gleichermaßen betrifft.

Nummer 2 definiert die vollzuglichen Zwecke und legt damit den Umfang und die Grenzen der Datenverarbeitung für vollzugliche Zwecke fest. Damit wird Artikel 8 der Richtlinie (EU) 2016/680 umgesetzt, wonach in gesetzlichen Regelungen unter anderem die Zwecke der Datenverarbeitung anzugeben sind. Erfolgt die Datenverarbeitung zu den genannten Zwecken, unterfällt sie stets dem Anwendungsbereich dieses Gesetzes (vgl. Erwägungsgrund 29 der Richtlinie (EU) 2016/680).

Nummer 2a bezeichnet den vollzuglichen Zweck der Resozialisierung, also die Befähigung der Gefangenen in Zukunft ein Leben in sozialer Verantwortung ohne Straftaten zu führen. Dieser Vollzugszweck ist sowohl völker- und europarechtlich verankert (vgl. Regel Nummer 88 der VN-Mindestgrundsätze für die Behandlung der Gefangenen, „Nelson-Mandela-Regeln“ und Nummer 102.1 der Europäischen Strafvollzugsgrundsätze) als auch auf nationaler Ebene verfassungsrechtlich geboten. Dies umfasst auch die Gesundheitsfürsorge, Beschäftigung sowie alle weiteren mit der Freiheitsentziehung in unmittelbarem Zusammenhang stehenden Aspekte.

Nummer 2b definiert den Schutz der Allgemeinheit vor weiteren Straftaten der Gefangenen als weiteren vollzuglichen Zweck. Dies bezieht sich unmittelbar auf die Haftzeit, als auch auf die Zeit nach der Entlassung. Nummer 2a und 2b sind im Zusammenhang zu sehen. Zwischen dem Eingliederungsziel des Vollzuges und dem Anliegen, die Allgemeinheit vor weiteren Straftaten zu schützen, besteht kein Gegensatz. Eine gelungene Resozialisierung gewährleistet zugleich auch den umfassenden Schutz der Allgemeinheit. Beides dient letztlich auch der Sicherheit der Bevölkerung. Der Staat kommt seiner Schutzpflicht insbesondere dadurch nach, dass er die Resozialisierung fördert.

Nummer 2c definiert den Schutz von Leib, Leben, Freiheit und Vermögen der Bediensteten und der Gefangenen, sowie des Vermögens des Landes durch die Aufrechterhaltung der Sicherheit und Ordnung innerhalb der Anstalt als vollzuglichen Zweck. Der Schutz der Individualrechtsgüter dient gleichzeitig der Aufrechterhaltung von Sicherheit und Ordnung im Vollzug und steht im Einklang mit dem Ziel der Resozialisierung.

Nummer 2d definiert die Verhinderung einer Befreiung und Entweichung der Gefangenen als vollzuglichen Zweck. Dieser dient der Sicherung des Vollzuges.

Nummer 2e definiert die Vermeidung von Nichtrückkehr und Missbrauch von Lockerungen als vollzuglichen Zweck. Der vollzuglichen Zweck dient der Sicherung des Vollzuges und dem Schutz der Allgemeinheit.

Nummer 2f definiert die Mitwirkung des Justizvollzugs an den ihm durch Gesetz übertragenen sonstigen Aufgaben als vollzuglichen Zweck.

Der zweite Halbsatz nach Nummer 2f weist darauf hin, dass der vollzugliche Zweck der Untersuchungshaft in der Sicherung des Strafverfahrens liegt.

Nummer 3 definiert den Begriff der „personenbezogenen Daten“ als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (vgl. Erwägungsgrund 21 der Richtlinie (EU) 2016/680).und führt aus Gründen der besseren Lesbarkeit den Begriff „betroffene Person“ ein.

Nummer 4 definiert den Begriff der „Verarbeitung“ mit oder ohne Hilfe automatisierter Verfahren und benennt Fallbeispiele (vgl. Erwägungsgrund 34 der Richtlinie (EU) 2016/680). Nummer 4a und 4b benennen die verschiedenen Vorgänge, die unter den Begriff Datenverarbeitung fallen.

Nummer 5 definiert den Begriff der „Einschränkung der Verarbeitung“. Er entspricht dem bisherigen Begriff der „Sperrung“.

Nummer 6 definiert den Begriff des „Profiling“.

Nummer 7 definiert den Begriff der „Pseudonymisierung“.

Nummer 8 definiert den Begriff der „Anonymisierung“. Die Begriffsbestimmung wurde aus § 3 Absatz 6 des Bundesdatenschutzgesetzes a.F. übernommen. Die Grundsätze des Datenschutzes gelten nicht für anonyme Informationen (vgl. Erwägungsgrund 21 der Richtlinie (EU) 2016/680).

Nummer 9 definiert den Begriff des „Dateisystems“. Der Begriff ist technologieneutral zu verstehen und soll für die automatisierte und die manuelle Verarbeitung gleichermaßen gelten(vgl. Erwägungsgrund 18 der Richtlinie (EU) 2016/680). Der Begriff entspricht der bisherigen Definition des Begriffs „Datei“ nach Artikel 2 Buchstabe c) Richtlinie 95/46/EG und bisher geltendem Datenschutzrecht.

Nummer 10 definiert den Begriff des „Verantwortlichen“ für den Anwendungsbereich dieses Gesetzes. Zum Schutz der Rechte und Freiheiten der betroffenen Personen verlangt die Richtlinie (EU) 2016/680 eine klare Zuständigkeit der Verantwortung für die Datenverarbeitung (vgl. Erwägungsgrund 54 der Richtlinie (EU) 2016/680).

Nummer 11 definiert den Begriff des „Auftragsverarbeiters“ als Datenverarbeiter im Auftrag des Verantwortlichen.

Nummer 12 definiert den Begriff des „Empfängers“.

Nummer 13 definiert den Begriff der „Verletzung des Schutzes personenbezogener Daten“.

Nummer 14 definiert den aus Artikel 10 der Richtlinie (EU) 2016/680 übernommenen Begriff der „besonderen Kategorien personenbezogener Daten“. Diese Daten sind auf Grund ihres Inhalts besonders sensibel.

Nummer 15 definiert den Begriff der „genetischen Daten“. Diese gehören zu den besonderen Kategorien personenbezogener Daten nach Nummer 14.

Nummer 16 definiert den Begriff der „biometrischen Daten“. Diese zählen zu den besonderen Kategorien personenbezogener Daten nach Nummer 14.

Nummer 17 definiert den Begriff der „Gesundheitsdaten“. Diese zählen zu den besonderen Kategorien personenbezogener Daten nach Nummer 14.

Nummer 18 definiert den Begriff der „internationalen Organisation“.

Nummer 19 definiert den Begriff der „Einwilligung“, deren Anwendungsbereich und Voraussetzungen in § 4 geregelt sind. In Anlehnung an die Vorgehensweise in § 46 Nummer 17 des Bundesdatenschutzgesetzes vom 30. Juni 2017 (BGBl. I Seite 2097) wurde die Definition der Einwilligung aus der Verordnung (EU) 2016/679 übernommen.

Nummer 20 definiert den Begriff der „anstaltsfremden Person“.

Nummer 21 und 22 definieren die Begriffe der „öffentlichen Stellen“ und „nichtöffentlichen Stellen“. Die Definitionen wurden aus § 2 Absatz 1, 2 und 4 des Bundesdatenschutzgesetzes übernommen. Die Definition der öffentlichen Stellen wurde um Buchstabe c ergänzt, um deutlich zu machen, dass nicht nur inländische öffentliche Stellen, sondern auch solche anderer Mitgliedsstaaten der Europäischen Union von der Definition umfasst sind und eine Übermittlung personenbezogener Daten an diese bei Vorliegen einer entsprechenden Rechtsgrundlage grundsätzlich möglich ist. Dies entspricht der Zielbestimmung von Artikel 1 Absatz 2 Buchstabe b der Richtlinie (EU) 2016/680. Nichtöffentliche Stellen, die hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen, sind öffentliche Stellen. Dies sind beispielsweise die im Justizvollzug tätigen Vertragsärztinnen und -ärzte. Auch freie Träger der Straffälligenhilfe können im Einzelfall, zum Beispiel wenn sie einen Täter-Opfer-Ausgleich (§ 46a StGB, § 155a StPO) durchführen, hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen.

Zu § 3 Grundsätze der Datenverarbeitung

Absatz 1 hebt das Recht der Gefangenen und anderer betroffener Personen auf informationelle Selbstbestimmung aus dem Grundgesetz und das Recht auf Schutz der sie betreffenden personenbezogenen Daten aus der Charta der Grundrechte der Europäischen Union hervor.

Die Zielbestimmung in Absatz 2 fordert, dass möglichst ein schonender Ausgleich zwischen den Interessen des Justizvollzugs an einer Datenverarbeitung und dem Recht der betroffenen Personen auf informationelle Selbstbestimmung und deren Recht auf Schutz der sie betreffenden personenbezogenen Daten herbeizuführen ist. Absatz 2 setzt damit Artikel 4 Absatz 1 der Richtlinie (EU) 2016/680 um.

In Absatz 3 wird Artikel 7 Absatz 1 der Richtlinie (EU) 2016/680 umgesetzt. Um die geforderte Unterscheidung zwischen faktenbasierten und einschätzungsbasierten Daten zu ermöglichen, wird eine entsprechende Kennzeichnung vorzunehmen sein, sofern sich nicht – wie es im Justizvollzug häufig der Fall sein wird – bereits aus den Daten selbst ergibt, welcher Kategorie diese zuzuordnen sind. In diesen Fällen ist eine gesonderte Kennzeichnung entbehrlich.

Absatz 4 setzt Artikel 11 der Richtlinie (EU) 2016/680 um und regelt das Verbot automatisierter, insbesondere auf Profiling basierender Einzelentscheidungen. Dadurch wird das Recht betroffener Personen gewahrt, keiner Entscheidung zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die nachteilige rechtliche Wirkung für sie entfaltet oder sie in erheblichen Maßen beeinträchtigt. Beispiele für eine nachteilige Rechtsfolge können sein, die Versagung von vollzugsöffnenden Maßnahmen, die Anordnung von Disziplinarmaßnahmen gegenüber Gefangenen oder die Erteilung eines Besuchsverbots. Interne Zwischenfestlegungen oder Zwischenauswertungen, die Ausfluss automatisierter Prozesse sind, fallen nicht darunter.

Zu § 4 **Rechtmäßigkeit der Datenverarbeitung, Einwilligung**

Absatz 1 greift § 3 Absatz 1 JVollzDSG SH in der bisherigen Fassung auf und Absatz 8 entspricht § 3 Absatz 3 JVollzDSG SH in der bisherigen Fassung.

Absatz 1 bestimmt grundlegend die Zulässigkeit der Datenverarbeitung durch die Justizvollzugsbehörden und setzt damit den aus dem Rechtsstaatsgebot und der Rechtsprechung des Bundesverfassungsgerichts folgenden Grundsatz des Vorbehalts des Gesetzes um. Absatz 1 bestimmt als bereichsspezifische Sonderregelung, dass die Justizvollzugsbehörden personenbezogene Daten u.a. nur dann verarbeiten dürfen, wenn dies für den Anwendungsbereich dieses Gesetzes in einer anderen Rechtsvorschrift ausdrücklich erlaubt oder angeordnet ist. Voraussetzung ist, dass eine andere Rechtsvorschrift auf die Verarbeitung personenbezogener Daten Gefangener oder anderer betroffener Personen, die von Justizvollzugsbehörden verarbeitet worden sind, ausdrücklich Bezug nimmt. Zugleich wird Artikel 8 Absatz 1 der Richtlinie (EU) 2016/680 umgesetzt, wonach eine Datenverarbeitung auf eine klare und präzise Rechtsgrundlage gestützt sein muss (vgl. Erwägungsgrund 33 zur Richtlinie (EU) 2016/680).

Aus Erwägungsgrund 35 zur Richtlinie (EU) 2016/680 lässt sich entnehmen, dass eine Einwilligung auch im Geltungsbereich dieser Richtlinie die Grundlage einer Datenverarbeitung sein kann, wenn sichergestellt ist, dass eine echte Wahlfreiheit der betroffenen Person besteht. Der Erwägungsgrund gibt zwar zu erkennen, dass eine solche Wahlfreiheit in Konstellationen zweifelhaft sein kann, in denen eine Behörde die betroffene Person anweisen oder auffordern kann, einer rechtlichen Verpflichtung nachzukommen. Zugleich werden aber auch Konstellationen – auch explizit für den Bereich der Strafvollstreckung – aufgeführt, in denen eine betroffene Person in eine Datenverarbeitung einwilligen kann. Auch wenn in der Richtlinie (EU) 2016/680 außerhalb der Erwägungsgründe eine Einwilligung – anders als in der Verordnung (EU) 2016/679 – nicht mehr erwähnt wird, ist sie daher als Rechtsgrundlage einer Datenverarbeitung möglich. Dies entspricht auch der Wertung des Bundesgesetzgebers, der in § 46 Nummer 17 und in § 51 des Bundesdatenschutzgesetzes gesetzliche Regelungen für die Einwilligung geschaffen hat. Ein möglicher Fall der Einwilligung von Gefangenen findet sich in § 47 Absatz 2.

Absatz 2 entspricht inhaltlich § 51 Absatz 1 des Bundesdatenschutzgesetzes. Hier wird Artikel 7 Absatz 1 der Verordnung (EU) 2016/679 mit redaktionellen Anpassungen wiedergegeben.

Absatz 3 entspricht § 51 Absatz 2 des Bundesdatenschutzgesetzes. Hier wird Artikel 7 Absatz 2 der Verordnung (EU) 2016/679 wiedergegeben.

Absatz 4 entspricht § 51 Absatz 3 des Bundesdatenschutzgesetzes. Hier wird Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 wiedergegeben.

Absatz 5 entspricht im Wesentlichen § 51 Absatz 4 des Bundesdatenschutzgesetzes. In dieser Bestimmung wurde der Ansatz aus § 4a Absatz 1 des Bundesdatenschutzgesetzes a. F. mit dem Gedanken aus Artikel 7 Absatz 4 der Verordnung (EU) 2016/679 kombiniert. Die Bestimmung stellt heraus, dass für die Beurteilung der Wirksamkeit einer Einwilligung auf die Umstände der Erteilung abzustellen ist. Die Bestimmung des Bundesdatenschutzgesetzes wurde hier noch dahingehend ergänzt, dass bei den Umständen der Erteilung im Anwendungsbereich des hiesigen Gesetzes insbesondere die besondere Situation der Freiheitsentziehung zu berücksichtigen ist. Diese beinhaltet regelmäßig ein besonderes Machtgefälle zwischen den Verantwortlichen der Datenverarbeitung und der betroffenen Person, soweit diese eine oder ein Gefangener ist. Von einer freiwilligen Erteilung ist aber regelmäßig dann auszugehen, wenn dieses besondere Machtgefälle die Entscheidung der

betroffenen Person nicht maßgeblich beeinflusst, insbesondere wenn für die betroffenen Personen ein rechtlicher oder tatsächlicher Vorteil erreicht wird oder die Justizvollzugsbehörden und die betroffenen Personen gleichgelagerte Interessen verfolgen.

Absatz 6 entspricht § 51 Absatz 5 des Bundesdatenschutzgesetzes, in dem die Regelung des § 4a des Bundesdatenschutzgesetzes a. F. aufgenommen ist. Damit wird dem in Artikel 10 der Richtlinie (EU) 2016/680 zum Ausdruck gebrachten Erfordernis des besonderen Schutzes besonderer Kategorien personenbezogener Daten entsprochen.

Gemäß Absatz 7 verbleibt auch nach der Verordnung (EU) 2016/679 bei dem Grundsatz, dass die Einwilligung nicht die Geschäftsfähigkeit im Sinne der bürgerlich-rechtlichen Vorschriften, sondern die tatsächliche Einsichtsfähigkeit der betroffenen Person voraussetzt. Diese Frage ist jeweils einzelfallbezogen zu beurteilen.

Gemäß Absatz 8 treten die gesetzlichen Vertreterinnen und Vertreter (Eltern - §§ 1626 und 1629 BGB -, Vormünder - § 1793 BGB -, Betreuerinnen und Betreuer - § 1902 BGB -, soweit dies zu ihrem Aufgabenkreis gehört, sowie Pflegerinnen und Pfleger - § 1909 -, soweit sich dies aus dem Text der Bestellung ergibt) in die Rechte der von ihnen vertretenen Gefangenen ein, wenn diese nicht die für die Entscheidung notwendige Einsichtsfähigkeit besitzen und vollzugliche Aufgaben hierdurch nicht gefährdet werden. Aus Sicht der betroffenen Gefangenen und des Justizvollzuges sind gesetzliche Vertreterinnen und Vertreter Dritte. Ihre Einbeziehung kann aber häufig für die Erfüllung vollzuglicher Aufgaben erforderlich sein. Die Bestimmung überträgt daher den Gedanken aus § 67 Jugendgerichtsgesetzes (JGG) auf die datenschutzrechtlichen Bestimmungen, indem gesetzliche Vertreterinnen und Vertreter hinsichtlich der genannten Rechte den Gefangenen gleichgestellt werden. Die Einschränkung, dass vollzugliche Aufgaben nicht beeinträchtigt werden dürfen, dient der Vermeidung von Missbrauch.

Zu § 5 Datengeheimnis

§ 5 entspricht im Wesentlichen § 4 JVollzDSG SH in der bisherigen Fassung.

Die Bestimmung übernimmt den Gedanken des § 53 des Bundesdatenschutzgesetzes. Die Bestimmung normiert die Pflicht der in Justizvollzugsbehörden tätigen Personen zur Verschwiegenheit, unabhängig davon, ob die Befassung mit der Verarbeitung von personenbezogenen Daten den Schwerpunkt der Tätigkeit darstellt. Entscheidend ist die faktische Zugangsmöglichkeit, so dass auch externe Personen, wie Handwerker und Reinigungskräfte unter diese Regelung fallen. In Abgrenzung zu § 5 stellt § 19 auf die Übermittlung von Daten an Externe durch die Justizvollzugsbehörden ab.

Nach Absatz 2 endet das Datengeheimnis nicht durch die Beendigung der Tätigkeit und entspricht § 53 Satz 3 des Bundesdatenschutzgesetzes.

Abschnitt 2

Erhebung

Zu § 6 Rechtmäßigkeit der Datenerhebung

Die Bestimmung enthält die grundlegende Regelung für die Zulässigkeit der Erhebung personenbezogener Daten durch die Justizvollzugsbehörden.

Nach Absatz 1 ist eine Datenerhebung nur zulässig, soweit sie für vollzugliche Zwecke, die in § 2 Nummer 2 definiert sind, erforderlich ist.

Absatz 2 trägt der besonderen Schutzbedürftigkeit besonderer Kategorien personenbezogener Daten, die in § 2 Nummer 14 – Artikel 10 der Richtlinie (EU) 2016/680 folgend – definiert sind, Rechnung. Die Daten sind besonders sensibel. Die mit diesen Daten verbundene gesteigerte Persönlichkeitsrelevanz, wie sie auch das Bundesverfassungsgericht betont (BVerfGE 115, 320,348), und die damit verbundene gesteigerte Intensität von Eingriffen in das Persönlichkeitsrecht der betroffenen Personen lassen eine Verarbeitung dieser Daten nur unter der engen Voraussetzung zu, dass diese zu vollzuglichen Zwecken unbedingt erforderlich ist. „Unbedingt erforderlich“ ist eine Datenübermittlung, wenn sie im konkreten Einzelfall für die jeweilige Zweckerreichung unerlässlich ist.

Zu § 7 Erhebung bei betroffenen Personen

Die Bestimmung regelt die Erhebung von personenbezogenen Daten bei den betroffenen Personen.

Absatz 1 enthält den Grundsatz der Direkterhebung, wonach eine Erhebung personenbezogener Daten grundsätzlich unter der Mitwirkung der betroffenen Person zu erfolgen hat. Damit ist Absatz 1 unmittelbar Ausfluss des Grundrechts auf informationelle Selbstbestimmung, da die betroffene Person wissen können soll, wer sich für ihre Daten interessiert.

Absatz 2 regelt die Voraussetzungen, unter denen auch ohne Kenntnis und ohne Mitwirkung der betroffenen Person, ausnahmsweise eine Erhebung personenbezogener Daten zulässig ist. Diese ist nur zulässig, wenn keine Anhaltspunkte vorliegen, dass überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen. Insofern hat eine Abwägung stattzufinden. Als Beispiele für Absatz 2 kommen hier die durch Bedienstete geführten Beobachtungsbögen bei beispielsweise suizidgefährdeten Gefangenen in Betracht sowie Arbeitsplatzkontrollen im offenen Vollzug bei Freigängern.

Zu § 8 Erhebung von Daten über Gefangene bei Dritten

Die Bestimmung regelt in Absatz 1 die Voraussetzungen für die Erhebung personenbezogener Daten über einwilligungsfähige Gefangene ohne deren Kenntnis und Mitwirkung bei Dritten. Für nicht einwilligungsfähige Gefangene sieht Absatz 2 die Datenerhebung bei den gesetzlichen Vertretern vor.

Die Datenerhebung über Gefangene bei Dritten greift stärker in die Rechte der Gefangenen ein, als dies bei einer Erhebung bei ihnen selbst der Fall wäre. Aus diesem Grunde bindet Absatz 1 diese Art der Erhebung an strenge Voraussetzungen. Der in Absatz 1 genannte Katalog ist abschließend. Durch die Verweisung auf § 6 soll sichergestellt werden, dass dessen Voraussetzungen kumulativ vorliegen, d.h. bei besonderen Kategorien personenbezogener Daten muss die Verarbeitung zu vollzuglichen Zwecken unbedingt erforderlich sein. Zudem müssen die Voraussetzungen des § 7 Absatz 2 vorliegen, da es sich um eine Datenerhebung ohne Kenntnis und Mitwirkung der betroffenen Person handelt. Sofern eine Datenerhebung bei Dritten mit Kenntnis der Gefangenen erfolgt, ist diese zulässig, sofern die Voraussetzungen des § 6 und eine Alternative aus dem in Absatz 1 aufgeführten Katalog vorliegen.

Absatz 2 erweitert die Erhebungsbefugnis um die Möglichkeit, personenbezogene Daten von Gefangenen bei ihren gesetzlichen Vertreterinnen und Vertretern zu erheben, wenn sie nicht die für die Einwilligung notwendige Einsichtsfähigkeit besitzen. Abhängig von der Kategorie von Daten müssen im Hinblick auf die besondere Kategorie personenbezogener Daten kumulativ noch die Voraussetzungen nach § 6 Absatz 2 vorliegen. Zudem wird durch den Verweis auf § 7 Absatz 2 klargestellt, dass – in Anbetracht dessen, dass es sich um eine Erhebung ohne Kenntnis und Mitwirkung der betroffenen Person handelt – im Einzelfall eine Abwägungsentscheidung mit den schutzwürdigen Interessen der Gefangenen stattzufinden hat.

Aufgrund der Tatsache, dass die Datenerhebung bei Dritten ohne Kenntnis und Mitwirkung der Gefangenen einen stärkeren Eingriff in die Rechtsposition der Gefangenen bedeutet, werden nach Absatz 3 nichtöffentliche Stellen auf die Rechtslage und andernfalls auf die Freiwilligkeit der Auskunft verwiesen. Nur so ist sichergestellt, dass die nichtöffentlichen Stellen in eigener Verantwortung entscheiden können, ob und in welchem Umfang sie eine Auskunft erteilen wollen oder nicht erteilen.

Die Bestimmung setzt Artikel 6 der Richtlinie (EU) 2016/680 um, der eine Differenzierung nach unterschiedlichen Kategorien betroffener Personen vorgibt.

Zu § 9 Erhebung von Daten über Personen, die nicht Gefangene sind

§ 9 setzt Artikel 6 der Richtlinie (EU) 2016/680 um.

Die Bestimmung regelt die Erhebung von Daten über Personen, welche keine Gefangenen sind, wie beispielsweise Angehörige, Freunde oder andere nahestehende Personen. Zur Erreichung vollzuglicher Zwecke ist es unumgänglich, mit den Gefangenen ihre Lebenssituation, ihre Kontakte und ihren Umgang zu erörtern. Unvermeidlich muss dabei auch über personenbezogene Daten anderer Personen gesprochen werden.

Die Bestimmung ermöglicht sowohl die Erhebung bei den Gefangenen als auch die Erhebung bei Dritten oder Stellen außerhalb des Justizvollzugs. Er enthält neben § 8 eine weitere Durchbrechung des Grundsatzes der Direkterhebung bei den betroffenen Personen, bindet die Erhebung aber an enge Voraussetzungen. Aufgrund der Tatsache, dass die Datenerhebung für die Erreichung der vollzuglichen Zwecke unbedingt erforderlich ist und gleichzeitig eine Abwägung mit den schutzwürdigen Interessen der betroffenen Personen erfolgt, ist gewährleistet, dass sich die Eingriffe in die Rechte Dritter in einem verhältnismäßigen Rahmen halten.

Abschnitt 3

Speicherung und Nutzung, Aktenführung

Zu § 10 Speicherung und Nutzung

§ 10 knüpft in weiten Teilen an § 9 JVoIzDSG SH in der bisherigen Fassung an.

Absatz 1 enthält den Grundsatz der Zweckbindung für die Speicherung und Nutzung von personenbezogenen Daten nach deren zulässigen Erhebung und dient zudem der Umsetzung des in Artikel 8 Absatz 1 der Richtlinie (EU) 2016/680 normierten Erforderlichkeitsprinzips. Danach ist eine Verarbeitung personenbezogener Daten nur zulässig, soweit dies zur Aufgabenerfüllung der zuständigen Justizvollzugsbehörde erforderlich ist. Die Bestimmung enthält auch die Befugnis der Justizvollzugsbehörden, die erhobenen Daten zu einem anderen vollzuglichen Zweck im Sinne des § 2 Nummer 2 zu speichern und zu nutzen, soweit dies erforderlich und verhältnismäßig ist. Diese Befugnis ist eine Grundvoraussetzung für einen funktionsfähigen Justizvollzug, der die ihm übertragenen gesetzlichen Aufgaben zur Sicherung des Vollzugs und der Behandlung der Gefangenen erfüllen und die Sicherheit in der Anstalt gewährleisten muss. So haben etwa personenbezogene Daten, die aus Gründen der Sicherheit und Ordnung in der Anstalt erhoben wurden, die gleiche hohe Relevanz für die Behandlung der Gefangenen und hätten auch zu diesem vollzuglichen Zweck erhoben werden dürfen. Die Verarbeitung der Daten für diesen anderen vollzuglichen Zweck ist verhältnismäßig und steht in Einklang mit dem verfassungsrechtlichen Grundsatz der hypothetischen Datenneuerhebung (BVerfG, Urteil des Ersten Senats vom 20. April 2016 - 1 BvR 966/09, 1 BvR 1140/09, Juris Rn. 284 ff.) und Artikel 4 Absatz 2 der Richtlinie (EU) 2016/680.

Absatz 2 regelt mit abschließendem Katalog die Voraussetzungen dafür, dass die Justizvollzugsbehörden die zulässig erhobenen personenbezogenen Daten auch zu einem anderen, nicht-vollzuglichem Zweck speichern und nutzen dürfen, als zu demjenigen, zu dem sie erhoben worden sind.

Absatz 3 regelt die Speicherung und Nutzung von besonderen Kategorien personenbezogener Daten im Sinne von § 2 Nummer 14. Die Bestimmung dient damit der Umsetzung von Artikel 10 der Richtlinie (EU) 2016/680. Dieser sieht vor, dass die Verarbeitung besonders schutzwürdiger Daten nur dann erlaubt ist, wenn dies unbedingt erforderlich ist und geeignete Garantien für die Rechte und Freiheiten der betroffenen Person vorgesehen sind. Satz 2 sieht eine Ausnahme zugunsten besonderer Kategorien personenbezogener Daten vor, die einem Amts- oder Berufsgeheimnis unterfallen (insb. Gesundheitsdaten) und in einer, eine Verschwiegenheitspflicht begründenden amtlichen oder beruflichen Funktion überlassen worden sind.

Absatz 4 beschränkt die Speicherung und Nutzung von personenbezogenen Daten betroffener Personen, die nicht Gefangene sind und dient der Umsetzung von Artikel 6 der Richtlinie (EU) 2016/680, wonach zwischen verschiedenen Kategorien betroffener Personen zu unterscheiden ist.

Absatz 5 trägt den Erfordernissen der vollzuglichen Praxis Rechnung und entspricht der bisherigen Fassung im JVoIzDSG SH. Absatz 5 ist erforderlich, da sich insbesondere bei einer aktenmäßigen Speicherung personenbezogener Daten nicht immer mit verhältnismäßigem Aufwand sicherstellen lässt, dass eine Trennung nach erforderlichen und nicht erforderlichen Daten möglich ist. Nur bei unvertretbarem Aufwand für die Trennung dürfen ausnahmsweise auch nicht für den konkreten Zweck erforderliche Daten gespeichert werden. Als Schranke ist jedoch die zusätzliche Voraussetzung zu beachten, dass das berech-

tigte Interesse von betroffenen Personen oder Dritten an deren Geheimhaltung offensichtlich überwiegt.

Absatz 6 knüpft an § 9 Absatz 6 JVollzDSG SH in der bisherigen Fassung an. Werden nach Satz 1 personenbezogene Daten ausschließlich zur Datenschutzkontrolle, zur Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert oder genutzt, greift für diese Daten eine besondere Zweckbindung. Eine zweckändernde Nutzung ist daher nur zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erlaubt. Satz 2 bezieht sich auf die weitere Verarbeitung von Protokolldaten in automatisierten Datenverarbeitungssystemen.

Zu § 11 Aktenführung

Absatz 1 regelt die Führung von Akten über Gefangene.

Absatz 2 entspricht § 10 JVoIzDSG SH in der bisherigen Fassung. Satz 1 trägt der technischen Entwicklung Rechnung und erlaubt ausdrücklich die Führung einer elektronischen Akte. Er bildet damit die gesetzliche Grundlage für diese Art der Aktenführung im Justizvollzug. Nach Satz 2 können Regelungen zur elektronischen Aktenführung durch Rechtsverordnung festgelegt werden.

Abschnitt 4 Übermittlung

Zu § 12 Übermittlung an öffentliche und nichtöffentliche Stellen, Verfahren zur Feststellung von Vorinhaftierungen

§ 12 regelt die Übermittlung personenbezogener Daten an öffentliche und nichtöffentliche Stellen und knüpft in weiten Teilen an § 11 JVoIzDSG SH in der bisherigen Fassung an.

Absatz 1 enthält die allgemeine Rechtsgrundlage für die Übermittlung personenbezogener Daten. Absatz 1 ist insbesondere die Rechtsgrundlage für den Datenaustausch zwischen Justizvollzugsbehörden im Falle von Verlegungen und Überstellungen von Gefangenen oder bei sonstigen Verwaltungsvorgängen, an denen mehrere Justizvollzugsbehörden beteiligt sind. Dies gilt namentlich für länderübergreifende Vorgänge. Voraussetzung ist, dass die empfangende Behörde die Daten zur Erreichung vollzoglicher Zwecke benötigt. Der Begriff der „vollzoglichen Zwecke“ ist in § 2 Nummer 2 bestimmt. Der in Absatz 1 normierte Erforderlichkeitsgrundsatz dient der Umsetzung von Artikel 8 der Richtlinie (EU) 2016/680 und ist in ihrem Anwendungsbereich europarechtskonform auszulegen.

Absatz 2 führt Fälle auf, in denen eine Übermittlung zulässig erhobener personenbezogener Daten an nichtöffentliche Stellen zulässig ist. Voraussetzung ist, dass die Daten zu Zwecken übermittelt werden, zu denen sie erhoben wurden. Insbesondere die Nutzung von Daten durch private Dritte zu vollzoglichen Zwecken wie Behandlungs-, Beratungs-, Therapie-, und Bildungsmaßnahmen außerhalb der Anstalt ist damit durch § 12 Absatz 2 angesprochen. Absatz 2 Nummer 1 umfasst unter anderem die Datenübermittlung an freie Träger der Straffälligenhilfe. Absatz 2 Nummer 2 Buchstabe e) erweitert die bisherige landesrechtliche Regelung auf die Inanspruchnahme von Maßnahmen der Entlassungsvorbereitung, des Übergangs in die Freiheit, der Schuldenregulierung, der Entlassung, der Wiedereingliederung, der nachgehenden Betreuung oder des freiwilligen Verbleibs. Hierdurch werden die in der Praxis regelmäßig anfallenden Maßnahmen zur Eingliederung der Gefangenen ergänzend erfasst und eine Datenübermittlung an nichtöffentliche Stellen insoweit ermöglicht.

Die Absätze 3, 4 und 5 regeln die Fälle, in denen der Übermittlungszweck ein anderer ist als der Erhebungszweck. Dabei unterscheiden sich die Voraussetzungen, unter denen eine Übermittlung zulässig ist danach, ob die Übermittlung an öffentliche (Absätze 3 und 4) oder nichtöffentliche Stellen (Absatz 5) erfolgt. Hierbei wird festgeschrieben, dass der Rahmen der Übermittlungszulässigkeit gegenüber öffentlichen Stellen weiter gefasst ist als gegenüber nichtöffentlichen Stellen.

Absatz 3 dient der Umsetzung von Artikel 4 Absatz 2 und Artikel 9 Absatz 1 Satz 1 der Richtlinie (EU) 2016/680 (Grundsätze der zweckändernden Datenverarbeitung) und ist in ihrem Anwendungsbereich europarechtskonform auszulegen. Eine „andere gesetzliche Bestimmung“ im Sinne von Absatz 3 Nummer 1, welche die zweckändernde Übermittlung personenbezogener Daten an eine öffentliche Stelle erlaubt, kann auch eine solche sein, die der Verordnung (EU) 2016/679 unterfällt. Hiermit wird der Tatsache Rechnung getragen, dass die vielfältigen Datenverarbeitungen des Justizvollzuges je nach Zweck der Datenverarbeitung im Einzelfall entweder der Richtlinie (EU) 680/2016 oder der Verordnung (EU) 2016/679 unterfallen können. Auch in letzterem Fall bedarf es einer gesetzlichen Ermächtigung zur Datenübermittlung an die zuständige öffentliche Stelle. Datenübermittlungen für Gnadensachen nach Absatz 3 Nummer 2 Buchstabe b) unterfallen nicht dem Unionsrecht. Die Bestimmung bedarf insoweit nicht der europarechtskonformen Auslegung. Datenübermittlungen für die Erfüllung von Aufgaben, die den für Sozialleistungen zustän-

digen Leistungsträgern durch Rechtsvorschriften übertragen worden sind (Absatz 3 Nummer 3 Buchstabe d)), für dienstliche Maßnahmen der Bundeswehr im Zusammenhang mit der Aufnahme und Entlassung von Soldatinnen und Soldaten (Absatz 3 Nummer 3 Buchstabe f)), für asyl- oder ausländerrechtliche Maßnahmen (Absatz 3 Nummer 3 Buchstabe g)), zur Erfüllung von Aufgaben der Jugendämter (Absatz 3 Nummer 3 Buchstabe h)), oder zur Durchführung der Besteuerung (Absatz 3 Nummer 3 Buchstabe i)) unterfallen der Verordnung (EU) 2016/679 und nicht der Richtlinie (EU) 680/2016. Die Datenübermittlung an öffentliche Stellen zur Erfüllung von Aufgaben der forensischen Ambulanzen, für asylrechtliche Maßnahmen, zur Erfüllung der Aufgaben der Jugendämter und für Falkonferenzen mit den Sicherheitsbehörden wurde neu in das Gesetz aufgenommen, um den entsprechenden Bedürfnissen der Praxis Rechnung zu tragen.

Absatz 4 schränkt die Übermittlungsbefugnis der Justizvollzugsbehörden zu Gunsten Untersuchungsgefangener und der in den in § 1 Absatz 2 Satz 2 genannten Haftarten befindlichen Gefangenen ein, weil für sie die Unschuldsvermutung gilt beziehungsweise eine nur vorläufig zu vollziehende Freiheitsentziehung angeordnet ist. Deshalb hat vor der Übermittlung eine Abwägung mit dem schutzwürdigen Interesse der Untersuchungsgefangenen an dem Ausschluss der Übermittlung stattzufinden. Absatz 4 dient der Umsetzung von Artikel 6 der Richtlinie (EU) 680/2016 (Unterscheidung verschiedener Kategorien betroffener Personen) und ist in deren Anwendungsbereich europarechtskonform auszulegen.

Absatz 5 dient der Umsetzung von Artikel 4 Absatz 2 und Artikel 9 Absatz 1 Satz 1 der Richtlinie (EU) 680/2016 (Grundsätze der Zweckänderung) und ist in deren Anwendungsbereich europarechtskonform auszulegen.

Wegen der erhöhten Sensibilität der besonderen Kategorien personenbezogener Daten dürfen diese ohne Einwilligung der betroffenen Personen gemäß Absatz 6 nur in den enumerativ genannten Ausnahmefällen übermittelt werden, wobei dieser wiederum zwischen öffentlichen (Nummer 1) und nichtöffentlichen Stellen (Nummer 2) unterscheidet. Die Möglichkeit zur Übermittlung zulässig erhobener besonderer Kategorien personenbezogener Daten an forensische Ambulanzen und Nachsorgeeinrichtungen zum Zweck von Behandlungsmaßnahmen, der Entlassungsvorbereitung und der Nachsorge wurde ergänzend eingefügt, um einem Bedürfnis der Praxis Rechnung zu tragen. „Unbedingt erforderlich“ im Sinne des Absatzes 6 ist eine Datenübermittlung, wenn sie im konkreten Einzelfall für die jeweilige Zweckerreichung unerlässlich ist.

Absatz 7 trägt dem Umstand Rechnung, dass bei Personen, die keine Gefangenen sind, ein Eingriff durch die Justizvollzugsbehörden in ihr informationelles Selbstbestimmungsrecht besonderes Gewicht hat. Der Verweis in Satz 1 auf Absatz 1 ist verfassungskonform eng im Hinblick auf die in § 10 Absatz 2 Nummer 1 bis 6 oder § 16 dahinterstehenden Rechtsgüter auszulegen. Satz 2 erweitert die Übermittlungsbefugnis der Justizvollzugsbehörden um die Möglichkeit, personenbezogene Daten Dritter zu übermitteln, um die Fahndung nach entwichenen Gefangenen und ihre Festnahme zu ermöglichen. Es handelt sich hier um eine bereichsspezifische Regelung. Bei den zulässig übermittelbaren Daten handelt es sich regelmäßig nur um Mitteilungen über Name und Adresse von Kontaktpersonen. Absatz 7 dient der Umsetzung von Artikel 6 der Richtlinie (EU) 680/2016 (Unterscheidung verschiedener Kategorien betroffener Personen) und ist in deren Anwendungsbereich europarechtskonform auszulegen.

Absatz 8 trägt den Bedürfnissen der vollzuglichen Praxis Rechnung und stellt im Hinblick auf die Interessen und Rechte der betroffenen Personen eine verhältnismäßige Regelung dar. Absatz 8 dient der Umsetzung von Artikel 6 der Richtlinie (EU) 680/2016 (Unterscheidung verschiedener Kategorien betroffener Personen) und ist in deren Anwendungsbereich europarechtskonform auszulegen.

Absatz 9 stellt klar, dass die Übermittlung der dort genannten personenbezogenen Daten nur aufgrund ausdrücklicher gesetzlicher Vorgabe zulässig ist und im Übrigen zu unterbleiben hat, wobei keinerlei Differenzierung zwischen öffentlichen und nichtöffentlichen Stellen erfolgt.

Die Feststellung von Vorinhaftierungen bei Neuzugängen und sicherheitsrelevanten Erkenntnissen im Rahmen der Vorinhaftierung erfordert bisher einen nicht unerheblichen Verwaltungs- und Zeitaufwand. Mit Absatz 10 soll der Datenaustausch zwischen den Justizvollzugsbehörden vereinheitlicht und verbessert werden. Der erste Schritt besteht in einem automatisierten Austausch von Identitätsdaten um herauszufinden, ob für die betroffene Person überhaupt personenbezogene Daten aus einer Vorinhaftierung vorliegen und aus einem automatisierten Austausch, ob aus der Vorinhaftierung sicherheitsrelevante Erkenntnisse vorliegen. Bei einem positiven Ergebnis obliegt es dann der Justizvollzugsbehörde im konkreten Einzelfall zu entscheiden, ob und in welchem Umfang weitergehende Informationen aus der Vorinhaftierung angefordert werden. Insoweit bleiben § 12 Absatz 1 bis 9 unberührt.

Zu § 13 Sicherheitsrelevante Erkenntnisse

Zunehmend wird der Justizvollzug auch als Teil der Sicherheitsarchitektur der Länder verstanden. Namentlich der Umgang mit extremistischen Gefangenen und Gefangenen, die der organisierten Kriminalität zuzuordnen sind, stellt die Sicherheitsbehörden und den Justizvollzug vor besondere Herausforderungen. Der Informationsaustausch mit den Sicherheitsbehörden ist hierbei von zentraler Bedeutung, um die Sicherheit der Justizvollzugsanstalten zu gewährleisten, um eine auf den einzelnen Gefangenen und seine Bedürfnisse abgestimmte Vollzugs- und Eingliederungsplanung zu ermöglichen, um weitergehende Radikalisierungen und Gefährdungen des Vollzugsziels bei anderen Gefangenen zu verhindern und um die Sicherheitsbehörden bei fortbestehender Gefahr in die Entlassungsvorbereitung einbinden zu können. Namentlich zu nennen sind insoweit die Unterbringung von Gefangenen in einer anderen Abteilung, die Verlegung von Gefangenen, die Veranlassung der Teilnahme an einem Deradikalisierungsprogramm, eine Überwachung von Besuchen, des Schriftverkehrs und der Telekommunikation sowie eine unter Einbeziehung der Sicherheitsbehörden erfolgende Eingliederungsplanung.

Die §§ 13 ff. sind in einem systematischen Zusammenhang mit den §§ 27 f. zu lesen. Letztere ermöglichen es den Justizvollzugsbehörden, die Identität von Gefangenen sicher festzustellen. Hierauf aufbauend ermöglichen dann die §§ 13 ff. speziell den Datenaustausch mit den Sicherheitsbehörden, um weitere Informationen zu den jeweiligen Gefangenen zu erlangen und gegebenenfalls eine hierauf abgestimmte Vollzugsplanung zu ermöglichen. Es besteht insofern ein gestufter Dreiklang aus Feststellung der Identität, gegebenenfalls durchzuführender Sicherheitsanfrage und Fallkonferenz bei fortbestehender Gefährlichkeit. Daneben besteht die Möglichkeit des punktuellen Informationsaustauschs nach den §§ 10 und 12.

Nach Absatz 1 prüfen die Justizvollzugsbehörden nach Maßgabe der §§ 14 und 15, ob sicherheitsrelevante Erkenntnisse über Gefangene und anstaltsfremde Personen, die Zugang zu den Justizvollzugsanstalten begehren, vorliegen. Absatz 1 ist als programmatischer Auftrag vor allem an die Justizvollzugsanstalten zu verstehen, bei Gefangenen und anstaltsfremden Personen stets eine sicherheitsbezogene Überprüfung nach § 14 und § 15 vorzunehmen. Davon unberührt bleibt, dass § 14 und § 15 ein Absehen von einer Überprüfung zulassen können, zum Beispiel, wenn die Sicherheitsanfrage im Ermessen der Justizvollzugsbehörden steht. Der Begriff der anstaltsfremden Person ist in § 2 Nummer 20 definiert.

Absatz 2 definiert den Begriff der sicherheitsrelevanten Erkenntnisse. Sicherheitsrelevant sind namentlich Erkenntnisse über extremistische, insbesondere gewaltorientierte Einstellungen oder Kontakte zu derartigen Organisationen, Gruppierungen oder Personen. Gleiches gilt für Kontakte zur organisierten Kriminalität. Die Auflistung ist nicht abschließend; sicherheitsrelevant können beispielsweise auch Erkenntnisse zu psychischen Auffälligkeiten von Gefangenen sein. Die Prüfkompetenz der Justizvollzugsanstalten im nachfolgenden § 15 wird dahingehend erweitert, dass nach Absatz 2 Satz 2 bei anstaltsfremden Personen, die an der Eingliederung von Gefangenen mitwirken, auch andere Erkenntnisse über erhebliche strafrechtliche Verurteilungen, eine bestehende Suchtproblematik oder andere für die Beurteilung der Zuverlässigkeit der Personen erhebliche Umstände sicherheitsrelevant sein können.

Zu § 14 Überprüfung Gefangener

Absatz 1 Satz 1 gibt den Justizvollzugsbehörden die Befugnis, sich mit einer Sicherheitsanfrage zu Gefangenen an die Justiz- und Sicherheitsbehörden zu wenden, wenn tatsächliche Anhaltspunkte für eine in einem überschaubaren Zeitraum drohende, einer oder einem Gefangenen zurechenbare Gefahr für die Sicherheit der Anstalt vorliegen.

Die drohende Gefahr begründet die Schwelle für den mit der Sicherheitsanfrage verbundeneren Eingriff in das Recht auf informationelle Selbstbestimmung des Gefangenen. Die Gefahrenprognose muss tatsächengestützt sein und darf sich nicht auf Vermutungen und allgemeine Erfahrungssätze stützen. Die „drohende Gefahr“ ist der konkreten Gefahr im polizeirechtlichen Sinne vorgelagert. Nicht die Verletzung des Schutzgutes „Sicherheit der Anstalt“ muss drohen, sondern eine Gefahr hierfür („Gefahr der Gefahr“). Es müssen folglich tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Sicherheit der Anstalt bestehen. Der zum Schaden führende Kausalverlauf muss noch nicht mit hinreichender Wahrscheinlichkeit vorhersehbar sein, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für die Sicherheit der Anstalt hindeuten. Ausreichend ist, dass ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, aus dem heraus die Verletzung der Sicherheit der Anstalt resultieren könnte. Aufgrund der als Voraussetzung in Satz 1 vorgesehenen „drohenden Gefahr“ sind daher nur relativ diffuse Anhaltspunkte für mögliche Gefahren für eine Sicherheitsanfrage demgegenüber ungenügend. Die Tatsachenlage ist dann häufig durch eine hohe Ambivalenz der Bedeutung einzelner Beobachtungen gekennzeichnet. Die Geschehnisse können in harmlosen Zusammenhängen verbleiben, aber auch den Beginn eines Vorgangs bilden, der in eine Gefahr mündet. Nicht ausreichend für eine Sicherheitsanfrage ist insoweit etwa allein die Erkenntnis, dass sich ein Gefangener zu einem fundamentalistischen Religionsverständnis hingezogen fühlt. Aufgrund der geforderten drohenden Gefahr ist auch eine Datenübermittlung, um überhaupt erst herauszufinden, ob eine Gefahr droht, ausgeschlossen. Die drohende Gefahr muss dem Gefangenen zurechenbar in dem Sinne sein, dass er in die Gefahrenlage als mutmaßlicher Störer „verstrickt ist“. Nach Absatz 1 Satz 1 steht es im Ermessen der Justizvollzugsbehörden („dürfen“) Justiz- und Sicherheitsbehörden bei Vorliegen einer drohenden Gefahr für die Sicherheit der Anstalt um Auskunft zu ersuchen. Zweck der Sicherheitsanfrage und des damit zusammenhängenden Datentransfers ist also der Schutz der Sicherheit der Anstalt vor einer drohenden Gefahr. Zu den Sicherheitsbehörden im Sinne der Bestimmung zählen die Polizeibehörden des Bundes und der Länder, die Verfassungsschutzbehörden der Länder sowie der Bundesnachrichtendienst und der militärische Abschirmdienst. Gleiches gilt für die entsprechenden Sicherheitsbehörden in den Mitgliedstaaten der Europäischen Union. Beispiele für Justizbehörden sind Gerichte, die Staatsanwaltschaften oder das Bundesamt für Justiz. Nach Absatz 1 Satz 2 Nummer 1 dürfen die Justizvollzugsbehörden insbesondere eine Auskunft nach § 41 Absatz 1 Nummer 1 des Bundeszentralregistergesetzes anfordern. Nach Absatz 1 Satz 2 Nummer 2 und 3 dürfen auch sicherheitsrelevante Erkenntnisse der Polizeibehörden des Bundes und der Länder und des Landesamtes für Verfassungsschutz angefragt werden. Entsprechend dem „Doppeltürmodell“ des Datenschutzrechtes, wonach es sowohl einer Befugnis für den Datenempfang als auch für die Datenabgabe bedarf, gibt Absatz 1 Satz 1 und 2 nur die Befugnis zu einer Datenanfrage. Absatz 1 Satz 3 konkretisiert den Begriff der drohenden Gefahr nach Absatz 1 Satz 1 dahingehend, dass sich tatsächliche Anhaltspunkte hierfür insbesondere aus Verurteilungen des Gefangenen und aus seinem Verhalten im Vollzug ergeben können. Hiermit sind auch Verurteilungen aus Strafverfahren, die der aktuellen Haft nicht zugrunde liegen sowie ein Vollzugsverhalten bei früheren Freiheitsstrafen angesprochen. Demgegenüber ist eine drohende Gefahr für die Sicherheit der Anstalt nach den Erfahrungen des Justizvollzugs beispielsweise eher fernliegend bei Gefangenen mit einem hohen Grundalter bei Aufnahme in den Vollzug, bei Gefangenen mit einer Direktaufnahme

in den offenen Vollzug und bei Gefangenen, die eine nur kurze Ersatzfreiheitsstrafe zu verbüßen haben.

Absatz 2 konkretisiert den Umfang und den konkreten Ablauf der Sicherheitsanfrage nach Absatz 1 Satz 2 Nummer 2 und 3. Insoweit wirkt die Bestimmung auch konkretisierend bezogen auf Anfragen bei den Polizeibehörden des Bundes und der Länder nach Absatz 1 Satz 1.

Absatz 3 regelt die mit der Sicherheitsanfrage im Zusammenhang stehende Datenübermittlung durch die Justizvollzugsbehörden an die angefragten Stellen. Das Ersuchen an die angefragten Behörden muss nach Absatz 3 Satz 1 die personenbezogenen Daten, insbesondere die gesicherten Identitätsdaten umfassen. Absatz 3 ist insoweit in einem Zusammenhang mit §§ 27 f. zu lesen, die es den Justizvollzugsbehörden ermöglichen, die Identität von Gefangenen sicher festzustellen. Über die Identitätsdaten hinaus sollen bekannt gewordene Aliaspersonalien, die voraussichtliche Vollzugsdauer sowie das Aktenzeichen der der Vollstreckung zugrunde liegenden Entscheidung mitgeteilt werden, um den angefragten Behörden eine sachhaltige Auskunft zu ermöglichen. Bei der Datenübermittlung nach Absatz 3 ist der enge Zweck der Datenübermittlung, die Anfrage nach sicherheitsrelevanten Erkenntnissen, zu berücksichtigen.

Nach Absatz 4 teilen die beteiligten Behörden den Justizvollzugsbehörden ihre sicherheitsrelevanten Erkenntnisse über Gefangene mit. Der Begriff der „sicherheitsrelevanten Erkenntnisse“ ist in § 13 Absatz 2 näher bestimmt. Für die Polizei- und Verfassungsschutzbehörden des jeweiligen Landes bedeutet diese Norm eine Befugnis zur Datenübermittlung an die jeweiligen Justizvollzugsbehörden. Mangels Gesetzgebungskompetenz ist die Bestimmung für Behörden anderer Länder, des Bundes und der Mitgliedstaaten der europäischen Union als bloßer Programmsatz zu verstehen, hier muss die Befugnis zur Datenübermittlung aus dem jeweiligen Fachrecht folgen.

Erst wenn sich aus den Anfragen nach Absatz 1 Satz 1 und Absatz 1 Satz 2 Hinweise auf eine konkrete Gefahr für die Sicherheit der Anstalt ergeben, steht es im Ermessen der Justizvollzugsbehörden („dürfen“), zusätzliche Auskünfte oder Unterlagen bei den Justiz- und Sicherheitsbehörden einholen. Wie aus der Formulierung „zusätzliche“ hervorgeht, handelt es sich hierbei um Informationen, die über die „sicherheitsrelevanten Erkenntnisse“ des Absatzes 4 hinausgehen. In Bezug auf die nicht näher bezeichneten Justiz- und Sicherheitsbehörden begründet Absatz 5 keine Übermittlungsbefugnis. Diese müssen in deren jeweiligen Fachgesetzen geregelt sein.

Absatz 6 bestimmt, dass die personenbezogenen Daten in gesonderten Akten oder Dateisystemen zu führen, das heißt zu verarbeiten und zu speichern, sind. Hintergrund ist der besondere Schutz dieser Daten, die sensible Informationen enthalten können.

Absatz 7 ermächtigt die Justizvollzugsbehörden, die im Rahmen der Sicherheitsanfrage gewonnenen Erkenntnisse zum Zweck der Vollzugs- und Eingliederungsplanung weiterzuverarbeiten. Zwar werden die Daten von den Justizvollzugsanstalten zuvörderst dafür benötigt, Sicherheitsrisiken vor Ort aufzudecken, um ihnen entgegenzutreten zu können. Stellt sich durch eine Sicherheitsanfrage aber heraus, dass Gefangene etwa besondere Radikalisierungstendenzen oder eine besondere Gewaltproblematik aufweisen, muss die Anstalt in die Lage versetzt werden, die betroffenen Gefangenen nicht nur zum Schutz Dritter sicher zu verwahren, sondern sie muss die Erkenntnisse auch im Besonderen für die weitere Vollzugs- und Eingliederungsplanung nutzen dürfen, nicht nur, um den Gefangenen zu helfen, sondern auch, um den Sicherheitsgefahren nachhaltig begegnen zu können. Beispielhaft zu nennen ist die Vermittlung des Gefangenen in spezifische Maßnahmenangebote zur Deradikalisierung oder zur Auseinandersetzung mit einer Gewaltproblematik. Es entspricht der Aufgabe des Justizvollzuges, die Allgemeinheit vor weiteren Straftaten zu schützen, indem einem als gefährlich einzustufenden Gefangenen ein auf ihn abgestimmtes

Behandlungsprogramm angeboten wird. Hierfür müssen die im Rahmen der Sicherheitsanfrage gewonnenen Erkenntnisse weiterverarbeitet werden können. Die Vorgaben zur Löschung der Daten und zu weiteren Rechten der betroffenen Personen folgen aus den übrigen Bestimmungen des Gesetzes.

Zu § 15 Überprüfung anstaltsfremder Personen

Absatz 1 Satz 1 statuiert den Grundsatz, dass anstaltsfremde Personen nur dann in einer Justizvollzugsanstalt tätig werden dürfen, wenn keine Sicherheitsbedenken bestehen. Der Begriff der anstaltsfremden Person ist in § 2 Nummer 20 definiert als eine Person, die zu den Justizvollzugsbehörden nicht in einem Dienst- oder Arbeitsverhältnis steht und nicht im Auftrag einer anderen Behörde tätig ist oder nicht als Organ der Rechtspflege handelt. Wie aus der Formulierung „in der Anstalt tätig werden sollen“ folgt, bezieht sich Satz 1 vor allem auf Fälle, in denen Dritte aus beruflichen Gründen Zugang zur Justizvollzugsanstalt begehren. Beispielhaft zu nennen sind insoweit Handwerksbetriebe oder der Anstaltskaufmann. Beispiele für eine nicht-berufliche Tätigkeit sind die Ableistung eines freiwilligen Praktikums oder die Tätigkeit im Rahmen eines Ehrenamtes. Auch Honorarkräfte oder Mitarbeiterinnen und Mitarbeiter externer Organisationen und Vereine unterfallen der Regelung. Eine Schlechterstellung anstaltsfremder Personen oder gar ein konkretes Misstrauen ist damit in keiner Weise verbunden, da auch für die eigenen Bediensteten des Vollzuges entsprechendes gilt. Im Ergebnis werden die anstaltsfremden Bediensteten den Anstaltsbediensteten gleichgestellt. Steht die Person zu den Justizvollzugsbehörden in einem Dienst- oder Arbeitsverhältnis oder soll sie im Auftrag einer anderen Behörde in der Justizvollzugsanstalt tätig werden, geht das Gesetz von der Fiktion aus, dass keine Sicherheitsbedenken bestehen. Personen, die zu der Anstalt oder der Aufsichtsbehörde nicht in einem Dienst- oder Arbeitsverhältnis stehen und die Anstalt im Auftrag einer anderen Behörde aufsuchen sind beispielsweise Bewährungshelferinnen und -helfer oder Polizeibeamtinnen und -beamte oder Referendarinnen und Referendare. Absatz 1 Satz 2 stellt klar, dass für den Regelfall („soll“) eine Zuverlässigkeitsprüfung durchzuführen ist. Die Zuverlässigkeitsprüfung soll zur Aufrechterhaltung der Sicherheit der Anstalt erfolgen. Eine Ausnahme von der regelhaft durchzuführenden Zuverlässigkeitsprüfung ist demnach immer dann angezeigt, wenn eine Gefährdung der Sicherheit der Anstalt fernliegend erscheint. Beispielhaft zu nennen sind solche anstaltsfremden Personen, die aufgrund ihrer Stellung und ihrer langjährigen Mitarbeit im Vollzug der Anstaltsleitung gut bekannt sind und denen die Anstalt aus guten Gründen bereits Vertrauen entgegen bringt. Weitere Beispiele sind die Mitarbeiterinnen und Mitarbeiter privater landeseigener Unternehmen, Bewerberinnen und Bewerber, die zu Vorstellungsgesprächen in eine Justizvollzugsanstalt kommen oder Vertreter von Unternehmen, die zu Vertragsverhandlungen dort anwesend sind. Die Zuverlässigkeitsprüfung hat mit Einverständnis der betroffenen Person zu erfolgen. Es bedarf daher ihrer zuvor erteilten Zustimmung. Um eine fundierte Entscheidung des Betroffenen zu ermöglichen, sind insbesondere der Anlass der Zuverlässigkeitsprüfung, ihr möglicher Umfang und die etwaigen Folgen einer verweigerten Zustimmung mitzuteilen. Absatz 1 Satz 3 gibt den Justizvollzugsbehörden die Befugnis zur Abfrage personenbezogener Informationen. Hierin eingeschlossen ist die Befugnis zur Übermittlung solcher Informationen, die für eine Zuverlässigkeitsüberprüfung von Polizei- und Verfassungsschutzbehörden notwendig sind, wie insbesondere der Identitätsdaten der anstaltsfremden Person. Die Anfrage bei Drittbehörden steht im Ermessen der Justizvollzugsbehörden („dürfen“). Bei der Ermessensentscheidung und der Anfrage ist der enge Zweck der Zuverlässigkeitsprüfung, die Sicherheit der Anstalt zu gewährleisten, zu berücksichtigen. Absatz 1 Satz 3 gibt nur die Befugnis zur Datenanfrage und zur Übermittlung der hierfür notwendigen Informationen. Gemäß dem „Doppeltürmodell“ des Datenschutzes muss die Befugnis der Drittbehörden zur Datenübermittlung an die Justizvollzugsbehörden aus deren jeweiligem Fachrecht folgen. Absatz 1 Satz 4 konkretisiert den Verhältnismäßigkeitsgrundsatz und erklärt, dass in Eilfällen an die Stelle der Zuverlässigkeitsprüfung die Beaufsichtigung der anstaltsfremden Person treten soll. Auch hiervon darf im Ausnahmefall abgewichen werden („soll“), wenn eine Gefährdung der Sicherheit der Anstalt fernliegend erscheint, beispielsweise, weil die Person dem Anstaltspersonal persönlich und als stets zuverlässig mit Blick auf Sicherheitsfragen bekannt ist.

Absatz 2 konkretisiert den Verhältnismäßigkeitsgrundsatz für die Ermessensentscheidung zur Datenabfrage nach Absatz 1 Satz 3. Danach soll von einem Datenaustausch abgesehen werden, wenn aufgrund des Anlasses, der Art, des Umfangs oder der Dauer des Aufenthalts oder der Tätigkeit in der Anstalt eine Gefahr für die Sicherheit der Anstalt fernliegend ist. Der im Datenaustausch liegende Eingriff in das Grundrecht auf informationelle Selbstbestimmung der anstaltsfremden Person ist insoweit mit der prognostisch festzustellenden Gefahr für die Sicherheit der Anstalt abzuwägen. Zu berücksichtigen ist hierbei etwa, ob die anstaltsfremde Person Kontakt zu Gefangenen hat und bei Ehrenamtlichen, mit welchem konkreten Angebot sie in die Anstalt kommen. Bei einer unklaren Ausgangslage darf die Datenabfrage weiterhin erfolgen, da in diesem Fall eine Gefahr für die Sicherheit der Anstalt nicht als fernliegend ausgeschlossen ist. Hierbei ist allerdings zu berücksichtigen, dass eine Zuverlässigkeitsüberprüfung der Justizvollzugsbehörden im Übrigen von Absatz 2 unberührt bleibt.

Absatz 3 hat die Zulassung zum Besuch von Gefangenen und der Justizvollzugsanstalt zum Gegenstand. Letzteres umfasst beispielsweise Maßnahmen der Resozialisierungs- und Öffentlichkeitsarbeit, etwa den Anstaltsbesuch, um einer Theaterveranstaltung von Gefangenen beizuwohnen. Anders als bei der Tätigkeit anstaltsfremder Personen steht hier nicht erst die Datenabfrage bei Drittbehörden, sondern bereits die Zuverlässigkeitsüberprüfung als solche im Ermessen der Justizvollzugsbehörden („dürfen“). Im Rahmen der Ermessensentscheidung sind die betroffenen Grundrechtspositionen zu berücksichtigen, beim Familienbesuch insbesondere das Grundrecht aus Artikel 6 GG und das aus dem Persönlichkeitsrecht der Gefangenen folgende Resozialisierungsziel. Zu berücksichtigen ist insoweit, dass der Zuverlässigkeitsprüfung eine abschreckende Wirkung zukommen kann. Die Ermessensentscheidung für eine Zuverlässigkeitsüberprüfung von Anstaltsbesucherinnen und -besuchern setzt voraus, dass tatsächliche Anhaltspunkte für eine drohende Gefahr der Sicherheit der Anstalt vorliegen. Die Gefahrenprognose muss also tatsachengestützt sein und darf sich nicht auf Vermutungen und allgemeine Erfahrungssätze stützen. Die „drohende Gefahr“ ist der konkreten Gefahr im polizeirechtlichen Sinne vorgelagert. Nicht die Verletzung des Schutzgutes „Sicherheit der Anstalt“ muss drohen, sondern eine Gefahr hierfür („Gefahr der Gefahr“). Tatsächliche Anhaltspunkte für eine drohende Gefahr der Sicherheit der Anstalt können insbesondere auch darin begründet sein, dass sicherheitsrelevante Erkenntnisse über einen Gefangenen vorliegen, der besucht werden soll. Die drohende Gefahr muss also nicht notwendigerweise von der Besucherin oder dem Besucher selbst ausgehen. Insoweit steht die Bestimmung in einem systematischen Zusammenhang zu Absatz 3 Satz 3. Absatz 3 dreht das „Regel-Ausnahme-Verhältnis“ der Absätze 1 und 2 insofern um, als die drohende Gefahr positiv festgestellt sein muss, bevor es zur Zuverlässigkeitsüberprüfung und den damit einhergehenden Eingriffen in die Betroffenenrechte kommt; diese unterbleiben nicht erst, wenn eine Gefahr für die Sicherheit der Anstalt als fernliegend ausgeschlossen werden kann. Hintergrund der Regelungssystematik ist, dass der Zugang anstaltsfremder Personen zu einer Justizvollzugsanstalt, um dort tätig zu werden, regelmäßig freiwillig erfolgt. Ein Tätigwerden in der Anstalt insbesondere aus beruflichen Gründen gibt darüber hinaus die Möglichkeit zu besonders weitgehenden Einblicken in die Abläufe der Justizvollzugsanstalt und ist daher in erhöhtem Maße gefahrgeneigt. Bei Gefangenenbesuchen nach Absatz 3 stehen demgegenüber Grundrechtspositionen der Gefangenen und der Betroffenen im Raum, die über das Grundrecht auf informationelle Selbstbestimmung hinausweisen (z. B. Artikel 6 GG) und die einen Besuch de facto als nicht vollständig freiwillig erscheinen lassen. Besuche erfolgen regelmäßig punktuell, beschränkt auf bestimmte Räumlichkeiten und lassen sich oftmals gut überwachen, so dass die Sicherheit der Anstalt vergleichsweise wenig gefährdet wird. Die Zuverlässigkeitsüberprüfung von Besucherinnen und Besuchern hat mit ihrem Einverständnis zu erfolgen. Es bedarf daher ihrer zuvor erteilten Zustimmung. Um eine fundierte Entscheidung der Besucherin oder des Besuchers zu ermöglichen, sind insbesondere der Anlass der Zuverlässigkeitsprüfung, ihr möglicher Umfang und die etwaigen Folgen einer verweigerten Zustimmung mitzuteilen. Absatz 3 Satz 2 verweist auf Absatz 1 Satz 3 und ermächtigt zur Datenabfrage bei Drittbehörden. Die Datenabfrage steht im Ermessen der Justizvollzugs-

behörden und ist auf den engen Zweck der Datenübermittlung, die Zuverlässigkeitsüberprüfung, beschränkt. Die Datenübermittlung durch die Justizvollzugsbehörden zum Zweck der Zuverlässigkeitsprüfung dürfte sich regelmäßig auf die Identitätsdaten der Besucherin oder des Besuchers beschränken. Absatz 3 Satz 3 erweitert die Befugnis zur Datenübermittlung an die Polizeibehörden und die Verfassungsschutzbehörden auf die Informationen, ob und für welchen Gefangenen die Zulassung zum Besuch begehrt wird.

Absatz 4 konkretisiert den Verhältnismäßigkeitsgrundsatz und nimmt Verteidigerinnen und Verteidiger, Beistände, Rechtsanwältinnen und Rechtsanwälte, Notarinnen und Notare sowie im Rahmen der Überwachung des Schriftwechsels der Gefangenen gesetzlich privilegierte Personen und Stellen von der Zuverlässigkeitsüberprüfung im Rahmen von Gefangenenbesuchen aus. Die geschützte Kommunikation der Gefangenen soll auch durch eine etwaig abschreckende Wirkung der Zuverlässigkeitsüberprüfung bei Gefangenenbesuchen nicht beeinträchtigt werden. Zudem gilt es, die genannten Gruppen aufgrund der ihnen zukommenden verfassungsmäßigen Rechte oder ihrer Rechtsstellung von einer Überprüfung auszunehmen.

Absatz 5 regelt die Folgen, wenn die Zuverlässigkeitsüberprüfung vom Betroffenen verweigert wird oder sich sicherheitsrelevante Erkenntnisse ergeben. Der Person wird nicht oder nur unter Beschränkungen Zutritt zur Justizvollzugsanstalt gewährt. Bei der Entscheidung sind die Grundrechtspositionen der Betroffenen zu berücksichtigen, insbesondere die Grundrechte der Gefangenen, der Resozialisierungsauftrag des Justizvollzuges sowie bei Familienbesuchen namentlich das Grundrecht aus Artikel 6 GG. Die betroffenen Rechtspositionen sind mit der festgestellten drohenden Gefahr oder Gefahr für die Sicherheit der Anstalt abzuwägen. Der Begriff der „sicherheitsrelevanten Erkenntnisse“ in Absatz 5 Satz 1 verweist auf § 13 Absatz 2. Absatz 5 verdeutlicht mit der Formulierung „werden [...] sicherheitsrelevante Erkenntnisse bekannt“, dass die Befugnis zur Zuverlässigkeitsprüfung nach Absatz 1 Satz 3 und Absatz 3 Satz 2 die Ermächtigung zum Empfang entsprechender Informationen von den angefragten Behörden beinhaltet.

Absatz 6 regelt die Wiederholung der Zuverlässigkeitsüberprüfung. Diese hat im Regelfall zu erfolgen („soll“), wenn neue sicherheitsrelevante Erkenntnisse nach § 13 Absatz 2 vorliegen. Gleiches gilt für den Fall, dass fünf Jahre seit der letzten Zuverlässigkeitsüberprüfung vergangen sind. Die Erforderlichkeit der erneuten Sicherheitsüberprüfung zur Gewährleistung der Sicherheit der Anstalt ist darzulegen. Der Erforderlichkeitsgrundsatz des Absatzes 6 dient der Umsetzung von Artikel 8 der Richtlinie (EU) 2016/680 und ist in deren Anwendungsbereich europarechtskonform auszulegen. Die Löschung der erhobenen Daten richtet sich nach §§ 59 f. Der Zeitpunkt der Erhebung von Daten anstaltsfremder Personen ist für die Kontrollfrist nach § 59 Absatz 2 von Bedeutung und daher zu dokumentieren.

Zu § 16 Fallkonferenzen

§ 16 hat Fallkonferenzen mit den Sicherheitsbehörden zum Gegenstand. Anders als dem punktuellen Datenaustausch wohnt diesen eine Dynamik insofern inne, als auf die jeweils ausgetauschte Information durch die empfangende Behörde unverzüglich reagiert und seinerseits der jeweils aktuelle Informationsstand mitgeteilt werden kann. Der Informationsaustausch baut hier aufeinander auf und kann dann aus dem Konferenzverlauf heraus an Umfang und Tiefe zunehmen. Fallkonferenzen sind ihrem Gegenstand nach oftmals nicht auf den bloßen Informationsaustausch begrenzt. Ziel ist es vielmehr, das Vorgehen der beteiligten Behörden untereinander abzustimmen und sich auf ein gemeinsames Vorgehen in der Sache zu einigen. Fallkonferenzen sind für die beteiligten Behörden insofern handlungsleitend. Die ausgetauschten Informationen sind Grundlage für das weitere operative Vorgehen. Die ausgetauschten Informationen dienen unmittelbar zu einem Tätigwerden den betroffenen Personen gegenüber. Sowohl die Dynamik des Informationsaustauschs im Rahmen von Fallkonferenzen als auch ihr handlungsleitender Charakter für die beteiligten Behörden begründen eine erhöhte Eingriffstiefe im Vergleich zum punktuellen Datenaustausch nach § 12. § 16 trägt der besonderen Eingriffstiefe Rechnung und schafft für Fallkonferenzen mit den Polizeibehörden des Bundes und der Länder sowie mit den Verfassungsschutzbehörden der Länder und dem Bundesamt für Verfassungsschutz eine normklare gesetzliche Regelung mit qualifizierten Eingriffsschwellen für die Übermittlung von Daten. § 16 unterscheidet zwischen Fallkonferenzen mit den Polizeibehörden des Bundes und der Länder (Absatz 1), Fallkonferenzen mit den Verfassungsschutzbehörden des Bundes und der Länder (Absatz 2) und Fallkonferenzen unter gleichzeitiger Beteiligung der Polizeibehörden des Bundes und der Länder und den Verfassungsschutzbehörden des Bundes und der Länder (Absatz 3) und legt hierfür jeweils eigenständige Voraussetzungen fest. Die Norm orientiert sich insoweit an der Rechtsprechung des Bundesverfassungsgerichts zum informationellen Trennungsprinzip. Danach unterliegen Regelungen, die den Austausch von Daten der Polizeibehörden und Nachrichtendienste ermöglichen, hinsichtlich des Grundrechts auf informationelle Selbstbestimmung gesteigerten verfassungsrechtlichen Anforderungen. Dass die Datenerhebungs- und Datenverarbeitungsbefugnisse der verschiedenen Behörden auf die jeweiligen Aufgaben zugeschnitten und dadurch begrenzt sind, ist von grundrechtlicher Bedeutung. Je verschiedenartiger Aufgaben, Befugnisse und Art der Aufgabenwahrnehmung sind, desto größeres Gewicht hat der Austausch entsprechender Daten (vgl. BVerfG, Urteil des Ersten Senats vom 24. April 2013 - 1 BvR 1215/07).

Absatz 1 Satz 1 ermächtigt die Justizvollzugsbehörden zur Übermittlung personenbezogener Daten an die Polizeibehörden des Bundes und der Länder im Rahmen von Fallkonferenzen. Die Einberufung der Fallkonferenz steht im Ermessen der Justizvollzugsbehörden, wie aus der Formulierung „dürfen“ hervorgeht. Klarstellend wird hervorgehoben, dass Gegenstand der Datenübermittlung auch der voraussichtliche Entlassungszeitpunkt, die voraussichtliche Entlassungsadresse sowie die Vollzugs- und Eingliederungspläne und auch besondere Kategorien personenbezogener Daten sein können. Die letztgenannte Gruppe von Daten ist in § 2 Nummer 14 näher bestimmt. Sofern biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person (§ 2 Nummer 14 Buchstabe c)) ausgetauscht werden, erweitert § 16 Absatz 1 als spezielle Ermächtigungsnorm die Übermittlungsbefugnisse nach § 27 Absätze 3 und 4. Voraussetzung für die Datenübermittlung ist, dass die Informationen zulässig erhoben wurden. Hiermit wird klargestellt, dass eine unzulässige Datenerhebung zu einer Löschung der Daten führen muss und deren weitere Verwendung im Rahmen einer Fallkonferenz ausgeschlossen ist. Als Übermittlungsschwelle nennt Absatz 1 Satz 1 tatsächliche Anhaltspunkte für die fortdauernde Gefährlichkeit der Gefangenen für die Allgemeinheit, einen voraussichtlichen Entlassungszeitpunkt in nicht mehr als einem Jahr und die Erforderlichkeit zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung. Die Voraussetzungen müssen kumulativ vorliegen. Eine fortdauernde

Gefährlichkeit der Gefangenen nach Absatz 1 Satz 1 Nummer 1 ist im Rahmen einer Gefahrenprognose für den Zeitpunkt der Entscheidung festzustellen. Die Prognose muss tatsächengestützt sein und darf nicht allein auf allgemeinen Erfahrungssätzen oder der bloßen Vermutungen beruhen. Das Erfordernis der fortdauernden Gefährlichkeit soll einen weitgehenden Gleichlauf mit den Voraussetzungen der Führungsaufsicht gewährleisten (§ 68 StGB). Die Fallkonferenz mit den Polizeibehörden des Bundes und der Länder setzt nach Absatz 1 Satz 1 Nummer 2 voraus, dass die betroffenen Personen aller Voraussicht nach in einem Zeitraum von nicht mehr als einen Jahr aus der Haft entlassen werden. Entscheidend ist die Vollzugsplanung im Zeitpunkt der Entscheidung. Die Bestimmung soll einer „Verpolizeilichung“ des Justizvollzuges entgegenwirken. Sie verdeutlicht die Ratio des Absatzes 1 Satz 1, einen Austausch mit den Polizeibehörden und ein mit diesen abgestimmtes Vorgehen zu ermöglichen zum Zweck einer koordinierten Entlassungsvorbereitung. Im Übrigen soll die Vollzugsplanung bei den Justizvollzugsbehörden verbleiben, wie auch Absatz 5 verdeutlicht. Absatz 1 Satz 1 Nummer 3 verdeutlicht, dass der Informationsaustausch im Rahmen der Fallkonferenz zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich sein muss. Die Anforderungen an die Gefahrenprognose der Nummer 1 werden insoweit konkretisiert. Es muss die Gefahr bestehen, dass die Gefangenen weitere Straftaten und nicht nur rechtswidrige Taten begehen werden. Straftaten von erheblicher Bedeutung sind insbesondere Verbrechen sowie schwerwiegende Vergehen. Die Straftat muss mindestens dem Bereich der mittleren Kriminalität zurechnen sein, den Rechtsfrieden empfindlich stören und dazu geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen. Entscheidend ist die konkrete Betrachtung im Einzelfall. Die Gefahr von Bagatelldelikten genügt den Anforderungen für eine Fallkonferenz nach § 16 nicht. Absatz 1 Satz 2 erlaubt eine Datenübermittlung im Rahmen einer Fallkonferenz an Polizeibehörden des Bundes und der Länder zur Vorbereitung von Ausführungen, Vorführungen, Ausantwortungen, Überstellungen und Verlegungen. Die im Ermessen der Justizvollzugsbehörde stehende Fallkonferenz dient hier also anders als im Satz 1 nicht der koordinierten Entlassungsvorbereitung, sondern soll die polizeiliche Absicherung der vorgenannten Vorgänge ermöglichen. Der im Vergleich zum Satz 1 begrenzte Zweck der Fallkonferenz ist beim Umfang der Datenübermittlung zu berücksichtigen. Voraussetzung für eine Fallkonferenz nach Satz 2 ist die Gefahr von Entweichungen, Gewalttätigkeiten gegen Personen oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, von Selbstverletzungen oder Selbsttötungen. Die Gefahrenprognose muss auf tatsächlichen Anhaltspunkten beruhen. Bloße Erfahrungswerte und Vermutungen sind insoweit unzureichend. Absatz 1 Satz 3 legt für den Regelfall („soll“) fest, dass an den Fallkonferenzen zur Entlassungsvorbereitung nach Satz 1 die Nachsorge, die Bewährungshilfe und die Führungsaufsichtsstellen zu beteiligen sind. Hierdurch soll sichergestellt werden, dass im Rahmen der Fallkonferenz eine Vielzahl von Einschätzungen Berücksichtigung findet, insbesondere auch solche, die nicht in den originären Aufgabenbereich der Polizeibehörden gehören, wie beispielsweise Fragen der sozialen und beruflichen Wiedereingliederung. Als Ausnahme vom Regelfall kann eine Fallkonferenz ohne Nachsorge, Bewährungshilfe und Führungsaufsichtsstelle stattfinden, wenn beispielsweise ganz überwiegend hochsensible Daten mit einem spezifischen Sicherheitsbezug ausgetauscht und hierüber weitergehend beraten werden soll. Im Rahmen der Ermessensentscheidung der Justizvollzugsbehörden bedarf eine solche Entscheidung der besonderen Begründung. Absatz 1 Satz 4 ermächtigt die Justizvollzugsbehörden, unter den Voraussetzungen des § 16 Absatz 1 Satz 1 und 2 personenbezogene Daten von den Polizeibehörden des Bundes und der Länder abzufragen und zu erheben. Die Bestimmung soll einer etwaigen „Schieflage“ von Justizvollzug und den Polizeibehörden entgegenwirken, wonach zwar eine Vielzahl von Informationen aus dem Justizvollzug heraus an die Sicherheitsbehörden übermittelt werden, umgekehrt aber nur wenige Informationen von den Sicherheitsbehörden in den Justizvollzug gelangen. Absatz 1 Satz 4 eröffnet den Justizvollzugsbehörden die Möglichkeit, bei den Polizeibehörden des Bundes und der Länder personenbezogene Informationen zu erheben, um ihren gesetzlichen Auftrag und die Vollzugsziele insbesondere bei solchen Gefangenen zu erfüllen, die sich bis zuletzt als fortdauernd gefährlich herausgestellt haben. Entsprechend dem „Doppeltürmodell“ des Daten-

schutzrechts gibt Absatz 1 Satz 4 nur die Befugnis des Justizvollzuges zur Abfrage und Erhebung von Daten. Die Befugnis der Polizeibehörden des Bundes und der Länder zur Datenübermittlung muss aus deren jeweiligem Fachrecht folgen. Gehören die zu übermittelnden Daten zur besonderen Kategorie personenbezogener Daten (§ 2 Nummer 14) ist die Übermittlung an eine andere öffentliche Stelle nur unter den Voraussetzungen des § 10 Absatz 3 zulässig, § 12 Absatz 6 Nummer 1. Nach § 10 Absatz 3 muss die Datennutzung für die in § 10 Absatz 2 genannten Zwecke unbedingt erforderlich sein. Gehören die zu übermittelnden Daten zur besonderen Kategorie personenbezogener Daten nach § 2 Nummer 14 ist die Übermittlung an die Polizeibehörden des Bundes und der Länder lediglich nur dann zulässig, wenn dies zur Zweckerfüllung unbedingt erforderlich ist. Gleiches gilt für die Erhebung solcher Daten bei den Polizeibehörden durch den Justizvollzug, § 10 Absatz 3.

Absatz 2 Satz 1 ermächtigt die Justizvollzugsbehörden zur Übermittlung personenbezogener Daten an die Verfassungsschutzbehörden des Bundes und der Länder im Rahmen von Fallkonferenzen. Die Einberufung der Fallkonferenz steht im Ermessen der Justizvollzugsbehörden, wie aus der Formulierung „dürfen“ hervorgeht. Absatz 2 Satz 1 ist von seiner Struktur her parallel zum Absatz 1 gefasst, so dass in weiten Teilen auf die vorstehende Begründung verwiesen werden kann. Bei den Schwellen zur Datenübermittlung weicht Absatz 2 von Absatz 1 ab. Absatz 2 trägt damit der Tatsache Rechnung, dass sich die Aufgaben der Polizeibehörden des Bundes und der Länder als Gefahrenabwehrbehörden und die Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder als Inlandsnachrichtendienste (Sammlung und Auswertung von Informationen) unterscheiden. Polizeibehörden und Verfassungsschutzbehörden sind gemäß dem informationellen Trennungsprinzip getrennt voneinander zu sehen, was der einheitlichen rechtlichen Einordnung als „ein Sicherheitskomplex“ entgegensteht. Absatz 2 spiegelt dies, indem er spezifisch auf die Verfassungsschutzämter zugeschnittene Befugnisse zur Datenübermittlung im Rahmen von Fallkonferenzen festlegt. Nach Absatz 2 Satz 1 dürfen personenbezogene Daten einschließlich solcher besonderer Kategorie an die Verfassungsschutzbehörden des Bundes und der Länder übermittelt werden, wenn bestimmte Tatsachen den Verdacht für Bestrebungen nach § 10 Absatz 2 Nummer 1 begründen, eine damit im Zusammenhang stehende Gefahr für die Sicherheit der Anstalt oder die Erreichung des Vollzugsziels in einem überschaubaren Zeitraum einzutreten droht und wenn dies zur Verhütung der vorgenannten Gefahren unbedingt erforderlich ist. Die Voraussetzungen müssen kumulativ vorliegen. Mit dem Verweis des § 16 Absatz 2 Satz 1 Nummer 1 auf Tätigkeiten oder Bestrebungen nach § 10 Absatz 2 Nummer 1 werden vor allem die dort genannten sicherheitsgefährdenden Tätigkeiten oder Bestrebungen, die durch Anwendung von Gewalt oder hierauf gerichtete Vorbereitungshandlungen gegen die freiheitlich demokratische Grundordnung oder die Sicherheit des Bundes oder eines Landes gerichtet sind, in Bezug genommen. Letztlich sind hiermit alle Bestrebungen gemeint, die den Aufgabenbereich der Verfassungsschutzämter eröffnen. Beispielhaft sind Bestrebungen aus dem Bereich des politischen oder des religiös begründeten Extremismus zu nennen. Der Verdacht für derartige Bestrebungen muss sich auf „bestimmte Tatsachen“ gründen. Vermutungen oder allgemeine Erfahrungssätze sind unzureichend. Absatz 2 Satz 1 Nummer 2 stellt klar, dass der bloße Verdacht von Tätigkeiten oder Bestrebungen, die in den Aufgabenbereich der Verfassungsschutzämter fallen, für eine Datenübermittlung unzureichend ist. Aufgrund der Tätigkeiten oder Bestrebungen muss entweder eine Gefahr für die Sicherheit der Anstalt oder die Erreichung des Vollzugsziels in einem überschaubaren Zeitraum einzutreten drohen. Absatz 2 Satz 1 Nummer 2 ist damit der konkreten Gefahr im polizeirechtlichen Sinne vorgelagert. Vorausgesetzt wird vielmehr eine drohende Gefahr („Gefahr der Gefahr“) für die Sicherheit der Anstalt oder die Erreichung eines der Vollzugsziele. Nicht der Schaden am Schutzgut, sondern eine Gefahr hierfür muss einzutreten drohen. Als Schutzgüter nennt Absatz 2 Satz 1 Nummer 2 die Sicherheit der Anstalt und die Erreichung des Vollzugsziels. Ausgehend vom Vollzugsziel, den Gefangenen zu befähigen, künftig in sozialer Verantwortung ein Leben ohne Straftaten zu führen, kann damit beispielsweise ein Datenaustausch mit den Verfassungsschutzämtern stattfinden, wenn aufgrund einer manifesten Radikalisierung Resoziali-

sierungserfolge nicht festzustellen sind. Die Gefahr für das Schutzgut „Vollzugsziel“ oder „Sicherheit der Anstalt“ muss der Norm nach „in einem überschaubaren Zeitraum“ einzutreten drohen. Es muss sich folglich um ein zeitlich absehbares Geschehen handeln. Nur relativ diffuse Anhaltspunkte für mögliche Gefahren, bei denen die Geschehnisse entweder in harmlosen Zusammenhängen verbleiben, oder auch den Beginn eines Vorgangs bilden können, der in einer Gefahr mündet, sind unzureichend. Allein die Erkenntnis, dass sich eine Person zu einem fundamentalistischen Religionsverständnis hingezogen fühlt, genügt zum Beispiel für die Annahme einer drohenden Gefahr nicht (vgl. BVerfG, Urteil des Ersten Senats vom 20. April 2016 - 1 BvR 966/09 -, Randnummer 113). Ebenfalls unzureichend ist der Austausch personenbezogener Daten mit den Verfassungsschutzbehörden, um überhaupt erst herauszufinden, ob eine drohende Gefahr vorliegt. Die drohende Gefahr ist Voraussetzung für die Fallkonferenz nach § 16 Absatz 2. Bedarf es insoweit einer weitergehenden Aufklärung des Sachverhalts, muss diese durch die Übermittlung nicht personenbezogener Informationen erfolgen. Nach Absatz 2 Satz 1 Nummer 3 muss die Datenübermittlung zur Verhinderung einer Gefahr für die Sicherheit der Anstalt oder das Erreichen des Vollzugszieles unbedingt erforderlich, das heißt im Sinne der Norm im konkreten Einzelfall unerlässlich sein. Dies ist im Rahmen der Ermessensentscheidung der Justizvollzugsbehörde zu berücksichtigen und steht standardisierten Fallkonferenzen mit den Verfassungsschutzbehörden entgegen. Da es sich bei den Verfassungsschutzbehörden anders als bei den Polizeibehörden nicht um Gefahrenabwehrbehörden handelt, übernimmt Absatz 2 Satz 1 nicht die Jahresfrist bis zur Entlassung des Satz 1 Satz 1 Nummer 2. Fallkonferenzen zum Informationsaustausch mit den Verfassungsschutzbehörden nach Absatz 2 sind daher während des gesamten Vollzuges möglich. Nach Absatz 2 Satz 2 sollen die Nachsorge, die Bewährungshilfe und die Führungsaufsichtsstellen an der Fallkonferenz beteiligt werden, sofern die Entlassung der Gefangenen in voraussichtlich nicht mehr als einem Jahr bevorsteht. Hierdurch soll sichergestellt werden, dass im Rahmen der Fallkonferenz eine Vielzahl von Einschätzungen Berücksichtigung findet, wenn die Entlassungsvorbereitung der Gefangenen bereits in Rede steht. Beispielhaft zu nennen sind solche Informationen, die nicht in den originären Aufgabenbereich der Verfassungsschutzbehörden gehören, wie beispielsweise Fragen der sozialen und beruflichen Wiedereingliederung. Als Ausnahme vom Regelfall kann eine Fallkonferenz ohne Nachsorge, Bewährungshilfe und Führungsaufsichtsstelle stattfinden, wenn beispielsweise ganz überwiegend hochsensible Daten mit einem spezifischen Sicherheitsbezug ausgetauscht werden sollen und hierüber weitergehend beraten werden soll. Im Rahmen der Ermessensentscheidung der Justizvollzugsbehörden bedarf eine solche Entscheidung der besonderen Begründung. Absatz 2 Satz 3 ermächtigt die Justizvollzugsbehörden, personenbezogene Daten von den Verfassungsschutzämtern des Bundes und der Länder abzufragen und zu erheben. Die Bestimmung soll einer etwaigen „Schieflage“ von Justizvollzug und den Verfassungsschutzbehörden entgegenwirken, wonach zwar eine Vielzahl von Informationen aus dem Justizvollzug heraus an die Sicherheitsbehörden übermittelt werden, umgekehrt aber nur wenige Informationen von den Sicherheitsbehörden in den Justizvollzug gelangen. Absatz 2 Satz 3 eröffnet den Justizvollzugsbehörden die Möglichkeit, bei den Verfassungsschutzbehörden des Bundes und der Länder personenbezogene Informationen zu erheben, um ihren gesetzlichen Auftrag und das Vollzugsziel insbesondere bei solchen Gefangenen zu erfüllen, die sich als extremistisch-gefährlich darstellen. Entsprechend dem „Doppeltürmodell“ des Datenschutzrechts gibt Absatz 2 Satz 3 nur die Befugnis des Justizvollzuges zur Abfrage und Erhebung von Daten. Die Befugnis der Verfassungsschutzbehörden des Bundes und der Länder zur Datenübermittlung muss aus deren jeweiligem Fachrecht folgen.

Absatz 3 ermächtigt die Justizvollzugsbehörden zum gleichzeitigen Austausch personenbezogener Daten mit den Polizeibehörden des Bundes und der Länder und mit den Verfassungsschutzbehörden des Bundes und der Länder im Rahmen von Fallkonferenzen. Die Einberufung der Fallkonferenz steht im Ermessen der Justizvollzugsbehörden, wie aus der Formulierung „dürfen“ hervorgeht. Bei den Schwellen zur Datenübermittlung weicht Absatz 3 Satz 1 von den Absätzen 1 und 2 ab. Absatz 3 trägt damit der Tatsache Rechnung, dass sich die Aufgaben der Polizeibehörden des Bundes und der Länder als Gefahrenabwehr-

behörden und die Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder als Inlandsnachrichtendienste (Sammlung und Auswertung von Informationen) unterscheiden, gemeinsame Fallkonferenzen aber gerade auf einen dynamischen Informationsaustausch über die jeweiligen Behördengrenzen hinweg angelegt sind. Ein Informationsaustausch zwischen Sicherheitsbehörden mit unterschiedlichen Aufgaben der insbesondere auch den Datenaustausch zwischen Polizei- und Sicherheitsbehörden umfasst, begründet nach der Rechtsprechung des Bundesverfassungsgerichts einen Grundrechtseingriff von erhöhtem Gewicht. Dies gilt in verstärktem Maße, wenn die ausgetauschten Informationen – wie bei einer Fallkonferenz regelmäßig üblich – in der Folge von den beteiligten Behörden handlungsleitend genutzt und damit den betroffenen Personen gegenüber zur operativen Anwendung gebracht werden. Der Datenaustausch ist in einem solchen Fall nur ausnahmsweise zulässig. Voraussetzung für die Überwindung des informationellen Trennungsprinzips ist, dass der Zugriff auf und die Nutzung der Daten dem Schutz besonders gewichtiger Rechtsgüter dient. Als Eingriffsschwelle nicht zu beanstanden ist eine gegenwärtige Gefahr für solche Schutzgüter. Die Gefahrenprognose muss durch bestimmte Tatsachen unterlegt sein (vgl. BVerfG, Urteil des Ersten Senats vom 24. April 2013 - 1 BvR 1215/07 -, Randnummern 112 ff., 201 ff.). Absatz 3 Satz 1 Nummern 1 bis 3 konkretisieren die verfassungsrechtlichen Vorgaben an einen Datenaustausch unter Überwindung des informationellen Trennungsprinzips und erlauben gemeinsame Fallkonferenzen von Justizvollzugsbehörden, Polizeibehörden und Verfassungsschutzbehörden wenn kumulativ eine gegenwärtige Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, vorliegt, wenn der Verdacht für Tätigkeiten oder Bestrebungen nach § 10 Absatz 2 Nummer 1 begründen und wenn der Informationsaustausch zur Gefahrenabwehr unbedingt erforderlich ist. Die Gefahrenprognose und der Verdacht von Tätigkeiten und Bestrebungen nach § 10 Absatz 2 Nummer 1 muss tatsächengestützt sein. Vermutungen und allgemeine Erfahrungssätze sind unzureichend. Gegenwärtig ist eine Gefahr, bei der die Einwirkung des schädigenden Ereignisses bereits begonnen hat oder bei der diese Einwirkung unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorsteht. Die Schutzgüter des Absatzes 3 Satz 1 Nummer 1 sind entsprechend den Bestimmungen des allgemeinen Polizeirechts auszulegen. Mit dem Verweis des Absatz 3 Satz 1 Nummer 2 auf Tätigkeiten oder Bestrebungen nach § 10 Absatz 2 Nummer 1 werden vor allem die dort genannten sicherheitsgefährdenden Tätigkeiten oder Bestrebungen, die durch Anwendung von Gewalt oder hierauf gerichtete Vorbereitungshandlungen gegen die freiheitlich demokratische Grundordnung oder die Sicherheit des Bundes oder eines Landes gerichtet sind, in Bezug genommen. Der Informationsaustausch ist nach Absatz 3 Satz 1 Nummer 3 zur Gefahrenabwehr unbedingt erforderlich, wenn er im konkreten Einzelfall hierfür unerlässlich ist. Absatz 3 Satz 2 erklärt Absatz 2 Satz 2 für entsprechend anwendbar. Auch bei gemeinsamen Fallkonferenzen mit Polizeibehörden und Verfassungsschutzbehörden sollen also die Nachsorge, die Bewährungshilfe und die Führungsaufsichtsstellen beteiligt werden, sofern die Entlassung der Gefangenen in voraussichtlich nicht mehr als einem Jahr bevorsteht. Hierdurch soll sichergestellt werden, dass im Rahmen der Fallkonferenz eine Vielzahl von Einschätzungen Berücksichtigung findet, wenn die Entlassungsvorbereitung der Gefangenen bereits in Rede steht. Beispielhaft zu nennen sind solche Informationen, die nicht in den originären Aufgabenbereich der Sicherheitsbehörden gehören, wie beispielsweise Fragen der sozialen und beruflichen Wiedereingliederung. Als Ausnahme vom Regelfall kann eine Fallkonferenz ohne Nachsorge, Bewährungshilfe und Führungsaufsichtsstelle stattfinden, wenn beispielsweise ganz überwiegend hochsensible Daten mit einem spezifischen Sicherheitsbezug ausgetauscht und hierüber weitergehend beraten werden soll. Absatz 3 Satz 3 ermächtigt die Justizvollzugsbehörden, personenbezogene Daten von den Verfassungsschutzämtern des Bundes und der Länder und von den Polizeibehörden des Bundes und der Länder im Rahmen der gemeinsamen Fallkonferenz abzufragen und zu erheben. Die Bestimmung soll einer etwaigen „Schieflage“ von Justizvollzug und den Sicherheitsbehörden entgegenwirken, wonach zwar eine Vielzahl von Informationen aus dem Justizvollzug heraus an die Sicherheitsbehörden übermittelt werden, umgekehrt aber nur wenige Informationen von den Sicherheitsbehörden in den Justizvoll-

zug gelangen. Absatz 3 Satz 3 eröffnet den Justizvollzugsbehörden die Möglichkeit, bei den Verfassungsschutzbehörden des Bundes und der Länder und bei den Polizeibehörden des Bundes und der Länder personenbezogene Informationen zu erheben, um ihren gesetzlichen Auftrag und das Vollzugsziel insbesondere bei solchen Gefangenen zu erfüllen, die sich als extremistisch darstellen und von denen zugleich eine gegenwärtige Gefahr für besonders gewichtige Schutzgüter ausgeht. Entsprechend dem „Doppeltürmodell“ des Datenschutzes gibt Absatz 3 Satz 3 nur die Befugnis des Justizvollzuges zur Abfrage und Erhebung von Daten. Die Befugnis der Verfassungsschutzbehörden des Bundes und der Länder und der Polizeibehörden des Bundes und der Länder zur Datenübermittlung muss aus deren jeweiligem Fachrecht folgen.

Nach § 16 Absatz 4 sind die wesentlichen Ergebnisse der Fallkonferenz zu dokumentieren. Die Dokumentation muss sachhaltig genug sein, um den erfolgten Datenaustausch und die gegebenenfalls erfolgte Festlegung auf ein einvernehmliches Vorgehen dergestalt nachvollziehen zu können, dass nachträglicher Rechtsschutz und eine nachträgliche Datenschutzkontrolle möglich sind.

§ 16 Absatz 5 stellt klar, dass die Vollzugs- und Eingliederungsplanung den Justizvollzugsbehörden vorbehalten bleibt. Absatz 5 ist in einem systematischen Zusammenhang mit den Absätzen 1 bis 3 zu lesen. Absatz 5 soll einer „Verpolizeilichung“ und einer „Vernachrichtendienstlichung“ des Justizvollzuges entgegenwirken. Er dient der Klarstellung, dass die Fallkonferenzen mit Polizeibehörden und Verfassungsschutzbehörden den Resozialisierungsauftrag des Justizvollzuges und dessen Verankerung bei den Justizvollzugsbehörden nicht in Frage stellen. Das Entscheidungsrecht über die Vollzugs- und Eingliederungsplanung liegt bei den Justizvollzugsbehörden und steht nicht unter einem etwaigen Primat oder Vorbehalt der Sicherheitsbehörden. Diese werden nur im konkreten Einzelfall und insoweit im Rahmen von Fallkonferenzen beteiligt, als es ihren gesetzlichen Aufgaben entspricht und die jeweiligen Voraussetzungen zur Datenübermittlung erfüllt sind.

Zu § 17 Weitere Zulässigkeitsvoraussetzungen für die Datenverarbeitung mit den Sicherheitsbehörden

Mit dem Urteil vom 20. April 2016 betreffend Regelungen des Bundeskriminalamtgesetzes hat das Bundesverfassungsgericht seine Rechtsprechung zur Datenerhebung und Datenweitergabe zusammengefasst, konsolidiert und fortentwickelt (vgl. BVerfG, Urteil des Ersten Senats vom 20. April 2016 - 1 BvR 966/09, Randnummer 292, m. w. N.). Der neue § 17 setzt das vom Bundesverfassungsgericht in der Entscheidung für den Datenaustausch mit den Sicherheitsbehörden konkretisierte Kriterium der hypothetischen Datenneuerhebung für den Bereich des Justizvollzugs um. Hintergrund hierfür ist die Erwägung, dass ein Datenaustausch nicht nur zwischen den verschiedenen Sicherheitsbehörden des Bundes und der Länder, sondern regelmäßig auch zwischen den Behörden des Justizvollzugs und den Sicherheitsbehörden stattfindet. Die ausgetauschten Informationen wurden dabei oftmals durch eingriffsintensive Überwachungsmaßnahmen wie den Eingriff in das Brief-, Post- und Fernmeldegeheimnis, die Überwachung der Hafträume der Gefangenen oder das Auslesen gefundener Datenträger und Mobiltelefone erlangt. Umgekehrt werden Informationen an die Justizvollzugsbehörden übermittelt und dort weiter verarbeitet, welche die Sicherheitsbehörden auf Grundlage mitunter schwerwiegender Grundrechtseingriffe erlangt haben. Das Bundesverfassungsgericht unterscheidet in seinem oben genannten Urteil hinsichtlich der weitergehenden Nutzung erhobener Daten entsprechend den Grundsätzen der Zweckbindung und der Zweckänderung. Eine weitere Nutzung bereits erhobener Daten innerhalb der ursprünglichen Zwecksetzung kommt dabei nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für die Datenerhebung maßgeblich waren (vgl. BVerfG, a. a. O., Randnummer 279). Da der Datenaustausch mit den Sicherheitsbehörden gerade auf die behördenübergreifende Wissenserweiterung angelegt ist, sind insoweit die verfassungsrechtlichen Vorgaben der Zweckänderung zu beachten. Hintergrund der verfassungsrechtlichen Vorgaben zur Zweckänderung ist, dass der Grundrechtseingriff der ursprünglichen Datenerhebung durch die Datenweitergabe und die neue Nutzung der Informationen vertieft wird. Dabei drohen die spezifischen Voraussetzungen, welche die Informationsgewinnung erlaubt haben, entwertet zu werden. Erlaubt der Gesetzgeber die weitere Nutzung von Daten zu anderen Zwecken als denen der ursprünglichen Datenerhebung (Zweckänderung), muss er folglich sicherstellen, dass dem Eingriffsgewicht der Datenerhebung auch hinsichtlich der neuen Nutzung Rechnung getragen wird. Die Ermächtigung zu einer Zweckänderung ist dabei am Verhältnismäßigkeitsgrundsatz zu messen. Hierbei orientiert sich das Gewicht, das einer solchen Regelung im Rahmen der Abwägung zukommt, am Gewicht des Eingriffs der Datenerhebung. Dabei unterscheidet das Bundesverfassungsgericht jeweils zwischen Gefahrentatbestand und Schutzgut einerseits und Tatverdacht und Straftatbestand andererseits. Voraussetzung für eine Zweckänderung ist jedenfalls, dass die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten (Grundsatz der hypothetischen Datenneuerhebung). Nicht in jedem Fall identisch sind die Voraussetzungen einer Zweckänderung mit denen einer Datenerhebung hingegen hinsichtlich des erforderlichen Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts. Verfassungsrechtlich geboten, aber regelmäßig auch ausreichend ist insoweit, dass sich aus den Daten ein konkreter Ansatz ergibt (vgl. BVerfG, a. a. O., Randnummern 286 ff.). Der Gesetzgeber kann danach - bezogen auf die Datennutzung von Sicherheitsbehörden - eine Zweckänderung von Daten grundsätzlich dann erlauben, wenn es sich um Informationen handelt, aus denen sich im Einzelfall konkrete Ansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter wie die ergeben, zu deren Schutz die entsprechende Datenerhebung zulässig ist (BVerfG, a. a. O., Randnummer 290). Anderes gilt für Informationen aus Wohnraumüberwachungen oder

dem Zugriff auf informationstechnische Systeme. Angesichts des besonderen Eingriffsgewichts dieser Maßnahmen muss für sie jede neue Nutzung der Daten wie bei der Datenerhebung selbst auch durch eine dringende Gefahr oder eine im Einzelfall hinreichend konkretisierte Gefahr gerechtfertigt sein (BVerfG, a. a. O., Randnummer 291). Der verfassungsrechtliche Grundsatz der hypothetischen Datenneuerhebung wird für den Informationsaustausch mit den Sicherheitsbehörden im neuen § 17 als allgemeiner Grundsatz definiert, der bei der Übermittlung von Daten an die Sicherheitsbehörden und bei der Erhebung von Daten bei diesen – unabhängig von der jeweiligen Eingriffsintensität der ursprünglichen Datenerhebung – zu beachten ist. Die Normstruktur ist dabei an § 12 des neuen Bundeskriminalamtgesetzes angelehnt. Hierdurch soll dem Petition der Innenminister von einer Angleichung der Rechtsvorschriften verschiedener Behörden mit Sicherheitsaufgaben Rechnung getragen werden. Perspektivisch soll zudem ein weitgehender Gleichlauf der Verwaltungspraxis von Justizvollzug und Sicherheitsbehörden beim Datenaustausch und in der Frage der hypothetischen Datenneuerhebung ermöglicht werden.

Absatz 1 übernimmt die Vorgaben des Bundesverfassungsgerichts an die zweckändernde Übermittlung personenbezogener Daten an Sicherheitsbehörden und führt damit den Grundsatz der hypothetischen Datenneuerhebung in das Justizvollzugsdatenschutzgesetz ein (vgl. BVerfG, a. a. O., Randnummern 288 bis 290). Die Norm ist im Zusammenhang mit den Befugnisnormen zum Datenaustausch mit den Sicherheitsbehörden zu lesen und begründet selbst keine Übermittlungsbefugnis. Absatz 1 übernimmt die verfassungsrechtlichen Vorgaben dahingehend, dass eine Übermittlung von Daten an Sicherheitsbehörden nur dann zulässig ist, wenn solch schwerwiegende Straftaten oder Ordnungswidrigkeiten verhütet, aufgedeckt oder verfolgt werden oder mindestens vergleichbar gewichtige Rechtsgüter geschützt werden, dass ein im Vergleich zur Datenerhebung gleichwertiger Rechtsgüterschutz sichergestellt ist. Darüber hinaus bedarf es im Einzelfall konkreter Ansätze zur Verhütung, Aufdeckung, oder Verfolgung von Straftaten oder Ordnungswidrigkeiten oder zur Abwehr von in einem überschaubaren Zeitraum drohenden Gefahren. Der Grundsatz der hypothetischen Datenneuerhebung wird hierbei in das Justizvollzugsdatenschutzgesetz eingeführt, ohne auf besonders eingriffsintensive Maßnahmen beschränkt zu sein. Der Begriff der „Sicherheitsbehörden“ meint die Polizeibehörden des Bundes und der Länder, die Landesämter und das Bundesamt für Verfassungsschutz sowie den Bundesnachrichtendienst und den militärischen Abschirmdienst. Gleiches gilt für die entsprechenden Sicherheitsbehörden in den Mitgliedstaaten der Europäischen Union. Mit der Datenübermittlung „zum Zwecke der Gefahrenverhütung, zum Zwecke der Gefahrenabwehr, zur Verhinderung oder Verfolgung von Ordnungswidrigkeiten, zur Verhinderung oder Verfolgung von Straftaten oder zu den in § 10 Absatz 2 Nummer 1 genannten Zwecken“ ist die gesamte Tätigkeit der Sicherheitsbehörden auf dem Zeitstrahl erfasst, von der Erstellung von Lagebildern durch die Ämter für Verfassungsschutz über die klassische Gefahrenabwehr der Polizeibehörden bis zur Verfolgung von Straftaten und Ordnungswidrigkeiten. Der Begriff „im Einzelfall konkrete Ansätze zur Verhütung, Aufdeckung oder Verfolgung der Straftaten oder Ordnungswidrigkeiten“ bleibt hinter dem Tatverdacht im strafprozessualen Sinne zurück. Gemeint ist ein spezifischer Anlass im Einzelfall zum Beispiel in Form eines konkreten Ermittlungsansatzes, aus dem sich die Datenübermittlung rechtfertigt. Eine Datenübermittlung „ins Blaue hinein“ und allein getragen von der Hoffnung auf Erkenntnisse ist ausgeschlossen. Der Begriff „im Einzelfall konkrete Ansätze [...] zur Abwehr von in einem überschaubaren Zeitraum drohenden Gefahren [...] für bedeutsame Rechtsgüter“ schließt eine Datenübermittlung „ins Blaue hinein“ und getragen allein von der Hoffnung auf Erkenntnisse ebenfalls aus. Vielmehr bedarf es eigenständiger Anhaltspunkte etwa aus den vorliegenden Informationen selbst, dass eine Gefahrenlage entstehen könnte („Gefahr einer Gefahr“). Ausreichend ist danach, dass ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, aus dem heraus eine Rechtsgutsverletzung resultieren könnte. Gleiches gilt, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass es in überschaubarer Zukunft zur Schädigung eines Schutzgutes kommt. Die „in einem überschaubaren Zeitraum drohende Gefahr“ ist der konkreten Gefahr im polizeirechtlichen Sinne folglich vorgelagert. Eine Datenübermittlung

an die Sicherheitsbehörden, um überhaupt erst herauszufinden, ob eine Gefahr droht, ist gleichwohl ausgeschlossen. Mit der Formulierung „im Vergleich zur Datenerhebung gleichwertiger Rechtsgüterschutz“ wird normativ erfasst, dass sich das Gewicht des Grundrechtseingriffs der Datenweitergabe am Grundrechtseingriff der Datenerhebung zu orientieren hat. Die „Vergleichbarkeit“ folgt aus den rechtsgutsbezogenen Erhebungsschwellen in Form einer „Gewichtungsklasse“, welche die Rechtsgüter oberhalb dieser Schwelle umfasst. Bei Informationen aus einer Maßnahme der Gefahrenabwehr ist insoweit auf das Schutzgut Bezug zu nehmen, das der Datenerhebung zugrunde lag. Bei Informationen aus einer Strafverfolgungsmaßnahme bedarf die aufzuklärende Straftat der näheren Einordnung. Wenn zum Beispiel § 24 JVollzDSG SH eine gegenwärtige Gefahr für Leib oder Leben voraussetzt, um die optisch-elektronische Überwachung eines Haftraums zu ermöglichen, dürften Zufallserkenntnisse aus einer solchen Überwachung zur Abwehr einer Freiheitsgefahr verwendet werden. Die Abwehr der Freiheitsgefahr erscheint zwar gegenüber der Abwehr der Lebensgefahr (als ursprünglichem Erhebungszweck) nicht gleichgewichtig, mit Blick auf die Erhebungsschwelle der Art der jeweiligen Maßnahme aber vergleichbar gewichtig. Anderes würde zum Beispiel bei der Nutzung solcher Informationen zur Verfolgung eines Beleidigungsdeliktes als strafrechtliches Antragsdelikt gelten. Der Begriff des Rechtsgutes bezieht sich auf Individualrechtsgüter und Universalrechtsgüter. Besonders bedeutsame Individualrechtsgüter sind insbesondere das Leben, die Freiheit, die körperliche Unversehrtheit oder die sexuelle Selbstbestimmung. Besonders bedeutsame Universalrechtsgüter sind beispielsweise der Schutz der Sicherheit der Bundesrepublik Deutschland oder eines Landes oder der Schutz der freiheitlich demokratischen Grundordnung (vgl. BVerfG, a. a. O., Randnummer 100). Das Kriterium des gleichwertigen Rechtsgüterschutzes von Datenerhebung und Datenweitergabe an die Sicherheitsbehörden stellt sich für die Behörden des Justizvollzuges als vergleichsweise unproblematisch dar. Regelmäßig lassen die Justizvollzugsgesetze Datenerhebungen unter Voraussetzungen zu, die im Vergleich zu den Eingriffsschwellen der Polizeigesetze erheblich abgesenkt sind. § 34 BremStVollzG beispielsweise erlaubt die Überwachung des Schriftwechsels schon dann, wenn dies „aus Gründen der Sicherheit“ oder zur Abwehr der „Gefährdung der Erreichung des Vollzugszieles“ erforderlich ist. Da der Grundrechtseingriff der Datenweitergabe sich am Grundrechtseingriff der Datenerhebung orientieren muss und weil die Voraussetzungen der Datenerhebung bei der Datenweitergabe fortwirken, sind die vergleichsweise niedrigen Datenerhebungsschwellen bei der Datenweitergabe an die Sicherheitsbehörden zu berücksichtigen. Die Übermittlungsschwellen des § 17 Absatz 1 gewährleisten, dass es nicht zu einer Datenübermittlung an Sicherheitsbehörden kommt zur allgemeinen Unterstützung bei deren Aufgabenwahrnehmung. Eine Datenübermittlung schon weil dies „erforderlich ist zur Aufgabenwahrnehmung und der Wahrung der öffentlichen Sicherheit“ oder weil „Tatsachen den Verdacht begründen, dass die Daten zur Aufgabenerfüllung erforderlich sind“ ist – den verfassungsrechtlichen Vorgaben entsprechend (vgl. BVerfG, a. a. O., Randnummern 293 ff.) – unzulässig. Konkret bedeutsam ist dies beispielsweise mit Blick auf eine Datenübermittlung nach § 10 Absatz 2 Nummer 1 in Verbindung mit § 12 Absatz 3 Nummer 2 Buchstabe j), der isoliert betrachtet einen Datenaustausch an die Verfassungsschutzämter bereits zulässt, wenn dies für deren Aufgabenerfüllung erforderlich ist.

Absatz 2 regelt, dass die Vorgaben zur Datenübermittlung an die Sicherheitsbehörden umgekehrt auch gelten, wenn die Justizvollzugsbehörden Informationen von diesen übermittelt bekommen. Insoweit werden die Vorgaben des Bundesverfassungsgerichts an die zweckändernde Übermittlung personenbezogener Daten durch die Sicherheitsbehörden übernommen. Das Kriterium der hypothetischen Datenerhebung ist zu beachten, wenn Daten erhoben werden „zum Zwecke der Gefahrenverhütung, zum Zwecke der Gefahrenabwehr, zur Verhinderung oder Verfolgung von Ordnungswidrigkeiten oder zur Verhinderung oder Verfolgung von Straftaten“. Angesprochen ist damit zuvörderst die Datenerhebung bei den Sicherheitsbehörden zum Zwecke der Gewährleistung der Sicherheit der Anstalt. Auf dem Zeitstrahl wird der gesamte Bereich von der Verhinderung des Eintritts einer Gefahrenlage über die Gefahrenabwehr bis zur Strafverfolgung erfasst. Mit der „Gefahrenverhütung“ ist der Auftrag des Justizvollzuges erfasst, die Allgemeinheit vor weiteren Straf-

taten zu schützen. Absatz 2 bezieht sich ebenso wie Absatz 1 auf den Schutz von Individualrechtsgütern und von Universalrechtsgütern. Den im Rahmen des Justizvollzuges in Rede stehenden Rechtsgütern kommt regelmäßig ein hohes Gewicht zu. Beispielhaft zu nennen sind insoweit das aus dem allgemeinen Persönlichkeitsrecht der Gefangenen und dem Sozialstaatsprinzip abgeleitete Resozialisierungsgebot, die Gewährleistung der Sicherheit der Anstalt, der Schutz der Allgemeinheit vor Straftaten oder auch die Sicherung des Strafverfahrens in der Untersuchungshaft. Mit der Sicherheit der Anstalt sind zugleich gewichtige Rechtsgüter wie Leben, die Freiheit, die körperliche Unversehrtheit oder die sexuelle Selbstbestimmung angesprochen, darüber hinaus die Gewährleistung eines resozialisierungsförderlichen Umfeldes. Ein Datenaustausch von den Sicherheitsbehörden zu den Justizvollzugsbehörden dürfte danach in weitem Umfang möglich sein. Absatz 2 gilt ebenso wie Absatz 1 nur für personenbezogene Daten. Werden seitens der Sicherheitsbehörden also Informationen ohne Personenbezug übermittelt, beispielsweise zur Einschätzung eines Buches, findet § 17 keine Anwendung.

Absatz 3 trägt den besonderen Anforderungen des Bundesverfassungsgerichts an die zweckändernde Nutzung von Daten Rechnung, die durch den Einsatz technischer Mittel in oder aus Wohnungen und durch verdeckte Eingriffe in informationstechnische Systeme erlangt wurden. Absatz 3 bezieht sich zwar nur auf Absatz 1 Nummer 1 Buchstabe b, gilt aber sowohl für den Empfang von Informationen der Sicherheitsbehörden als auch für die Übermittlung von Informationen an die Sicherheitsbehörden, da Absatz 2 auf Absatz 1 Bezug nimmt. Die Übermittlung von personenbezogenen Daten, die durch den Einsatz technischer Mittel in oder aus Wohnungen gewonnen wurden, ist gemäß Absatz 3 Nummer 1 im Falle des Vorliegens einer Gefahr nur möglich, wenn – wie Artikel 13 Absatz 4 GG bestimmt – im Einzelfall eine dringende Gefahr besteht. Als Schutzgüter nennt Absatz 3 Nummer 1 den Bestand oder die Sicherheit des Bundes oder eines Landes, Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist. Die Schutzgüter entsprechen den Vorgaben des allgemeinen Polizeirechts für den Einsatz technischer Mittel in oder aus Wohnungen und sind entsprechend auszulegen (vgl. BVerfG, a. a. O., Randnummer 183). Der Haftraum unterfällt nicht dem Schutzbereich des Artikel 13 GG. Dementsprechend werden dort keine Daten durch den „Einsatz technischer Mittel in oder aus Wohnungen“ gewonnen (vgl. BVerfG, Kammerbeschluss vom 30. Mai 1996 – 2 BvR 727/94). Die Übermittlung so gewonnener Informationen an die Sicherheitsbehörden unterfällt Absatz 3 Nummer 1 folglich nicht. Hinsichtlich des gleichwertigen Rechtsgüterschutzes von Datenerhebung und Datenübermittlung ist indes zu beachten, dass die Achtung der Menschenwürde und insbesondere der Privat- und Intimsphäre als Ausdruck des allgemeinen Persönlichkeitsrechts auch bezüglich des Haftraums von Gefangenen angezeigt ist. Dabei ist anzuerkennen, dass der gesonderte Haftraum für Gefangene regelmäßig die einzige verbleibende Möglichkeit bietet, sich eine gewisse Privatsphäre zu verschaffen und ungestört zu sein (vgl. BVerfG, Kammerbeschluss, a. a. O., Randnummer 13 f.). Da die Übermittlung von personenbezogenen Daten, die durch den Einsatz technischer Mittel in einem Haftraum gewonnen wurden, nicht Absatz 3 Nummer 1 unterfällt, ist der Anwendungsbereich der Bestimmung sehr gering. Absatz 3 Nummer 1 dürfte (in Verbindung mit Absatz 2) vor allem Anwendung finden, wenn es um den Empfang entsprechender Daten durch die Sicherheitsbehörden geht. Werden solche Informationen dann in einem nächsten Schritt vom Justizvollzug an andere Sicherheitsbehörden weiterübermittelt, ist Absatz 3 Nummer 1 ebenfalls einschlägig. Die Übermittlung von personenbezogenen Daten, die durch einen verdeckten Eingriff in informationstechnische Systeme erlangt wurden, ist gemäß Absatz 3 Nummer 2 nur zulässig, wenn im Einzelfall bestimmte Tatsachen jedenfalls die Annahme rechtfertigen, dass innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Schädigung von Leib, Leben oder Freiheit einer Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt, eintritt. Der Gefahrentatbestand ist der konkreten Gefahr im polizeirechtlichen Sinne vorgelagert und nimmt die entsprechende Rechtsprechung des Bundesverfassungsgerichts auf (vgl. BVerfG, a. a. O.,

Randnummer 213). Die Schutzgüter entsprechen denen des allgemeinen Polizeirechts für den verdeckten Eingriff in informationstechnische Systeme und sind entsprechend auszu-legen. Gegenstand des Absatzes 3 Nummer 2 sind Daten, die Durch den verdeckten Zu-griff auf das Telekommunikationsendgerät des Betroffenen erlangt wurden, insbesondere dessen Festplatte. Werden Mobiltelefone beschlagnahmt und in der Folge ausgelesen, dürfte es sich nicht um den verdeckten Zugriff auf ein informationstechnisches System handeln (vgl. BVerfG, Urteil des Zweiten Senats vom 02. März 2006 - 2 BvR 2099/04 -, Randnummern 93 ff.). Anderes gilt für das Auslesen zum Beispiel über das Internet. Der praktische Anwendungsbereich des Absatzes 3 Nummer 2 dürfte für den Justizvollzug da-her, vergleichbar dem Absatz 3 Nummer 1, gering sein. Absatz 3 Nummer 2 dürfte (in Ver-bindung mit Absatz 2) vor allem Anwendung finden, wenn es um den Empfang entspre-chender Daten durch die Sicherheitsbehörden geht. Werden solche Informationen dann in einem nächsten Schritt vom Justizvollzug an andere Sicherheitsbehörden weiterübermittelt, ist Absatz 3 Nummer 2 ebenfalls einschlägig.

Absatz 4 sieht durch seinen Verweis auf den erkennungsdienstlichen Datenaustausch nach § 28 und § 35 Absatz 4 vor, dass die Vorgaben der Zweckbindung und der Grundsatz der hypothetischen Datenneuerhebung nicht gelten, wenn die Grunddaten einer Person zu Identifizierungszwecken verwendet werden sollen. Dies entspricht der Rechtsprechung des Bundesverfassungsgerichts zur Abfrage und Nutzung von einfachen Grunddaten zum Zweck der Identifizierung (vgl. BVerfG, Urteil des Ersten Senats vom 24. April 2013 - 1 BvR 1215/07 -, Randnummern 193 ff.). Die Datenverwendung ist hier durch die bloße Nutzung von Grunddaten und den Nutzungszweck der Identifizierung in doppelter Weise eng be-grenzt, das Eingriffsgewicht der Datenübermittlung entsprechend reduziert. Weitere Daten – etwa die weiteren zu einer als „Treffer“ identifizierten Person gespeicherten Erkenntnisse – sind hingegen von Absatz 4 nicht erfasst; insoweit bleibt es bei den Vorgaben der Absät-ze 1 bis 3.

Zu § 18 Verantwortung für die Übermittlung und Verfahren

Absatz 1 entspricht § 12 Satz 1 JVollzDSG SH in der bisherigen Fassung; Absatz 6 stimmt wiederum mit § 13 Absatz 1 JVollzDSG SH in der bisherigen Fassung überein.

Absatz 1 überträgt die Verantwortung für die Prüfung der Zulässigkeit einer Übermittlung personenbezogener Daten grundsätzlich der übermittelnden Justizvollzugsbehörde.

Nach Absatz 2 Satz 1 trägt bei einer Übermittlung auf Ersuchen einer öffentlichen Stelle jedoch diese die Verantwortung, die sich ihrerseits für die Datenerhebung auf eine Rechtsgrundlage stützen muss. Satz 2 regelt in diesem Fall das Verfahren zur Prüfung der Zulässigkeit einer Übermittlung.

Absatz 3 regelt das Verfahren bei Ersuchen einer nichtöffentlichen Stelle, damit die Justizvollzugsbehörden die nötige Prüfung der Zulässigkeit einer Übermittlung personenbezogener Daten durchführen können.

Absatz 4 und 5 dienen der Umsetzung von Artikel 7 Absatz 2 der Richtlinie (EU) 2016/680 hinsichtlich der Überprüfung der Qualität der personenbezogenen Daten. Die Beschränkung auf die Übermittlung personenbezogener Daten zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit in Absatz 3 resultiert aus dem Anwendungsbereich der Richtlinie gemäß Artikel 1 Absatz 1 Richtlinie (EU) 2016/680. Absatz 5 soll nämlich nur für den Anwendungsbereich der Richtlinie (EU) 2016/680 gelten.

Absatz 6 ist Ausfluss des Erforderlichkeitsgrundsatzes. Typischerweise ist die Übermittlung personenbezogener Daten, die einer konkreten Person zugeordnet werden können, an nichtöffentliche Stellen nicht erforderlich. Um die betroffenen Personen zu schützen, sind diese Daten deshalb grundsätzlich zu pseudonymisieren. Pseudonymisierung ist in § 2 Nummer 7 legaldefiniert. Nur sofern die Pseudonymisierung der Erfüllung des Übermittlungszwecks zuwider läuft, ist ausnahmsweise von der Pseudonymisierung Abstand zu nehmen. Die Gefangenenbuchungsnummer ist im Justizvollzug ein praktikables Instrument, um den Interessen der Gefangenen an der Pseudonymisierung gerecht zu werden. Für die Verarbeitung von Daten im Auftrag (§ 24) gilt Absatz 6 entsprechend, auch dort soll die Pseudonymisierung erfolgen. Auch bei der Inanspruchnahme von Telekommunikations- und Mediendienstleistungen bei nichtöffentlichen Stellen (§ 12 Absatz 2 Nummer 2 Buchstabe d)) sind die Daten ohne Ausnahme zu pseudonymisieren.

Zu § 19 Förmliche Verpflichtung Dritter

§ 19 entspricht § 14 Absatz 1 bis 3 JVollzDSG SH in der bisherigen Fassung.

Die Bestimmung ergänzt § 5 und stellt sicher, dass Mitarbeiterinnen und Mitarbeiter nicht-öffentlicher Stellen, denen personenbezogene Daten von den Justizvollzugsbehörden übermittelt wurden, über ihre Pflicht zur Verschwiegenheit belehrt und auf die gewissenhafte Erfüllung ihrer Obliegenheiten verpflichtet werden. Dies beinhaltet insbesondere die Verpflichtung zur Verschwiegenheit gegenüber Dritten und das Verbot, personenbezogene Daten zu einem anderen als dem zur Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder unbefugt zu offenbaren.

Nach § 24 Absatz 8 gilt für die Verarbeitung von Daten im Auftrag § 19 entsprechend.

Zu § 20 Mitteilung über Haftverhältnisse

§ 20 fußt weitgehend auf § 15 JVollzDSG SH in der bisherigen Fassung.

Absatz 1 regelt, in welchem Umfang die Justizvollzugsbehörden Auskunft über die genannten Haftverhältnisse geben dürfen. Auch hier erfolgt eine sachgerechte Differenzierung zwischen öffentlichen und nichtöffentlichen Stellen. Bei Letzteren sind die Interessen des Gefangenen ausdrücklich in die Prüfung mit einzubeziehen. Die nichtöffentlichen Stellen müssen ihr Interesse glaubhaft darlegen, z.B. Darstellung einer Forderung und der beabsichtigten weiteren Schritte wie gerichtlicher Geltendmachung oder Zwangsvollstreckung unter Vorlage des Titels. Die Justizvollzugsbehörden trifft keine Pflicht zur Überprüfung der Rechtmäßigkeit der angestrebten Maßnahmen.

Die Absätze 2 und 3 regeln die Auskunft an unmittelbar und mittelbar von einer Straftat betroffene Personen. Auch Rechtsnachfolgerinnen und Rechtsnachfolger sind auskunftsberechtigt. Sollte im Rahmen der Straftat öffentliches Eigentum beschädigt worden sein, ist auch die öffentliche Hand als Verletzte einer Straftat anzusehen. Absatz 2 Nummer 2 und 3 sind § 406 d Absatz 2 Nummer 2 und 3 StPO angeglichen und geben betroffenen Personen das Recht, sowohl über erstmalige als auch über folgende Vollzugslockerungen in Kenntnis gesetzt zu werden. Dies dient dem Opferschutz. Hierbei ist zu berücksichtigen, dass die Regelung in Absatz 2 Nummer 3 – wie auch in § 406d Absatz 2 Nummer 3 StPO – als Ausnahme anzusehen ist. Dies kommt auch in der Differenzierung in Absatz 3 zum Ausdruck, der für die Fälle des Absatzes 2 Nummer 3 stets die gesonderte Darlegung eines berechtigten Interesses normiert und dieses nicht bereits wie für die Fälle des Absatzes 2 Nummer 2 unterstellt. Die Darlegung des berechtigten Interesses muss deutlich machen, warum ein Ausnahmefall vorliegt und durch die Erstmitteilung die Interessen der Verletzten oder des Verletzten nicht befriedigt werden konnten.

Absatz 3 verzichtet bei den dort genannten Personen auf die Darlegung eines berechtigten Interesses. Dieses wird angesichts des zugefügten Übels bzw. analog zu § 395 StPO unterstellt.

Absatz 4 privilegiert öffentlich-rechtliche Forderungen. Die öffentliche Hand soll wegen ihrer überragenden Bedeutung für die Daseinsvorsorge hinsichtlich von Auskünften über die Entlassungsadresse oder die Vermögensverhältnisse von Gefangenen Verletzten einer Straftat insoweit gleichgestellt werden (Absatz 2).

Der besonderen Stellung der Untersuchungsgefangenen – sie gelten als unschuldig – und der in einer Haft gemäß § 1 Absatz 1 Nummer 2 befindlichen Gefangenen ist auch im Rahmen der Mitteilung über ihre Haftverhältnisse an externe Stellen Rechnung zu tragen. Absatz 5 bestimmt deshalb, dass im Falle einer Mitteilung über Haftverhältnisse nur die Angabe erfolgen darf, ob sich eine Person in der Anstalt in Untersuchungshaft befindet. Aufgrund der Unschuldsvermutung erhalten mutmaßliche Verletzte oder deren Rechtsnachfolgerinnen und Rechtsnachfolger keine Auskunft.

Absatz 6 schreibt eine Interessenabwägung zwischen den Belangen der Auskunftsberechtigten und der oder des Gefangenen vor. Im Falle einer unterbliebenen Anhörung der Gefangenen hat nicht nur eine Mitteilung, sondern auch die Angabe des übermittelten Inhalts zu erfolgen.

Absatz 7 trägt den besonderen Interessen der Empfängerinnen und Empfänger Rechnung und dient ebenfalls dem Opferschutz.

Absatz 8 regelt die Dokumentationspflicht und dient der Transparenz.

Da hinsichtlich der erlaubten Mitteilungen über Haftverhältnisse zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen unterschieden wird, dient § 20 auch der Umsetzung von Artikel 6 der Richtlinie (EU) 2016/680.

Zu § 21 **Aktenüberlassung**

§ 21 entspricht im Wesentlichen § 16 JVollzDSG in der bisherigen Fassung.

Die Bestimmung enthält eine Sonderregelung für die Überlassung von Akten mit enumerativer Aufzählung der hierfür in Frage kommenden öffentlichen Stellen. Eine solche Aktenüberlassung ist gleichzeitig die Übermittlung aller in der Akte enthaltenen Daten. Dieser Umfang setzt zwingend eine gesetzliche Übermittlungsbefugnis voraus. Von dieser Regelung nicht erfasst wird die Ausübung des Auskunfts- und Akteneinsichtsrecht der Gefangenen durch eine beauftragte Verteidigerin, Rechtsanwältin, Notarin oder einen beauftragten Verteidiger, Rechtsanwalt oder Notar (§§ 54, 55). Auch in diesen Fällen ist die Übersendung der Akte zulässig (§ 55 Absatz 3).

Absatz 2 schreibt eine Interessenabwägung vor, sofern eine untrennbare Verquickung von Daten vorliegt. Bei besonderen Kategorien von personenbezogenen Daten wird regelmäßig von vornherein ein überwiegend berechtigtes Interesse der betroffenen Person an der Geheimhaltung ihrer Daten unterstellt, sodass eine Übermittlung im Wege der Aktenüberlassung und damit eine Aktenüberlassung selbst unzulässig ist. Die Speicherung, Nutzung und Übermittlung der untrennbar verbundenen Daten der betroffenen Person oder Dritter durch die empfangende öffentliche Stelle ist unzulässig.

Da in Absatz 2 zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen unterschieden wird, dient dies auch der Umsetzung von Artikel 6 der Richtlinie (EU) 2016/680.

Zu § 22 Auskunft und Akteneinsicht für wissenschaftliche Zwecke

§ 22 entspricht § 17 JVOllzDSG SH in der bisherigen Fassung.

Die Bestimmung regelt die Voraussetzungen für Aktenauskunft und -einsicht an Einrichtungen, die wissenschaftliche Forschung betreiben, und öffentliche Stellen für wissenschaftliche Zwecke.

Absatz 1 entspricht in angepasster Form dem § 186 StVOllzG. Wie dort wird auf § 476 StPO Bezug genommen. Während jedoch § 476 StPO voraussetzt, dass die betreffenden Daten in Akten gespeichert sind, ist die Übermittlungsmöglichkeit eingedenk der technischen Entwicklungen auch auf elektronisch gespeicherte Daten erweitert.

Die Übermittlung der personenbezogenen Daten kann nach Absatz 1 Satz 2 auch auf elektronischem Weg erfolgen. Die Übermittlung personenbezogener Daten an die in § 22 genannten Adressaten ist nach § 476 Absatz 1 Satz 1 zulässig, soweit dies für die Durchführung bestimmter wissenschaftlicher Forschungsarbeiten erforderlich ist (Nummer 1), die Nutzung anonymisierter Daten zu diesem Zweck nicht möglich oder die Anonymisierung mit einem unverhältnismäßigem Aufwand verbunden ist (Nummer 2) und das öffentliche Interesse an der Forschungsarbeit das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung erheblich überwiegt (Nummer 3). Bei der Abwägung nach Satz 1 Nummer 3 ist im Rahmen des öffentlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen. In personaler Hinsicht müssen die Empfänger Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete bzw. zur Geheimhaltung Verpflichtete (vgl. § 476 Absatz 3 StPO) sein.

Absatz 2 trägt im Vollzug der Untersuchungshaft und der Freiheitsentziehungen nach § 1 Nummer 2 der Unschuldsvermutung Rechnung.

Die Regelung entspricht dem bisherigen § 17 JVOllzDSG SH und setzt auch die Vorgaben von Artikel 4 Absatz 3 der Richtlinie (EU) 2016/680 um.

Zu § 23 Einsichtnahme in Gefangenenpersonalakten, Gesundheitsakten und Krankenblätter

Nach Artikel 8 Absatz 2 Buchstabe d der Europäischen Konvention zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe hat Deutschland als Vertragspartei dem europäischen Ausschuss zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe (nachfolgend Ausschuss) alle Auskünfte, die er zur Erfüllung seiner Aufgabe benötigt, zur Verfügung zu stellen. Hierbei beachtet der Ausschuss die innerstaatlichen Rechtsvorschriften, zu denen laut den Anmerkungen zu den Bestimmungen des Übereinkommens insbesondere die Regelungen des Datenschutzes gehören (Ziffer 64 des erläuternden Berichts).

Im Sinne der weiteren Ausführungen in dem erläuternden Bericht, dass mögliche Schwierigkeiten in diesem Bereich im Geiste des gegenseitigen Verständnisses und der Zusammenarbeit, auf die sich das Übereinkommen gründet, gelöst werden sollten, schafft die Bestimmung eine Rechtsgrundlage, um dem Ausschuss die für die Erfüllung seiner Aufgabe notwendigen Informationen zur Verfügung zu stellen.

§ 23 sieht für die Mitglieder der Delegation des Ausschusses vor, dass diesen die Einsichtnahme in Gefangenenpersonalakten, Gesundheitsakten und Krankenblätter während eines Anstaltsbesuchs zu gewähren ist, soweit dies unbedingt erforderlich ist. Damit wird einer Forderung des Ausschusses aus dem Jahr 2016 entsprochen, Maßnahmen zu ergreifen, damit Besuchsdelegationen künftig unbeschränkte Einsicht in die Personal- und Gesundheitsakten von Gefangenen erhalten zu können. Eine Überlassung von Akten erfolgt ausschließlich im Rahmen der Anstaltsbesuche. Die Akten können daher nur vor Ort durch die Mitglieder der Delegation des Ausschusses eingesehen werden. Die Gewährung der Einsichtnahme in die besagten Akten – insbesondere auch die Gesundheitsakten und Krankenblätter mit ihren besonderen Kategorien personenbezogener Daten – wird gewährt, soweit dies zur Wahrnehmung der Aufgaben der Mitglieder der Delegation des Ausschusses unbedingt erforderlich ist. Das Recht zur Einsichtnahme der Mitglieder des Ausschusses unterliegt damit dem Grundsatz der Zweckbindung und setzt Artikel 10 der Richtlinie (EU) 2016/680 um. Sowohl in den Gefangenenpersonalakten als auch in den Gesundheitsakten und Krankenblättern sind besondere Kategorien personenbezogener Daten (vgl. § 2 Nummer 14) im Sinne der Richtlinie (EU) 2016/680 zu finden. Der mit der Einsichtnahme verbundene Eingriff in das Recht der Gefangenen auf informationelle Selbstbestimmung ist, insbesondere mit Blick auf die in Rede stehenden besonders schutzwürdigen Daten, nicht unerheblich, jedoch hinsichtlich der Aufgabe und des Zwecks verhältnismäßig. Die Mitglieder der Delegation haben die als besonders wichtig zu bewertende Aufgabe, die Behandlung von Personen, denen die Freiheit entzogen ist, zu überprüfen, um damit den Schutz vor Folter und anderen verbotenen Behandlungsweisen sicherzustellen. Eine Delegation des Ausschusses geht im Rahmen ihres Besuchs in einer Anstalt wie folgt vor: Sie trifft zunächst eine stichprobenartige Auswahl aus allen vorhandenen Akten, um dies kurzfristig durchzusehen. Ergibt sich dadurch ein Anlass zu genaueren Nachfragen, so werden im Anschluss Gespräche mit den betroffenen Gefangenen geführt. Auf diese Weise können sich die Mitglieder der Besuchsdelegation ein realistisches und fundiertes Bild über die aktuellen Zustände innerhalb der Anstalt machen. Hierfür ist der ungehinderte Zugang zu dem gesamten Aktenbestand hinsichtlich der Gefangenen erforderlich. Eine vorherige Auswahl von Akten bspw. danach, ob die Gefangenen in die Einsichtnahme eingewilligt haben, würde keine unvoreingenommene Stichprobenauswahl mehr ermöglichen. Eine solche Auswahl wäre manipulationsanfällig und zwar nicht nur durch explizite oder versteckte Drohungen gegenüber Gefangenen für den Fall ihrer Einwilligung, sondern auch im Hinblick auf indirekte Manipulationen, etwa durch missverständliche oder irreführende Darstellungen der Aufgaben der Besuchsdelegation. Die Kernaufgabe des Ausschusses als Ausfluss der menschenrechtlichen Garantien in Europa ist eine anlasslose Kontrolle, zu der auch die umfassende Einsichtnahme in den über die Gefangenen geführten Aktenbe-

stand gehört. Schließlich zielt der besagte Eingriff in die informationelle Selbstbestimmung gerade auf den Schutz der Rechte der betroffenen Personen ab, um Gefangene vor Übergriffen und unangemessener Behandlung im Vollzug zu schützen. Die Mitglieder der Delegation unterliegen nach Artikel 11 der Europäischen Konvention zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe der Vertraulichkeit hinsichtlich der erhaltenen Informationen; personenbezogene Daten dürfen nicht ohne ausdrückliche Zustimmung der betroffenen Personen veröffentlicht werden. In die Gesundheitsakten und Krankenblätter der Gefangenen nehmen grundsätzlich nur Mitglieder der Besuchsdelegation, die über den entsprechenden beruflichen, d.h. medizinischen, Sachverstand verfügen, in der Anstalt Einsicht. In dieser speziellen Konstellation ist die normierte Einsichtnahme in Akten mit dem Schutz der Grundrechte der Gefangenen unter Beachtung der Vorgaben des Artikels 10 der Richtlinie (EU) 2016/680 vereinbar.

Von der Bestimmung ist ebenfalls gedeckt, dass Berufsgeheimnisträgerinnen und Berufsgeheimnisträger den Mitgliedern der Besuchsdelegation mit dem entsprechenden beruflichen Sachverstand Auskünfte und Erläuterungen zum Inhalt der Gesundheitsakten und Krankenblättern geben.

Abschnitt 5

Besondere Formen der Datenverarbeitung

Zu § 24 Datenverarbeitung im Auftrag

Die Bestimmung dient der Umsetzung von Artikel 22 der Richtlinie (EU) 2016/680. Sie lehnt sich an § 62 des Bundesdatenschutzes an.

Absatz 2 greift die Regelung in § 18 Absatz 1 JVollzDSG SH in der bisherigen Fassung auf.

Absatz 3 beschreibt an den Auftragsverarbeiter zu stellende Anforderungen und setzt Artikel 22 Absatz 1 der Richtlinie (EU) 2016/680 um.

In Absatz 4 werden Voraussetzungen für die Eingehung von Unterauftragsverarbeitungsverhältnissen normiert und dadurch Artikel 22 Absatz 2 der Richtlinie (EU) 2016/680 umgesetzt.

In Absatz 5 wird in Übernahme von Elementen aus Artikel 28 Absatz 4 der Verordnung (EU) 2016/679 die Überführung der den Auftragsverarbeiter treffenden Pflichten auf einen Unterauftragnehmer thematisiert.

In Absatz 6 werden die erforderlichen Inhalte einer der Auftragsverarbeitung zugrundeliegenden Vereinbarung niedergelegt. Diese Inhalte sind sowohl Artikel 22 Absatz 3 der Richtlinie (EU) 2016/68, Artikel 28 Absatz 3 der Verordnung (EU) 2016/679 als auch § 11 Absatz 2 und 3 des Bundesdatenschutzgesetzes a. F. entnommen; so werden in Satz 2 Nummer 1 Elemente aus Artikel 28 Absatz 3 Buchstabe a der Verordnung (EU) 2016/679 und § 11 Absatz 3 Satz 2 des Bundesdatenschutzgesetzes a. F., in Nummer 5 und 6 Elemente aus Artikel 28 Absatz 3 Buchstabe h der Verordnung (EU) 2016/679, in Nummer 7 Elemente aus Artikel 28 Absatz 3 Buchstabe d der Verordnung (EU) 2016/679 und in Nummer 8 und 9 Elemente aus Artikel 28 Absatz 3 Buchstabe c und f der Verordnung (EU) 2016/679 aufgenommen. Absatz 6 Satz 1 trifft in Umsetzung von Artikel 22 Absatz 4 der Richtlinie (EU) 2016/680 zudem Aussagen zur Form der Vereinbarung.

Absatz 7 dient der Umsetzung von Artikel 22 Absatz 5 der Richtlinie (EU) 2016/680.

Nach Absatz 8 gelten die Pflicht zur Pseudonymisierung aus § 18 Absatz 6 und die förmliche Verpflichtung nach § 19 für die Datenverarbeitung im Auftrag entsprechend.

Zu § 25 Datenverarbeitung bei Übertragung von Vollzugsaufgaben

Die Bestimmung regelt die Voraussetzungen der Verarbeitung personenbezogener Daten durch öffentliche oder nichtöffentliche Stellen außerhalb des räumlichen und organisatorischen Bereichs der Justizvollzugsbehörden, denen Aufgaben des Vollzuges zur eigenständigen Erledigung innerhalb des räumlichen und organisatorischen Bereichs der Justizvollzugsbehörden übertragen wurden oder übertragen werden sollen. Die Befugnisnormen zur Übertragung von vollzuglichen Aufgaben selbst befinden sich in den Vollzugsgesetzen der Länder und beispielsweise auch in § 155 Absatz 1 StVollzG.

Soweit eine Übertragung vollzuglicher Aufgaben zulässig ist, bedarf es zusätzlich einer gesetzlichen Grundlage für die Verarbeitung personenbezogener Daten zur Erledigung der übertragenen Aufgaben.

Als denkbare Übertragung kann insbesondere die weitgehend selbstständige Organisation der Gefangenearbeit oder Versorgung der Gefangenen und deren medizinischen Betreuung, fachdienstliche Behandlung oder die Heranziehung privater Kaufleute zur weitgehend selbstständigen Abwicklung des Anstaltseinkaufes innerhalb der Anstalt angesehen werden.

Für die Ausgestaltung von solchen Übertragungen stellt Absatz 2 Regeln über die Auswahl des Auftragnehmers (Satz 1), die Gewährleistung datenschutzrechtlicher Standards (Satz 2), die schriftliche oder in einem elektronischen Format festzulegende Erteilung des Auftrages (Satz 3) zum Gegenstand und zum Umfang der Aufgabenübertragung, zur Erforderlichkeit der Verarbeitung personenbezogener Daten zur Erfüllung übertragener Aufgaben und die förmliche Verpflichtung des hierfür einzusetzenden Personals nach § 1 des Verpflichtungsgesetzes (Satz 4) auf. Satz 5 verpflichtet den Auftraggeber, die Einhaltung der von Auftragnehmern getroffenen datenschutzrechtlichen Maßnahmen regelmäßig zu überprüfen und dies zu dokumentieren.

Soweit die übertragenen Vollzugsaufgaben geleistet werden, findet dieses Gesetz nach Absatz 3 auf die Verarbeitung personenbezogener Daten Anwendung.

Zu § 26 Gemeinsame Verantwortung der Justizvollzugsbehörden

Die Bestimmung dient der Umsetzung von Artikel 21 der Richtlinie (EU) 2016/680. Zum Schutz der Rechte und Freiheiten der betroffenen Personen einerseits und der Festlegung der Verantwortung und Haftung der beteiligten Justizvollzugsbehörden andererseits bedarf es einer klaren Zuteilung der Verantwortlichkeiten im Rahmen der zu treffenden Vereinbarung.

Zu § 27 Erkennungsdienstliche Maßnahmen

§ 27 greift § 20 JVollzDSG SH in der bisherigen Fassung auf.

Die zweifelsfreie Klärung der Identität eines Gefangenen ist für den Justizvollzug notwendig, um Identitätsverwechslungen auszuschließen und damit zu verhindern, dass Eingriffe in die Grundrechte Unbeteiligter stattfinden. Um die Gefangenen zu befähigen, künftig in sozialer Verantwortung ein Leben ohne Straftaten zu führen und um eine auf den Einzelnen und seine Historie zugeschnittene Vollzugsplanung zu gewährleisten, bedarf es der zweifelsfreien Feststellung der Identität. Darüber hinaus ist die zweifelsfreie Feststellung der Identität aller Gefangenen notwendig, um die Sicherheit der Anstalt zu gewährleisten. Zahlreiche Maßnahmen zur Gewährleistung der Sicherheit der Anstalt wie beispielsweise die Überprüfung der Gefangenen nach § 14 oder der Austausch personenbezogener Daten mit den Sicherheitsbehörden setzen voraus, dass die Identität des Betroffenen zweifelsfrei geklärt ist. Darüber hinaus dient die Erhebung von Daten zur Identität des Gefangenen der Sicherung des Vollzuges, indem namentlich etwa eine etwaige Fahndung und Wiederergriffung im Fall der Flucht ermöglicht werden. Auch gilt es, irrtümliche Entlassungen zu verhindern. Schließlich soll den Vollzugsbediensteten eine Identifizierung aller Gefangenen ermöglicht werden, um so einen möglichst reibungslosen Vollzugsalltag zu ermöglichen. § 27 steht in einem systematischen Zusammenhang zu § 28. § 27 regelt die zulässigen erkennungsdienstlichen Maßnahmen, um die Identität des Gefangenen feststellen zu können. Verbleiben Zweifel, erfolgt ein erkennungsdienstlicher Datenabgleich mit dem Landeskriminalamt, dem Bundeskriminalamt, oder dem Bundesamt für Migration und Flüchtlinge auf Grundlage der erhobenen Informationen, § 28.

Absatz 1 regelt abschließend die zulässigen erkennungsdienstlichen Maßnahmen zur Erhebung von Daten der Gefangenen. Hervorgehoben wird die Gewährleistung der Sicherheit der Anstalt. Als weiterer Zweck der Datenerhebung wird die Feststellung der Identität des Gefangenen genannt, die letztlich aber dem vorgenannten Zweck gleichsam als Sekundärzweck dient. Aus der Fassung „sind [...] zulässig“ ergibt sich, dass die Vollzugsbehörden nicht verpflichtet sind, die genannten Maßnahmen zu ergreifen. Dies liegt in ihrem Ermessen. Erkennungsdienstliche Maßnahmen sind folglich nicht zwingender Bestandteil des Aufnahmeverfahrens. Da die erkennungsdienstlichen Maßnahmen nach Absatz 1 durchgeführt werden dürfen, kann die Ermessensentscheidung auf eine Vielzahl von Gründen gestützt werden. Zumindest die Aufnahme von Lichtbildern dürfte regelmäßig zulässig sein, schon um einen reibungslosen Vollzugsalltag zu ermöglichen. Darüber hinaus können beispielweise auch eine Flucht und Fluchtversuche, die Zugehörigkeit zu einer kriminellen Vereinigung oder die Länge der Vollzugsdauer bei der Entscheidung berücksichtigt werden. Eine Begrenzung auf Gefangene mit einer bestimmten Mindestvollzugsdauer ist im Gesetz nicht angelegt. Im Rahmen der Ermessensausübung ist der Grundsatz der Erforderlichkeit zu beachten. Die Erhebung der Daten ist zu jeder Zeit des Vollzuges zulässig. Insbesondere bei Lichtbildaufnahmen ist im Laufe der Zeit zu prüfen, ob diese noch aktuell sind (Bart, Haarwuchs). Zumindest nach Ablauf von drei Jahren dürfte die Anfertigung neuer Lichtbilder jeweils gerechtfertigt sein. Aus der Natur der Norm als Ermessensvorschrift und aus dem Grundsatz der Verhältnismäßigkeit folgt, dass die Maßnahmen in jedem Einzelfall zu prüfen, zu wählen und zu begründen sind. Dies schließt ermessensleitende Standardisierungen für den Vollzugsalltag nicht aus. Die Aufnahme von Lichtbildern nach Absatz 1 Nummer 1 kann den ganzen Körper oder auch nur einzelne Körperteile zum Gegenstand haben. Nach der herkömmlichen Definition sind Lichtbilder ihrer technischen Herstellung nach solche Abbildungen, die eine Strahlungsquelle (Licht, Wärme oder Röntgenstrahlen) durch chemische Veränderungen auf strahlenempfindlichen Schichten hervorruft, also vor allem die Schwarzweiß- und Farbfotografie. Lichtbilder sind nur dann „biometrische Daten“, wenn sie mit speziellen technischen Mitteln verarbeitet werden. Lichtbilder werden folglich nicht per se den besonderen Regelungen biometrischer Daten unterworfen, sondern nur dann, wenn sie genutzt werden, um aus ihnen physische, physiologische oder verhaltens-

typische Merkmale zu gewinnen oder diese zu analysieren (vgl. Schreiber in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Artikel 4 DSGVO). Die Abnahme von Finger- und Handflächenabdrücken nach Absatz 1 Nummer 2 darf auch digital zum Beispiel durch einen Fingerabdruckscanner erfolgen. Zu den äußeren körperlichen Merkmalen nach Absatz 1 Nummer 3 gehören auch Tätowierungen. Mit Messungen nach Absatz 1 Nummer 4 sind beispielsweise die Größe und das Gewicht eines Gefangenen angesprochen. Darüber hinaus unterfällt auch die Gesichtsfeldererkennung dem Absatz 1 Nummer 4. Die Schriftprobe eines Gefangenen unterfällt der Nummer 4 nicht. Absatz 1 Nummer 5 erlaubt die Erhebung biometrischer Merkmale. Zu den körperlichen biometrischen Merkmalen gehören beispielsweise die Gesichtsform, die Augennetzhaut, die Stimme, die Handgeometrie oder die Venenstruktur. Die biometrische Erfassung von Merkmalen des Gesichts, der Augen, der Hände oder der Stimme ist eine sichere Methode, die Identität einer Person festzustellen. Sie ist einfach zu handhaben, nur mit relativ geringen Eingriffen verbunden und wird deshalb in Sicherheitsbereichen außerhalb des Justizvollzuges bereits angewendet. Auch wenn es sich um sehr sensible personenbezogene Daten handelt, kann der Einsatz im erforderlichen Umfang für den Betroffenen insgesamt eine geringere Belastung bedeuten, da Kontrollmaßnahmen effektiver, schneller und gleichzeitig weniger belastend durchgeführt werden können. Bei der Unterschrift nach Absatz 1 Nummer 6 handelt es sich um ein verhaltenstypisches Merkmal einer Person. Die Daten dürfen nur mit Kenntnis des Gefangenen erhoben werden. Insoweit wird der Verhältnismäßigkeitsgrundsatz konkretisiert. § 27 ermöglicht die Erhebung biometrischer Daten. Nach § 2 Nummer 16 handelt es sich bei biometrischen Daten um mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, insbesondere Gesichtsbilder oder daktyloskopische Daten. Die Definition entspricht Artikel 3 Nummer 13 der Richtlinie (EU) 2016/680 und ist entsprechend europarechtskonform auszulegen. Bei biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person handelt es sich um besondere Kategorien personenbezogener Daten (§ 2 Nummer 14 Buchstabe c)), was bei der Erhebung und weiteren Verarbeitung dieser Daten zu berücksichtigen ist. Nach § 6 Absatz 2 dürfen besondere Kategorien personenbezogener Daten nur erhoben werden, wenn dies zu vollzughlichen Zwecken unbedingt erforderlich ist, das heißt im konkreten Einzelfall unerlässlich ist.

Absatz 2 stellt klar, dass die erhobenen Daten nicht nur in Papierform in Gefangenenpersonalakten abgelegt, sondern auch in Gestalt der (elektronischen) Speicherung in personenbezogenen Dateisystemen verarbeitet werden dürfen. Sie sind so zu sichern, dass eine Kenntnisnahme nur zu den im Gesetz nachfolgend genannten Zwecken möglich ist. Hiermit sind organisatorische Maßnahmen und Fragen der Technikgestaltung angesprochen, wie zum Beispiel die gesonderte Ablage in der Gefangenenpersonalakte.

Absatz 3 regelt die Nutzung der erhobenen Daten. § 16 und damit die Nutzung der erkennungsdienstlichen Daten im Rahmen von Fallkonferenzen bleibt von der Regelung des Absatzes 3 unberührt. Absatz 3 Nummer 1 greift den Grundsatz der Zweckbindung auf und legt fest, dass die erhobenen Daten zu den Zwecken, zu denen sie erhoben wurden, genutzt werden dürfen. Absatz 3 Nummer 2 erlaubt die Nutzung der erkennungsdienstlichen Daten zum Zweck der Identifikation des entwichenen oder sich sonst ohne Erlaubnis außerhalb der Anstalt aufhaltenden Gefangenen im Rahmen einer Fahndung und Festnahme. Absatz 3 Nummer 3 erlaubt die Nutzung der erkennungsdienstlichen Daten für den Zweck des § 10 Absatz 2 Nummer 1 sowie zur Identitätsfeststellung nach § 28. Gehören die erhobenen erkennungsdienstlichen Daten zur besonderen Kategorie personenbezogener Daten nach § 2 Nummer 14 Buchstabe c), ist ihre Speicherung oder Nutzung für Zwecke, zu denen sie nicht erhoben wurden, ohne Einwilligung der betroffenen Personen nur zulässig, soweit dies zu einem der in § 10 Absatz 2 genannten Zwecke unbedingt erforderlich ist, § 10 Absatz 3. Die zweckändernde Nutzung erkennungsdienstlicher Daten nach § 27 Absatz 3 Nummer 2 und 3 muss folglich unbedingt erforderlich sein, wenn es sich um Daten handelt, die zur besonderen Kategorie personenbezogener Daten gehören.

Absatz 4 regelt die Übermittlung der nach Absatz 1 erhobenen Daten. Die Empfänger der Daten werden in den nachfolgenden Ziffern genannt. Absatz 4 Nummer 1 ist in einem Zusammenhang mit Absatz 3 Nummer 2 zu lesen und nennt die zuständigen Empfangsbehörden im Falle einer Fahndung und Festnahme. Absatz 4 Nummer 2 ist im Zusammenhang mit Absatz 3 Nummer 3 zu lesen. Absatz 4 Nummer 3 erfasst den Fall der Übermittlung der erhobenen erkennungsdienstlichen Daten auf Ersuchen einer öffentlichen Stelle. Absatz 4 Nummer 3 greift den Grundsatz der hypothetischen Datenneuerhebung auf und erlaubt die zweckändernde Datenübermittlung an eine öffentliche Stelle auf deren Ersuchen, wenn die Neuerhebung der entsprechenden Daten durch die anfragende Stelle im konkreten Fall zulässig wäre. Nicht explizit genannt sind in § 27 Absatz 4 die Empfänger bei einer Datenübermittlung zum Zweck der Identifizierung nach § 27 Absatz 3 Nummer 3 und § 28. Die empfangenen Behörden und die Befugnis zur Übermittlung ergeben sich hier bereits direkt aus dem Normtext des § 28. Gleiches gilt für die Regelung des § 16. Gehören die erhobenen erkennungsdienstlichen Daten zur besonderen Kategorie personenbezogener Daten nach § 2 Nummer 14 Buchstabe c) ist die Übermittlung an eine andere öffentliche Stelle nur unter den Voraussetzungen des § 10 Absatz 3 zulässig (§ 12 Absatz 6 Nummer 1). Nach § 10 Absatz 3 muss die Datennutzung für die in § 10 Absatz 2 genannten Zwecke unbedingt erforderlich sein. Gehören die erhobenen erkennungsdienstlichen Daten zur besonderen Kategorie personenbezogener Daten nach § 2 Nummer 14 Buchstabe c), ist die Übermittlung an eine andere öffentliche Stelle folglich nur dann zulässig, wenn dies zur Zweckerfüllung unbedingt erforderlich ist.

Absatz 5 regelt, wann die erhobenen Daten zu löschen sind. Dies muss unverzüglich, das heißt ohne schuldhaftes Zögern nach der Entlassung des Gefangenen aus dem Vollzug erfolgen. Wie der Verweis auf § 59 verdeutlicht, kann von einer Löschung abgesehen werden, wenn die Daten noch für vollzugliche Zwecke benötigt werden. Vollzugliche Zwecke können beispielsweise dann fortbestehen, wenn ein Gefangener unter Bewährung oder unter Führungsaufsicht entlassen wird. Eine fortdauernde Speicherung für die Durchführung wissenschaftlicher Forschungsvorhaben oder zu statistischen Zwecken, wie § 59 sie erlaubt, ist von der Verweisung nicht erfasst. Eine solche Nutzung der erkennungsdienstlichen Daten ist von § 27 Absatz 3 nicht gedeckt und damit von vornherein ausgeschlossen. Bei einer fortdauernden Speicherung der erkennungsdienstlichen Daten über den Zeitpunkt der Entlassung hinaus sind die Kontroll- und Löschfristen des § 59 zu beachten. Statt einer Löschung der Daten kommt auch eine Einschränkung in der Verarbeitung in Betracht, wie der Verweis auf § 60 verdeutlicht. Auch in diesem Fall müssen die möglichen Nutzungen des § 27 Absatz 3 beachtet werden, die durch § 60 nicht erweitert werden. Sind die Daten nach § 60 in ihrer Verarbeitung eingeschränkt, sind die diesbezüglichen Vorgaben des § 60 zu beachten. Die Löschung der Daten ist in den Gefangenenpersonalakten zu dokumentieren. Die Dokumentation muss sachhaltig genug sein, um etwaigen Rechtsschutz und eine Datenschutzkontrolle zu ermöglichen. Absatz 5 dient der Umsetzung von Artikel 4 Absatz 1 Buchstabe e), Artikel 5 der Richtlinie (EU) 2016/680 und ist in deren Anwendungsbereich richtlinienkonform auszulegen.

Zu § 28 Erkennungsdienstlicher Datenabgleich

Die zweifelsfreie Klärung der Identität der Gefangenen ist für den Justizvollzug notwendig, um Identitätsverwechslungen auszuschließen und damit zu verhindern, dass Eingriffe in die Grundrechte Unbeteiligter stattfinden. Um die Gefangenen zu befähigen, künftig in sozialer Verantwortung ein Leben ohne Straftaten zu führen und um eine auf den Einzelnen und seine Historie zugeschnittene Vollzugsplanung zu gewährleisten, bedarf es der zweifelsfreien Feststellung der Identität. Darüber hinaus ist die zweifelsfreie Feststellung der Identität aller Gefangenen notwendig, um die Sicherheit der Anstalt zu gewährleisten. Zahlreiche Maßnahmen zur Gewährleistung der Sicherheit der Anstalt wie beispielsweise die Überprüfung der Gefangenen nach § 14 oder der Austausch personenbezogener Daten mit den Sicherheitsbehörden setzen voraus, dass die Identität des Betroffenen zweifelsfrei geklärt ist. Der ererkennungsdienstliche Datenabgleich nach § 28 baut auf den ererkennungsdienstlichen Maßnahmen nach § 27 auf. Der ererkennungsdienstliche Datenabgleich folgt der Erhebung der ererkennungsdienstlichen Daten nach.

Absatz 1 Satz 1 regelt, dass ererkennungsdienstliche Daten nach § 27 sowie die Daten nach § 14 Absatz 3 übermittelt werden dürfen, wenn Zweifel an der Identität der Gefangenen bestehen und die Datenübermittlung zur Identitätsfeststellung erforderlich ist. Der Zweck der Datenübermittlung ist auf die Identitätsfeststellung begrenzt. Die Daten, die zur Identitätsfeststellung übermittelt werden dürfen, ergeben sich abschließend aus § 27 und § 14 Absatz 3. In der Folge dürfen nur Grunddaten wie namentlich Nachname, Geburtsname, Vorname, Geburtsdatum, Geschlecht, Geburtsort, Geburtsland, Staatsangehörigkeit, Aliaspersonen, zur Identitätsfeststellung gefertigte Lichtbilder, Finger- und Handflächenabdrücke, festgestellte äußere körperliche Merkmale, Messungen, biometrische Merkmale von Fingern, Händen, Gesicht, Augen, der Stimme und die erfasste Unterschrift übermittelt werden. Als Schwelle für eine Datenübermittlung legt § 28 Absatz 1 Satz 1 „Zweifel an der Identität“ der Gefangenen fest. Damit orientiert sich die Norm an der Rechtsprechung des Bundesverfassungsgerichts, wonach eine Übermittlung von Grunddaten ausschließlich zum Zweck der Identitätsfeststellung nicht zu beanstanden ist, wenn es sich um Einzelabfragen handelt und ein konkreter Anlass für die Datenübermittlung besteht (vgl. BVerfG, Urteil des Ersten Senats vom 24. April 2013 - 1 BvR 1215/07 -, Randnummern 192 ff.). Dass die Datenübermittlung für die Identitätsfeststellung „erforderlich“ sein muss, verweist auf die Notwendigkeit einer sachhaltigen Prüfung des Übermittlungsanlasses im Einzelfall (vgl. BVerfG, a. a. O., Randnummer 194). Als Empfänger der Datenübermittlung nennt § 28 Absatz 1 Satz 1 das Landeskriminalamt. Nach Absatz 1 Satz 2 veranlasst das Landeskriminalamt den Abgleich der übermittelten Daten zum Zweck der Identifizierung der Gefangenen und teilt das Ergebnis den Justizvollzugsbehörden mit. Die Norm wirkt insoweit als Befugnisnorm für das Landeskriminalamt. Sie ermächtigt sowohl zum Datenabgleich als auch zur Übermittlung des Ergebnisses an die Justizvollzugsbehörden zum Zweck der Identifizierung. Die Nutzung der übermittelten Daten wird durch Absatz 1 Satz 2 folglich auf die Identifizierung der Gefangenen beschränkt. Zu einem darüber hinausgehenden Austausch von ermittlungs- oder handlungsleitenden Informationen ermächtigt § 28 Absatz 1 nicht. Hierfür bedarf es eines Vorgehens nach Maßgabe anderer Bestimmungen. Gehören die zu übermittelnden ererkennungsdienstlichen Daten zur besonderen Kategorie personenbezogener Daten nach § 2 Nummer 14 Buchstabe c) ist ihre Nutzung für Zwecke, zu denen sie nicht erhoben wurden, ohne Einwilligung der betroffenen Personen nur zulässig, soweit dies zu einem der in § 10 Absatz 2 genannten Zwecke unbedingt erforderlich ist (§ 10 Absatz 3). Die zweckändernde Übermittlung ererkennungsdienstlicher Daten nach § 28 muss folglich unbedingt erforderlich sein, wenn es sich um Daten handelt, die zur besonderen Kategorie personenbezogener Daten gehören.

Absatz 2 erweitert den Kreis der Behörden, an die Daten zum Zweck der Identitätsfeststellung übermittelt werden und die um einen Datenabgleich ersucht werden dürfen, auf das Bundeskriminalamt und auf das Bundesamt für Migration und Flüchtlinge. Da es sich bei §

28 Absatz 2 um eine landesrechtliche Regelung handelt, muss die Befugnis zum Datenabgleich und zur Übermittlung des Ergebnisses des Datenabgleichs an die Justizvollzugsbehörden aus dem jeweiligen Fachrecht der Bundesbehörden folgen.

§ 28 birgt das Risiko, dass die Datensätze, die bei den empfangenden Stellen zu den Personen / Gefangenen bereits vorhanden sind, um entsprechende Informationen, die Gegenstand der Anfrage sind, angereichert werden. Dies soll Absatz 3 verhindern. Aus kompetenzrechtlichen Gründen kann eine solche Verpflichtung nicht für Empfänger nach Abs. 2 normiert werden.

Zu § 29 **Einsatz optisch-elektronischer Einrichtungen und biometrischer Zu- und Ausgangskontrollen**

§ 29 entspricht in den Absätzen 1 bis 5 im Wesentlichen § 21 JVollzDSG SH in der bisherigen Fassung.

Die Bestimmung regelt allgemein die Voraussetzungen für den Einsatz optisch-elektronischer Einrichtungen (Videoüberwachung) in beziehungsweise an den Anstalten. In § 30 bis § 32 werden dann spezielle Regelungen für unterschiedliche örtliche Bereiche einer Anstalt aufgestellt. Der Einsatz optisch-elektronischer Beobachtungs- und Überwachungseinrichtungen stellt einen besonders intensiven Eingriff in das informationelle Selbstbestimmungsrecht dar, da die Gefangenen grundsätzlich keine Möglichkeit haben, sich diesen Maßnahmen zu entziehen.

Absatz 1 bindet ihren Einsatz deshalb ausdrücklich an eine entsprechende gesetzliche Bestimmung. Auch in diesem Rahmen ist der Einsatz ausschließlich aus Gründen der Sicherheit zulässig.

Vor diesem Hintergrund verlangt Absatz 2 ein einheitliches Konzept innerhalb der jeweiligen Anstalt und die laufende Fortschreibung zur Anpassung an sich verändernde Verhältnisse.

Nach Absatz 3 ist bereits bei der Planung sicherzustellen, dass eine optisch-elektronische Beobachtung nur aus Gründen der Sicherheit und im erforderlichen Umfang erfolgt. Gleichzeitig muss gewährleistet sein, dass den Gefangenen Bereiche verbleiben, in denen sie sich außerhalb einer optisch-elektronischen Erfassung aufhalten können.

Absatz 4 stellt sicher, dass die Gefangenen Kenntnis von der Videoüberwachung haben. Da die Gefangenen aus allen Kulturkreisen und Gesellschaftsschichten kommen und nicht alle in der Lage sind, die deutsche Sprache zu verstehen, ist sowohl durch sprachliche als auch durch nichtsprachliche Hinweise dafür zu sorgen, dass die Gefangenen in eindeutig erkennbarer Weise Kenntnis von der Tatsache und auch von der Reichweite, also der konkreten räumlichen Erstreckung, haben. Ein genereller Hinweis, dass sich die optisch-elektronische Beobachtung beispielsweise auf das gesamte Anstaltsgelände erstreckt, reicht nicht aus.

Absatz 5 regelt die Zulässigkeit der Videoüberwachung in Transportfahrzeugen des Justizvollzuges und trägt damit einem Bedürfnis der vollzuglichen Praxis und der technischen Ausstattung der neuen Gefangenen-Transportwagen Rechnung. Während des Transportes kann so die ständige und unmittelbare Beaufsichtigung der Gefangenen im Gefangenen-Transportwagen mittels optisch-elektronischer Einrichtungen erfolgen. Auch für diese Beobachtung gelten die Regelungen des Absatzes 4 sowie des § 32 Absatz 4, der eine angemessene Rücksichtnahme auf elementare Bedürfnisse der Gefangenen nach Wahrung der Intimsphäre verlangt, entsprechend.

Absatz 6 erlaubt mit Kenntnis der Bediensteten die elektronische Erfassung biometrischer Merkmale und Messungen im Rahmen von Zu- und Ausgangskontrollen, soweit es zur Sicherung der Anstalten erforderlich ist. Die Erfassung biometrischer Merkmale ist eine sichere Methode, die Identität einer Person festzustellen. Sie ist einfach zu handhaben, nur mit geringen Eingriffen verbunden und wird deshalb in anderen Ländern im Justiz- und Maßregelvollzug und auch außerhalb des Vollzugs in anderen Sicherheitsbereichen erfolgreich angewendet. Neben der Rechtsgrundlage zur Erfassung biometrischer Merkmale und Messungen ist auch eine Rechtsgrundlage zur Verarbeitung dieser Daten erforderlich. Die Daten dürfen nur für die Zwecke verarbeitet werden, für die sie erhoben worden sind. Sie sind unverzüglich zu löschen, sobald die betroffenen Bediensteten aus dem Dienst aus-

scheiden.

Zu § 30 **Optisch-elektronische Einrichtungen im Umfeld der Anstalt**

§ 30 entspricht weitgehend § 20 JVollzDSG SH in der bisherigen Fassung.

Bei Beobachtung der Außengrenzen von Anstalten kann es dazu kommen, dass auch außerhalb des Anstaltsgeländes liegende Flächen von optisch-elektronischer Beobachtung mit erfasst werden. Soweit es sich hierbei um öffentlich zugängliche Räume handelt, können diese ausnahmsweise beobachtet werden. Hierbei sind die Belange möglicherweise betroffener Dritter, das Hausrecht der Anstaltsleiterin oder des Anstaltsleiters und die Notwendigkeit, die Sicherheit der Anstalt zu gewährleisten nach den in der Vorschrift genannten Maßstäben gegeneinander abzuwägen.

Zu § 31 **Optisch-elektronische Einrichtungen innerhalb der Anstalt**

§ 31 stimmt mit § 23 JVollzDSG SH in der bisherigen Fassung überein.

Insbesondere aus Gründen der Sicherheit ermöglicht die Bestimmung die optisch-elektronische Beobachtung von Räumen und Freiflächen innerhalb der Anstalt. Eine wesentliche Einschränkung befindet sich in § 32.

Zu § 32 **Optisch-elektronische Einrichtungen innerhalb von Hafträumen und Zimmern**

§ 32 entspricht im Wesentlichen § 24 JVollzDSG SH in der bisherigen Fassung.

Absatz 1 stellt klar, dass eine optisch-elektronische Beobachtung in Hafträumen und Zimmern grundsätzlich unzulässig ist, da Hafträume und Zimmer die einzige Rückzugsmöglichkeit für die Gefangenen darstellen und auch sie Anspruch auf eine unbeobachtete Privatsphäre haben.

Nach Absatz 2 ist eine optisch-elektronische Beobachtung innerhalb eines Haftraumes oder Zimmers ausnahmsweise zulässig im Rahmen einer Beobachtung als besondere Sicherungsmaßnahme, soweit dies im Einzelfall zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben der zu beobachtenden Gefangenen erforderlich ist. Die Beobachtung mittels optisch-elektronischer Einrichtungen kann nur zusätzlich zu einer unmittelbaren Beobachtung genutzt werden. Wegen des starken Eingriffs in das Recht auf informationelle Selbstbestimmung bedarf es einer ausdrücklichen schriftlichen Anordnung und Begründung.

Absatz 3 bestimmt, dass Gefangene über den Umstand ihrer Beobachtung in Kenntnis zu setzen sind und dies für sie wahrnehmbar sein muss.

Absatz 4 trägt den elementaren Bedürfnissen der Gefangenen nach Wahrung ihrer Intimsphäre Rechnung, insbesondere indem besonders sensible Bereiche wie sanitäre Einrichtungen ausgenommen werden oder durch technische Maßnahmen dafür Sorge getragen wird, dass diese Bereiche im Rahmen der Beobachtung auf dem Monitor nicht sichtbar sind. Dies kann beispielsweise mit einer ausreichenden Verpixelung erreicht werden, wobei eine Verpixelung in unterschiedlichen Graden möglich und zulässig ist. Nur in besonderen Ausnahmefällen bei akuter Selbstverletzungs- oder Suizidgefahr kann im Einzelfall eine uneingeschränkte Überwachung erfolgen. Auch dies ist in der schriftlichen Anordnung festzuhalten und zu begründen. Die Regelungen in dieser Vorschrift orientieren sich an den Empfehlungen der Nationalen Stelle zur Verhütung von Folter (Jahresbericht 2013 der Bundesstelle und der Länderkommission der Nationalen Stelle zur Verhütung von Folter, Seite 27/28).

Absatz 5 ist mit seiner Unterbrechungsregelung Ausfluss des Erforderlichkeitsgrundsatzes, dient andererseits aber auch dem Schutz besonderer Vertrauensverhältnisse. Bei Anwesenheit Dritter wird eine elektronische Beobachtung regelmäßig nicht erforderlich sein. Eine Beobachtung ist z.B. für Gespräche der Gefangenen mit ihren Verteidigerinnen oder Verteidigern ausgeschlossen. Durch die kurzzeitige und absehbare Unterbrechung wird die Anstalt entlastet. Zur Fortsetzung zum gleichen Zweck und bei weiterhin bestehenden Voraussetzungen ist keine neue Anordnung erforderlich.

Zu § 33 **Speicherung mittels optischer oder akustischer Einrichtungen erhobener Daten, Dokumentation**

§ 33 greift im Wesentlichen § 25 JVOllzDSG SH in der bisherigen Fassung auf.

Absatz 1 bestimmt, dass eine Speicherung der durch eine optisch-elektronische Einrichtung erhobenen Daten nur im erforderlichen Umfang erfolgen darf und erhobene Daten anderenfalls zu löschen sind. Soweit im Einzelfall die Erforderlichkeit geprüft werden muss, steht hierzu unter den in Absatz 1 genannten Voraussetzungen ein Zeitraum von 4 Wochen zur Verfügung. Der Verweis auf § 60 Absatz 1 Nummer 1 bis 3 und 5 enthält abschließend die Fallgestaltungen, in denen an die Stelle der Löschung eine Einschränkung der Verarbeitung tritt, da die Daten aus den dort genannten Gründen noch benötigt werden.

Nach Absatz 2 sind auch die durch akustisch-elektronische Einrichtungen erhobenen Daten bei einer Speicherung entsprechend den Daten aus einer optisch-elektronischen Beobachtung zu behandeln. Erfasst sind hierbei alle mittels akustischer Überwachung gewonnenen Daten. Hierzu zählen auch die Daten aus einer Telefonüberwachung.

Absatz 3 dient dem Schutz des Kernbereichs privater Lebensgestaltung. Er trägt der besonderen Lage, in der sich Gefangene befinden, Rechnung. Dem Kernbereich unterfallen Äußerungen durch die Empfindungen, Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck kommen. Dazu zählt auch die Kommunikation mit Personen des höchstpersönlichen Vertrauens. Bei derartigen Daten besteht ein absolutes Verarbeitungsverbot, insbesondere dürfen sie auch nicht gespeichert werden. Durch präventive Maßnahmen ist sicherzustellen, dass eine solche Verarbeitung ausgeschlossen ist. Sollte es dennoch zu einer Speicherung kommen, sind diese Daten unverzüglich zu löschen. Die Kommunikation unmittelbar über Straftaten ist vom Kernbereich privater Lebensgestaltung nicht geschützt, selbst wenn sie auch Höchstpersönliches zum Gegenstand hat. Die Besprechung und Planung von Straftaten gehört ihrem Inhalt nach nicht zum Kernbereich privater Lebensgestaltung, sondern hat Sozialbezug. Ein höchstpersönliches Gespräch fällt allerdings nicht schon dadurch aus dem Kernbereich privater Lebensgestaltung heraus, dass es für die Aufklärung von Straftaten oder Gefahren hilfreiche Aufschlüsse geben kann. Aufzeichnungen oder Äußerungen im Zwiegespräch, die zum Beispiel ausschließlich innere Eindrücke oder Gefühle wiedergeben und keine Hinweise auf konkrete Straftaten enthalten, gewinnen nicht schon dadurch einen Gemeinschaftsbezug, dass sie Ursachen oder Beweggründe eines strafbaren Verhaltens freizulegen vermögen. Auch können trotz Straftatenbezugs Situationen, in denen einzelnen gerade ermöglicht werden soll, ein Fehlverhalten einzugestehen oder sich auf dessen Folgen einzurichten, wie Beichtgespräche oder vertrauliche Gespräche mit einem Psychotherapeuten oder einem Verteidiger oder Verteidigerin der höchstpersönlichen Privatsphäre unterfallen, die dem Staat absolut entzogen ist. Ein hinreichender Sozialbezug besteht demgegenüber dann, wenn Gespräche auch mit Vertrauenspersonen in einem anderen Zusammenhang unmittelbar Straftaten zum Gegenstand haben (vgl. BVerfG, Urt. des 1. Senats vom 20.04.2016 – 1 BvR 966/09, Rn. 122 nach juris).

Absatz 4 dient der Datenschutzkontrolle und verpflichtet zur Dokumentation der Verarbeitung der mittels optisch-elektronischer oder akustisch-elektronischer Einrichtungen erhobenen Daten.

Zu § 34 **Auslesen von Datenspeichern**

§ 34 knüpft in weiten Teilen an § 26 JVollDSG SH in der bisherigen Fassung an.

Absatz 1 gestattet unter engen Voraussetzungen das Auslesen von elektronischen Datenspeichern sowie von elektronischen Geräten mit Datenspeichern, die ohne Erlaubnis in die Anstalt eingebracht wurden. Nach dem derzeitigen Stand der Technik sind hiervon vor allem Mobiltelefone und Smartphones erfasst. Das Auslesen dieser Datenspeicher dient vornehmlich der Aufklärung subkultureller Strukturen und der Verhinderung der Weiterleitung oder Bekanntmachung der darauf möglicherweise gespeicherten Daten der Anstalt (z.B. Bilder von sicherheitsrelevanten Einrichtungen). Zwar ist das Auslesen kein Eingriff in das Telekommunikationsgeheimnis, greift aber in die Integrität und Vertraulichkeit informationstechnischer Systeme ein. Mit Blick auf die Bedeutung des Eingriffs ist nur die Anstaltsleiterin oder der Anstaltsleiter zur Anordnung befugt. Vor dem Auslesen bedarf es einer Interessenabwägung. Die Gründe müssen auf konkreten tatsächlichen Anhaltspunkten beruhen und in der Anordnung aus Rechtsschutzgründen schriftlich festgehalten werden. Das Auslesen darf nur unter Beachtung der Rechte der betroffenen Person erfolgen und ist möglichst auf die Inhalte zu beschränken, deren Kenntnis zur Aufrechterhaltung der Sicherheit und Ordnung der Anstalt erforderlich ist. Insbesondere ist es zu vermeiden, Daten aus dem absolut geschützten Bereich privater Lebensgestaltung auszulesen.

Absatz 2 gestattet die Weiterverarbeitung der nach Absatz 1 erhobenen Daten für vollzugliche Zwecke.

Absatz 3 verbietet die Weiterverarbeitung der erhobenen Daten, wenn sie den Kernbereich der privaten Lebensgestaltung der Gefangenen oder Dritter berühren und ordnet ihre Löschung an.

Nach Absatz 4 sind die Gefangenen schon bei der Aufnahme in den Justizvollzug darüber zu belehren, dass Datenspeicher ausgelesen werden, wenn sie ohne Genehmigung in die Anstalt eingebracht werden.

Zu § 35 **Identifikation anstaltsfremder Personen**

§ 35 knüpft im Wesentlichen an § 27 JVollzDSG SH in der bisherigen Fassung an.

Zur Gewährleistung der Sicherheit der Anstalt, namentlich zur Ermöglichung der Kontrolle von Besuchsverboten und der Verhinderung einer Entweichung durch Austausch von Besucherinnen und Besuchern mit Gefangenen, sieht Absatz 1 zur Identitätsfeststellung neben der Angabe der Personalien und dem Nachweis durch amtlichen Ausweis die Möglichkeit vor, unter engen Voraussetzungen die biometrische Erfassung der genannten Merkmale der anstaltsfremden Personen vorzunehmen. Durch diese Regelungen ist die Anstalt eine zur Identitätsfeststellung berechnigte Behörde im Sinne des § 2 Absatz 2 des Personalausweisgesetzes (PAuswG) und kann daher auch nach § 1 Absatz 1 Satz 3 und 4 PAuswG die Hinterlegung des Personalausweises verlangen. Die biometrische Erfassung der genannten Merkmale stellt einen nicht unerheblichen Eingriff in die informationelle Selbstbestimmung dar und darf deshalb nach Absatz 1 Nummer 2 nur erfolgen, soweit dies zur Verhinderung eines Austausches von Gefangenen unbedingt erforderlich ist. Deshalb ist beispielsweise das Erfassen der genannten Merkmale von weiblichen Personen beim Betreten einer Anstalt, in der nur männliche Gefangene untergebracht sind, nicht zulässig. Die biometrische Erfassung der genannten Merkmale ist auch dem Einzelfall vorzubehalten. Es darf keine allgemeine biometrische Besuchskontrolle vorgenommen werden.

Absatz 2 stellt eine enge Zweckbindung der nach Absatz 1 erhobenen Daten sicher. Eine Zweckänderung ist nach Absatz 2 Nummer 2 nur zur Verfolgung von Straftaten und nur in dem für die Verfolgung von Straftaten erforderlichen Umfang zulässig.

Absatz 3 gewährleistet, dass in das informationelle Selbstbestimmungsrecht der betroffenen Person nur so lange als unbedingt notwendig eingegriffen wird.

Nach Absatz 4 ist auch ein erkennungsdienstlicher Datenabgleich hinsichtlich anstaltsfremder Personen möglich.

Zu § 36 **Lichtbildausweise**

§ 36 entspricht § 28 JVollzDSG SH in der bisherigen Fassung.

Absatz 1 Satz 1 ermächtigt die Anstalt, die Gefangenen zu verpflichten, aus Gründen der Sicherheit oder Ordnung der Anstalt einen Lichtbildausweis mit sich zu führen. Dies umfasst auch die Herstellung der Lichtbildausweise, die bei der Entlassung der Gefangenen oder ihrer Verlegung einzuziehen und zu vernichten sind. Satz 2 stellt sicher, dass auf einem Lichtbildausweis außer dem Bild nur solche Daten gespeichert werden, die für die Aufrechterhaltung von Sicherheit und Ordnung der Anstalt erforderlich sind.

Absatz 2 verlangt die Einziehung und Vernichtung bei Entlassung oder Verlegung der Gefangenen.

Abschnitt 6

Schutzanforderungen

Zu § 37 Zweckbindung

§ 37 greift § 29 JVOllzDSG SH in der bisherigen Fassung auf.

Bei der Bestimmung handelt es sich um eine Schutzvorschrift, die den zweckgebundenen Umgang mit den personenbezogenen Daten der betroffenen Personen, auch nach der Übermittlung, gewährleistet. Dies wirkt einem etwaigen Missbrauch entgegen.

Für andere Zwecke dürfen die Empfänger die Daten nur speichern, nutzen und übermitteln, soweit sie ihnen auch für diese Zwecke hätten überlassen werden dürfen. Für die Zweckbindung bei Weiterverarbeitung von Daten durch nichtöffentliche Stellen sieht Satz 2 darüber hinaus als zusätzliche Beschränkung vor, dass die Justizvollzugsbehörden der Weiterverarbeitung zugestimmt haben.

Satz 3 dient der Umsetzung von Artikel 9 Absatz 3 der Richtlinie (EU) 2016/680, wonach vorzusehen ist, dass immer dann, wenn für die Verarbeitung besondere Bedingungen gelten, die übermittelnde zuständige Behörde die Empfänger der Daten darauf hinweist, dass die Bedingungen gelten und einzuhalten sind.

Zu § 38 Schutzvorkehrungen

§ 38 knüpft an § 30 JVOllzDSG SH in der bisherigen Fassung an.

Die Vorschrift dient der Umsetzung von Artikel 4 Absatz 1 Buchstabe f der Richtlinie (EU) 2016/680, wonach personenbezogene Daten in einer Weise verarbeitet werden müssen, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Gleichzeitig setzt die Bestimmung auch die Vorgaben aus Artikel 19 der Richtlinie (EU) 2016/680 um, wonach der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umzusetzen hat.

Absatz 1 regelt den sicheren Umgang mit personenbezogenen Daten in Akten und Dateisystemen. Für Art und Umfang der hierzu erforderlichen technischen und organisatorischen Maßnahmen verweist Absatz 1 Satz 2 auf die Vorschriften zum Verzeichnis von Verarbeitungstätigkeiten, zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen sowie zur Durchführung einer Datenschutz-Folgenabschätzung bei hohem Risiko für die Rechtsgüter von betroffenen Personen.

Absatz 2 betrifft den Umgang Bediensteter mit und deren Zugang zu personenbezogenen Daten. Jeder Bedienstete darf nur auf solche personenbezogenen Daten zugreifen, die er für die Erfüllung der ihm übertragenen Aufgaben braucht. Diese aus dem Erforderlichkeitsprinzip resultierenden Anforderungen müssen durch technische und organisatorische Schutzmaßnahmen gewährleistet werden, beispielsweise bei Anlage und Aufbewahrung von Akten.

Nach § 11 Absatz 1 werden über Gefangene Gesundheitsakten geführt. Absatz 3 verpflichtet die Justizvollzugsbehörden diese Akten, da sie besonders schützwürdige Daten enthalten, getrennt von anderen Unterlagen zu führen und gegen unbefugten Zugang und unbefugten Gebrauch besonders sichern. Sie unterliegen nur dem Zugriff der jeweiligen Ärztinnen und Ärzte und dem Personal des medizinischen Dienstes.

Zu § 39 **Verzeichnis von Verarbeitungstätigkeiten**

Die Vorschrift, die die bisherigen datenschutzrechtlichen Vorschriften der Länder zur Führung von Verfahrensverzeichnissen ablöst, entspricht § 70 des Bundesdatenschutzgesetzes und dient der Umsetzung von Artikel 24 der Richtlinie (EU) 2016/680. Die Bestimmung verpflichtet die Justizvollzugsbehörden zur Führung eines Verzeichnisses über bei ihnen durchgeführte Kategorien von Datenverarbeitungstätigkeiten. Dieses Verzeichnis dient vor allem der oder dem Landesdatenschutzbeauftragten dazu, einen Überblick über die bei der jeweiligen Justizvollzugsbehörde durchgeführten Datenverarbeitungen zu erhalten.

In Absatz 1 werden die in das Verzeichnis aufzunehmenden Angaben benannt. Der Begriff „Kategorien“ von Verarbeitungstätigkeiten stellt hierbei klar, dass sich das Verzeichnis nicht auf einzelne Datenverarbeitungsvorgänge, sondern auf sinnvoll abgrenzbare und kategorisierbare Teile der bei den Justizvollzugsbehörden durchgeführten Datenverarbeitungen bezieht. Die Reihenfolge der Nummern nach Absatz 1 entspricht derjenigen des Artikels 30 Verordnung (EU) 2016/679. Dies dient der Praktikabilität bei der Erstellung der Verarbeitungsverzeichnisse durch die Justizvollzugsbehörden, die die Verzeichnisse auch im Geltungsbereich der Verordnung (EU) 2016/679 im Rahmen ihrer Verwaltungstätigkeit (Personal- und Wirtschaftsbereich) zu erstellen haben.

Absatz 2 normiert, dass auch der Auftragsverarbeiter ein Verzeichnis aller Kategorien von Verarbeitungen zu führen hat, wengleich auch in geringerem Umfang.

Absatz 3 trifft Aussagen zur Form des Verzeichnisses.

Nach Absatz 4 wird das Verzeichnis der oder dem Landesdatenschutzbeauftragten auf Anforderung zur Verfügung gestellt.

Zu § 40 **Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen**

Die Bestimmung dient der Umsetzung der Artikel 19, 20 und 29 der Richtlinie (EU) 2016/680, die Vorgaben zu den Pflichten des Verantwortlichen, zum Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen sowie zur Sicherheit der Verarbeitung treffen.

Absatz 1 entspricht der Regelung in § 64 Absatz 1 des Bundesdatenschutzgesetzes. Dem Absatz liegt der Gedanke zugrunde, dass die Erforderlichkeit der Maßnahmen daran zu bemessen ist, ob ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht.

Absatz 2 übernimmt den Anforderungskatalog, der dem Standard-Datenschutzmodell entspricht. Er setzt damit zugleich die Artikel 19, 20 und 29 Absatz 1 der Richtlinie (EU) 2016/680 um, die von den Justizvollzugsbehörden verlangen, zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst angemessene Vorkehrungen zu treffen, die geeignet sind, die Datenschutzgrundsätze wie etwa die Datensparsamkeit wirksam umzusetzen, und die sicherstellen, dass die gesetzlichen Anforderungen eingehalten und die Rechte der betroffenen Personen geschützt werden. Die zu treffenden Vorkehrungen haben den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen zu berücksichtigen. Die Gewährleistungsziele des Standard-Datenschutzmodells, denen der Anforderungskatalog entnommen ist, decken sich mit den Anforderungen der Richtlinie (EU) 2016/680 (vgl.

Schlehn, DuD 2018, 32, 36). Neben den Artikeln 19, 20 und 29 Absatz 1 lassen sich außerdem die Artikel 4, 5, 8 bis 14, 16 bis 18, 22, 24, 25, 28, 30 und 31 der Richtlinie (EU) 2016/680 diesen Zielen zuordnen. Die Umsetzung der in Absatz 2 genannten Maßnahmen kann jede Justizvollzugsbehörde in eigener Verantwortung festlegen. Erfolgt die Datenverarbeitung über ein elektronisches Buchhaltungs- und Abrechnungssystem im Justizvollzug, wird die Umsetzung der erforderlichen organisatorischen und technischen Maßnahmen regelmäßig durch die Teilnahme an diesem System erfüllt sein. So ermöglicht beispielsweise das System BASIS-Web alle Funktionen, die für die Umsetzung der genannten Maßnahmen erforderlich sind, insbesondere ein komplexes Rollen- und Rechtssystem. Die tatsächliche Zuordnung der Rechte und Rollen bleibt in der Regel Aufgabe der Anstaltsleiterin oder des Anstaltsleiters.

Absatz 3 dient der Umsetzung von Artikel 29 Absatz 2 der Richtlinie (EU) 2016/680. Satz 1 benennt die Ziele, die im Hinblick auf automatisierte Verarbeitungen durch die Etablierung geeigneter technisch-organisatorischer Maßnahmen verfolgt und erreicht werden sollen. Gemäß Satz 2 können die Zwecke der Datenträgerkontrolle, Speicherkontrolle, Benutzerkontrolle und Zugriffskontrolle insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

Absatz 4 setzt Artikel 20 Absatz 2 der Richtlinie (EU) 2016/680 um. Es ist sicherzustellen, dass durch Voreinstellungen jeweils nur die personenbezogenen Daten verarbeitet werden, deren Verarbeitung nach dem jeweiligen bestimmten Verarbeitungszweck erforderlich ist.

Absatz 5 entspricht im Wesentlichen der Rechtslage in den bisherigen Landesdatenschutzgesetzen. Die Bestimmung verlangt die Erarbeitung eines Sicherheitskonzepts und die Einschätzung von Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für das Recht auf informationelle Selbstbestimmung. Im Gegensatz zur bisherigen Rechtslage sieht der Musterentwurf in Einklang mit der neuen Terminologie und den Vorgaben aus Artikel 27 der Richtlinie (EU) 2016/680 nicht mehr eine Vorabkontrolle durch den Verantwortlichen (wie noch Artikel 20 der Richtlinie 95/46/EG) vor. Eine Vorabkontrolle sehen die Richtlinie (EU) 2016/680 und dementsprechend auch der Entwurf nur noch bei einem hohen Risiko für das Recht auf informationelle Selbstbestimmung im Rahmen der nach § 41 durchzuführenden Datenschutz-Folgenabschätzung vor. Gleichwohl soll die bewährte Praxis einer Einschätzung von Risiken für das Recht auf informationelle Selbstbestimmung anhand eines Sicherheitskonzepts auch für Verarbeitungsvorgänge unterhalb dieser Schwelle beibehalten werden. Nach Absatz 5 sollen die Folgen von Datenverarbeitungssystemen daher unabhängig von den Voraussetzungen einer Datenschutz-Folgenabschätzung bereits im Rahmen eines Sicherheitskonzepts eingeschätzt werden. Dadurch werden zugleich die Vorgaben aus Artikel 20 Absatz 1 und Artikel 29 Absatz 1 der Richtlinie (EU) 2016/680 umgesetzt, wonach der für die Datenverarbeitung Verantwortliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken zu bewerten und auf dieser Grundlage technische und organisatorische Maßnahmen zu ergreifen hat. § 41, der die Durchführung einer umfassenden Datenschutz-Folgenabschätzung bei hohem Risiko für die Rechtsgüter betroffener Personen regelt, bleibt unberührt.

Zu § 41 Datenschutz-Folgenabschätzung bei hohem Risiko, Konsultations-pflicht

Die Vorschrift entspricht im Wesentlichen der Regelung in § 67 des Bundesdatenschutzgesetzes.

Absatz 1 dient der Umsetzung von Artikel 27 der Richtlinie (EU) 2016/680. Kriterien für die Entscheidung, ob die vorgesehene Verarbeitung qualitativ erhöhte Gefahren für die Rechtsgüter der betroffenen Personen zur Folge hat, können beispielsweise die Art der zur Datenerhebung eingesetzten Mittel oder der Kreis der zugriffsberechtigten Personen, mit hin die Eingriffsintensität der mit der Verarbeitung verbundenen Maßnahmen im Sinne einer Gesamtwürdigung sein. Dabei ist zu beachten, dass das Erfordernis der Durchführung einer Datenschutz-Folgenabschätzung nur für neue nach Inkrafttreten dieses Gesetzes eingesetzte Verarbeitungssysteme oder wesentliche Veränderungen an bestehenden Systemen gilt.

Absatz 2 nimmt Artikel 35 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 und Absatz 3 nimmt Artikel 35 Absatz 2 der Verordnung (EU) 2016/679 auf, die eine sinnvolle Ergänzung der Vorgaben der Richtlinie (EU) 2016/680 darstellen.

Absatz 4 legt den Inhalt der Datenschutz-Folgenabschätzung fest und konkretisiert die in Artikel 27 Absatz 2 der Richtlinie (EU) 2016/680 enthaltenen allgemeinen Angaben durch Übernahme der in Artikel 35 Absatz 7 der Verordnung (EU) 2016/679 enthaltenen Vorgaben.

Absatz 5 entspricht § 69 Absatz 1 Bundesdatenschutzgesetz.

Absatz 6 entspricht § 69 Absatz 2 Bundesdatenschutzgesetz.

Absatz 7 entspricht § 69 Absatz 3 Bundesdatenschutzgesetz.

Absatz 8 entspricht § 69 Absatz 4 Bundesdatenschutzgesetz.

Zu § 42 Protokollierung

Die Vorschrift dient der Umsetzung von Artikel 25 der Richtlinie (EU) 2016/680 und ermöglicht eine Kontrolle der Rechtmäßigkeit der Datenverarbeitungsvorgänge.

Absatz 1 regelt in Umsetzung von Artikel 25 Absatz 1 Satz 1 der Richtlinie (EU) 2016/680 eine Pflicht zur Protokollierung von bestimmten Datenverarbeitungsvorgängen in automatisierten Verarbeitungssystemen. In Erweiterung der Vorgaben der Richtlinie (EU) 2016/680 wurde der Katalog in Nummer 1 um die Speicherung der Daten und in Nummer 6 um die Einschränkung der Verarbeitung ergänzt. Die Regelung erfasst unter anderem auch die Protokollierung automatisierter Datenübertragungen an Schnittstellen von Verfahren zu anderen Verfahren sowie Verarbeitungsvorgänge durch den Administrator. Ebenfalls erfasst wird die Protokollierung so genannter „lesender Zugriffe“, bei denen Informationen aus dem Verarbeitungssystem im Sinne des Artikels 25 Absatz 1 Satz 1 der Richtlinie (EU) 2016/680 abgefragt werden (vgl. *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, Artikel 4 DSGVO Rn. 27; Schaffland/Wiltfang, DS-GVO/BDSG, Artikel 4 DSGVO Rn. 74; nach anderer Auffassung handelt es sich bei dem lesenden Zugriff um einen Unterfall der Erhebung, vgl. *Schild*, in: BeckOK Datenschutzrecht, Artikel 4 DSGVO Rn. 47; *Ernst*, in: Paal/Pauly, DS-GVO/BDSG, Artikel 4 DSGVO Rn. 28).

Absatz 2 enthält konkrete Vorgaben für den Inhalt der Protokolle. Dem Erwägungsgrund Nummer 57 der Richtlinie (EU) 2016/680 lässt sich entnehmen, dass die Identität der Person, die personenbezogene Daten abgefragt oder offengelegt hat, protokolliert wird und sich daraus die Begründung für die Verarbeitungsvorgänge ableiten lassen sollte. Die Protokollierung lesender Zugriffe erfolgt ab dem Jahr 2023 bei Aufruf der jeweiligen Hauptkarteikarte im Verfahren BASIS-Web, dem ein differenziertes Rechte- und Rollenkonzept für Zugriffsberechtigungen zugrunde liegt. Dieses Konzept lässt einen Rückschluss auf den Grund einer Abfrage oder Offenlegung zu und erfüllt damit die Anforderungen des Artikels 25 der Richtlinie (EU) 2016/680.

Absatz 3 Satz 1 befasst sich mit den Verwendungsbeschränkungen für Protokolldaten. Grundsätzlich dürfen die Protokolldaten nur zum Zwecke der Datenschutzkontrolle, Eigenüberwachung und Aufrechterhaltung der Datensicherheit verwendet werden. Die Protokollierung dient dem Schutz des Rechts auf informationelle Selbstbestimmung und ist eine den Grundrechtseingriff abmildernde Verfahrenssicherung. Unter engen Voraussetzungen dürfen die Protokolle nach Absatz 3 Satz 2 auch zur Verfolgung von Straftaten und Ordnungswidrigkeiten oder zur Einleitung beamtenrechtlicher oder disziplinarrechtlicher Maßnahmen im Zusammenhang mit einer Verletzung des Datengeheimnisses sowie zur Verfolgung von Straftaten von erheblicher Bedeutung verarbeitet werden. Die entsprechende Zweckänderung wird in Artikel 25 Absatz 2 der Richtlinie (EU) 2016/680 zugelassen.

Nach der Entscheidung des EuGH in der Rechtssache C-553/07 (EuGH, Urteil vom 7. Mai 2009, C-553/07) sind Protokolldaten für einen Zeitraum aufzubewahren, der es den betroffenen Personen ermöglicht, die Rechtmäßigkeit der Verarbeitung nachzuvollziehen. Das Bundesverfassungsgericht hat in seiner Entscheidung zum Bundeskriminalamtgesetz (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09) ausgeführt, dass durch technische und organisatorische Maßnahmen sichergestellt werden muss, dass die Protokolldaten der oder dem Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben zu dem zu kontrollierenden Vorgang enthält. Angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle kommt ihrer regelmäßigen Durchführung besondere Bedeutung zu. Die Kontrollen sind in angemessenen Abständen – deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf – durchzuführen (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 141). Absatz 4 legt daher fest, dass die Protokolldaten erst zwei Jahre

nach ihrer Generierung gelöscht werden, was eine effektivere Kontrolle der Verarbeitungsvorgänge ermöglicht.

Absatz 5 legt fest, dass die Protokolle der oder dem Landesdatenschutzbeauftragten zum Zweck der Datenschutzkontrolle zur Verfügung gestellt werden müssen. Die Vorschrift setzt Artikel 25 Absatz 3 der Richtlinie (EU) 2016/680 um.

Die Bestimmung tritt gemäß § 65 Absatz 2 erst am 6. Mai 2023 in Kraft.

Zu § 43 **Kenntlichmachung innerhalb der Anstalt**

§ 43 entspricht im Wesentlichen § 31 JVVollzDSG SH in der bisherigen Fassung.

Die Bestimmung erlaubt nach Absatz 1 in engen Grenzen die Kenntlichmachung personenbezogener Daten innerhalb der Justizvollzugsanstalt. Eine Bestimmung dieses Gesetzes, die der Kenntlichmachung entgegenstehen könnte, ist § 10.

Besondere Kategorien personenbezogener Daten dürfen nach Absatz 2 nicht kenntlich gemacht werden.

Zu § 44 **Erkenntnisse aus Beaufsichtigungs-, Überwachungs- und Kontrollmaßnahmen**

§ 44 greift § 32 JVVollzDSG SH in der bisherigen Fassung auf.

Erkenntnisse aus Überwachungsmaßnahmen unterliegen einem besonderen Schutz, da durch Überwachungsmaßnahmen in besonders sensibler Weise in das informationelle Selbstbestimmungsrecht der betroffenen Personen eingegriffen wird. Häufig stammen diese Erkenntnisse aus einem zulässigen Eingriff in Artikel 10 Absatz 1 GG. Der Schutzbereich des Artikels 10 GG umfasst auch die Informations- und Datenverarbeitungsprozesse, die sich an die Kenntnisnahme von geschützten Kommunikationsdaten anschließen, sowie den Gebrauch dieser Kenntnisse (vgl. BVerfGE 100, 313, 359). Dabei stellt jede Kenntnisnahme, Aufzeichnung und Verwertung von Kommunikationsdaten sowie die Auswertung des Inhalts und die sonstige Verwendung durch die öffentliche Gewalt einen eigenständigen Grundrechtseingriff dar (vgl. BVerfGE 85, 386, 398; 100, 313, 366; 110, 33, 52 ff.).

Um den Grundrechtsschutz zu gewährleisten, darf nach Absatz 1 eine Verarbeitung nur mit Einwilligung der Gefangenen oder aufgrund der privilegierten Zwecke in Absatz 1 Satz 2 Nummer 2 und 3 erfolgen. Missbräuchen ist durch besondere Kennzeichnung der sensiblen Daten vorzubeugen.

Absatz 2 erweitert die privilegierten Zwecke für die spezifischen Belange der Untersuchungshaft und der in § 1 Absatz 1 Nummer 2 genannten Haftarten.

Soweit der Kernbereich der privaten Lebensgestaltung betroffen ist, darf eine Verarbeitung der personenbezogenen Daten nach Absatz 3 Satz 1 nicht erfolgen, also auch keine Aufzeichnung oder Protokollierung durch die beaufsichtigenden Beamten. Satz 2 stellt klar, dass vom Kernbereich der privaten Lebensgestaltung Gespräche über Straftaten oder Gespräche, durch die Straftaten begangen werden, in der Regel nicht erfasst sind. Zur näheren Konkretisierung des Kernbereichs privater Lebensgestaltung wird auf die Begründung zu § 33 Absatz 3 Satz 4 verwiesen. Sollten dennoch Daten gespeichert worden sein, sind sie unverzüglich zu löschen. Durch die in Absatz 3 festgeschriebene Löschungspflicht und die damit verbundene Dokumentationspflicht soll dem Grundrechtsschutz Rechnung getragen und dessen Einhaltung kontrollierbar gemacht werden.

Abschnitt 7

Besondere Bestimmungen für Geheimnisträgerinnen und Geheimnisträger**Zu § 45 Geheimnisträgerinnen und Geheimnisträger**

Die Bestimmung dient der Umsetzung von Artikel 10 der Richtlinie (EU) 2016/680 und entspricht § 33 JVollzDSG SH in der bisherigen Fassung.

In Absatz 1 sind im und für den Justizvollzug arbeitende Personen aufgeführt, die einer gesetzlichen Geheimhaltungspflicht unterliegen beziehungsweise deren Tätigwerden eine Geheimhaltungspflicht erfordert. Die in Absatz 1 Satz 1 Nummer 1 bis 3 aufgeführten Personen unterliegen der gemäß § 203 Absatz 1 StGB sanktionierten Verschwiegenheitsverpflichtung. Für diese Personen wie auch für die in Absatz 1 Satz 1 Nummer 4 genannten Seelsorgerinnen und Seelsorger schreibt Absatz 1 die grundsätzliche Verschwiegenheit untereinander sowie gegenüber den Justizvollzugsbehörden vor. Diese Schweigepflicht erfasst auch ihre Gehilfinnen und Gehilfen und die Personen, die zur Berufsausübung bei ihnen tätig sind, jedoch nicht im Verhältnis zu den Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern selbst.

Absatz 2 verpflichtet die Anstalt, externe Berufsgeheimnisträger bei ihrer Beauftragung auf die vollzugsspezifischen Offenbarungsbefugnisse und –pflichten hinzuweisen. Bei externen Ärzten, Psychologen usw., die nicht regelmäßig mit der Behandlung von Gefangenen befasst sind, kann nicht vorausgesetzt werden, dass diesen die in diesem Gesetz konstituierten besonderen Offenbarungsbefugnisse und –pflichten geläufig sind. Die Hinweispflicht ermöglicht es einerseits den Behandlern, ihre Interaktion mit den Gefangenen entsprechend zu gestalten und vermeidet andererseits spätere Komplikationen, etwa wenn die Anstalt Auskunft zu bestimmten Behandlungsergebnissen auf der Grundlage des § 34 verlangt.

Zu § 46 Offenbarungspflicht

Die Bestimmung dient der Umsetzung von Artikel 10 der Richtlinie (EU) 2016/680 und stimmt weitgehend mit § 34 JVollzDSG SH in der bisherigen Fassung überein.

Die Berufsheimnisträgerinnen und Berufsheimnisträger sind nach Absatz 1 verpflichtet, die ihnen bekannt gewordenen personenbezogenen Daten gegenüber der Anstaltsleiterin oder dem Anstaltsleiter zu offenbaren, wenn Gefahr für Leib oder Leben oder eine erhebliche Straftat droht.

Nach Absatz 2 haben staatlich anerkannte Sozialarbeiterinnen und Sozialarbeiter sowie Sozialpädagoginnen und Sozialpädagogen, die als Bedienstete im Justizvollzug tätig sind, über Absatz 1 hinaus eine weitergehende Offenbarungspflicht. Sie sind als Bedienstete Teil der Anstalt und haben keine besondere Vertrauensstellung, wie sie üblicherweise außerhalb des Justizvollzuges besteht. Deshalb müssen sie ihre Kenntnisse der Anstaltsleiterin oder dem Anstaltsleiter bereits dann mitteilen, wenn dies zu vollzuglichen Zwecken erforderlich ist.

Absatz 3 erleichtert die Erfüllung der Offenbarungspflicht von Berufsheimnisträgerinnen und Berufsheimnisträgern außerhalb des Justizvollzuges. Da sie regelmäßig im Kontakt mit den Berufsheimnisträgerinnen und Berufsheimnisträgern innerhalb des Justizvollzuges stehen, ist auf diesem Kommunikationsweg eine schnellere und effektivere Information der Anstalt zu erwarten. Es ist bei dieser Konstellation Aufgabe der Anstalt, Berufsheimnisträgerinnen und Berufsheimnisträger außerhalb des Justizvollzuges über die Offenbarungspflichten in Kenntnis zu setzen, da nicht davon ausgegangen werden kann, dass diese ohne eine solche Information Kenntnis über diese besonderen Verpflichtungen haben.

Die gesamte Bestimmung stellt eine Rechtfertigungsnorm für Berufsheimnisträgerinnen und Berufsheimnisträger dar.

Zu § 47 Offenbarungsbefugnis

Die Bestimmung dient der Umsetzung von Artikel 10 der Richtlinie (EU) 2016/680 und entspricht im Wesentlichen § 35 JVollzDSG SH in der bisherigen Fassung.

Regelmäßig ist davon auszugehen, dass Berufsheimnisträgerinnen und Berufsheimnisträger aufgrund eigener Sachkunde beurteilen können, inwieweit die ihnen bekannt gewordenen personenbezogenen Daten für vollzugliche Zwecke auch unter Berücksichtigung der Interessen der Gefangenen an der Geheimhaltung unbedingt erforderlich sind. Deshalb obliegt ihnen die Entscheidung, ob sie Informationen an die Anstaltsleiterin oder den Anstaltsleiter weitergeben. Auch hier obliegt es der Anstalt, die außerhalb des Justizvollzuges tätigen Berufsheimnisträgerinnen und Berufsheimnisträger über die hier eingeräumte Befugnis zu informieren. Die Bestimmung stellt wie die vorhergehende ebenfalls eine Rechtfertigungsnorm dar.

Um eine effektive Behandlung der Gefangenen zu gewährleisten, konstituiert Absatz 2 im Verhältnis der Berufsheimnisträgerinnen und Berufsheimnisträger untereinander eine Offenbarungsbefugnis und damit eine Ausnahme von der Schweigepflicht nach § 33 JVollzDSG SH. Beim Vorliegen der genannten Voraussetzungen sind die Berufsheimnisträgerinnen und Berufsheimnisträger zur gegenseitigen Information und Auskunft befugt. Dies ist notwendig, um eine zielgerichtete Behandlung zu ermöglichen. Die Offenbarungsbefugnis gilt berufsgruppenübergreifend. Die gegenüber Absatz 1 erleichterte Offenbarungsbefugnis gegenüber anderen Berufsheimnisträgern gilt jedoch nicht, wenn die Adressatin oder der Adressat einer Mitteilung auch andere, insbesondere exekutive

Aufgaben in der Anstalt ausübt, da sonst der behandlungsbezogene Vertraulichkeitsschutz nicht ausreichend sichergestellt wäre.

Zu § 48 **Benachrichtigung der Gefangenen über Offenbarungen**

Die Bestimmung dient der Umsetzung von Artikel 10 und Artikel 12 Absatz 2 der Richtlinie (EU) 2016/680 und stimmt weitgehend mit § 36 JVollzDSG SH in der bisherigen Fassung überein.

Damit die Gefangenen selbstbestimmt über die Preisgabe von Informationen entscheiden können, müssen sie über die Offenbarungspflichten und Offenbarungsbefugnisse der Berufsheimnisträgerinnen und Berufsheimnisträger informiert sein. Zum Ausschluss von Missverständnissen und zum Nachweis einer ausreichenden Information haben die Unterrichtungen durch die Berufsheimnisträgerinnen und Berufsheimnisträger vor der Erhebung schriftlich zu erfolgen.

Als verantwortliche Stelle hat die Anstalt bei Einschaltung von Berufsheimnisträgerinnen und Berufsheimnisträgern außerhalb der Anstalt selbst dafür zu sorgen, dass die Gefangenen vor der Erhebung über die Offenbarungspflichten und Offenbarungsbefugnisse der Berufsheimnisträgerinnen und Berufsheimnisträger informiert sind.

Während in Absatz 1 die grundsätzliche und abstrakte Vorabinformation der Gefangenen geregelt ist, schreibt Absatz 2 Satz 1 die Information nach konkreter Offenbarung vor, damit die Gefangenen über die tatsächliche Weiterleitung von Daten Kenntnis erlangen.

Zu § 49 **Zweckbindung offenbarter personenbezogener Daten, Zulassung von Offenbarungsempfängern**

§ 49 entspricht § 37 JVollzDSG SH in der bisherigen Fassung.

Absatz 1 schreibt wegen der Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung bei der Offenbarung von personenbezogenen Daten aus einem besonderen Vertrauensverhältnis die strenge Zweckbindung der offenbarten Daten vor.

Nach Absatz 2 kann die Anstaltsleiterin oder der Anstaltsleiter allgemein festlegen, gegenüber welchen anderen Bediensteten eine Offenbarung erfolgen darf.

Zu § 50 **Zugriff auf Daten in Notfällen**

Die Bestimmung dient der Umsetzung von Artikel 8 Absatz 1 der Richtlinie (EU) 2016/680 und entspricht weitgehend § 38 JVollzDSG SH in der bisherigen Fassung.

Durch die Bestimmung wird der Zugriff auf personenbezogene Daten in Notfällen ermöglicht und damit klargestellt, dass datenschutzrechtliche Regelungen eine Notfallrettung nicht behindern dürfen. Die direkte Kenntnisverschaffung ist jedoch auf die im Justizvollzug tätigen Personen beschränkt, die dann eine Weitergabe an die für die Notfallrettung eingesetzten - im Regelfall anstaltsfremden - Personen vorzunehmen haben.

Absatz 2 dehnt unter den dortigen Voraussetzungen die Rechte und Pflichten aus Absatz 1 ausdrücklich auch auf die personenbezogene Daten aus, die von Berufsheimnisträgerinnen und Berufsheimnisträgern erhoben wurden.

Durch das Verbot einer anderweitigen Zweckverwendung und durch die Dokumentationspflicht in Absatz 3 wird einer Missbrauchsgefahr vorgebeugt.

Abschnitt 8

Rechte der betroffenen Personen**Zu § 51 Allgemeine Informationen zur Datenverarbeitung**

Die Vorschrift dient der Umsetzung von Artikel 13 Absatz 1 der Richtlinie (EU) 2016/680. Die Justizvollzugsbehörden haben hier aktive Informationspflichten gegenüber betroffenen Personen unabhängig von der Geltendmachung von Betroffenenrechten. Diesen Informationspflichten können die Justizvollzugsbehörden in allgemeiner Form nachkommen. Betroffene Personen sollen unabhängig von der Datenverarbeitung im konkreten Fall in leicht zugänglicher Weise einen Überblick über die Verarbeitungszwecke und eine Übersicht über ihre Betroffenenrechte erhalten. Wie sich aus Erwägungsgrund 42 der Richtlinie (EU) 2016/680 ergibt, kann dieser Verpflichtung zum Beispiel durch entsprechende Informationen auf einer Internetseite nachgekommen werden. Bei Gefangenen wird dieser Verpflichtung durch allgemeine Informationen in Schriftform bei der Aufnahme in den Justizvollzug nachgekommen werden können.

Zu § 52 Hinweispflicht bei der Datenerhebung mit Kenntnis und Mitwirkung der betroffenen Personen

Diese Vorschrift überträgt den Justizvollzugsbehörden die Verantwortung dafür, dass die betroffenen Personen über den Zweck der Datenerhebung und ihre Rechte in Kenntnis gesetzt werden. Nur so können sie im Rahmen ihrer Möglichkeiten selbstbestimmt über den Umgang mit ihren personenbezogenen Daten entscheiden, darauf Einfluss nehmen oder sich informieren. Durch die Information an die Gefangenen soll Rechtsnachteilen vorgebeugt werden.

Zu § 53 Benachrichtigung bei Datenerhebung ohne Kenntnis und Mitwirkung der betroffenen Personen

Die Bestimmung dient der Umsetzung von Artikel 13 Absatz 2 der Richtlinie (EU) 2016/680. In „besonderen Fällen“ muss die Benachrichtigung der betroffenen Person weitere Informationen umfassen. Die besonderen Fälle werden in der Richtlinie (EU) 2016/680 nicht näher definiert. Auch die Erwägungsgründe geben darüber keinen weiteren Aufschluss. Aus Artikel 13 Absatz 2 Buchstabe d der Richtlinie (EU) 2016/680 lässt sich schließen, dass hierunter vor allem die Fälle zu fassen sind, in denen von Gefangenen oder anderen betroffenen Personen ohne deren Wissen Daten erhoben werden. Es ist jedoch davon auszugehen, dass auch eine Übermittlung der Daten zu anderen als den ursprünglichen Erhebungszwecken eine Benachrichtigungspflicht auslöst, da damit ein vertiefter Eingriff in das Recht auf informationelle Selbstbestimmung verbunden ist.

Absatz 1 sieht eine Benachrichtigungspflicht der Justizvollzugsbehörden vor, wenn ohne Kenntnis und Mitwirkung der betroffenen Person personenbezogene Daten erhoben oder übermittelt worden sind. In diesen Fällen sind neben den in § 51 genannten Informationen weitere Angaben über die Rechtsgrundlage der Verarbeitung, die Dauer der Verarbeitung und die Empfängerinnen und Empfänger sowie die Herkunft der Daten zu machen sind.

Absatz 2 ermöglicht es, in Umsetzung von Artikel 13 Absatz 3 der Richtlinie (EU) 2016/80 von der Bereitstellung der in Absatz 1 genannten Informationen abzusehen. Absatz 2 sieht entsprechend den bisherigen Regelungen in den jeweiligen Datenschutzbestimmungen des Justizvollzuges (z.B. § 39 Absatz 1 JVollzDSG SH) einen Katalog von Ausnahmen von der Benachrichtigungspflicht vor, der um die in Artikel 13 Absatz 3 der Richtlinie (EU) 2016/680 genannten Tatbestände erweitert wurde. Die Ausnahmen von der Benachrichtigungspflicht korrespondieren mit den entsprechenden Einschränkungen bei der Erteilung

von Auskünften an die betroffenen Personen in Artikel 15 Absatz 1 der Richtlinie (EU) 2016/680 (§ 54). Die Entscheidung, die Benachrichtigung aufzuschieben, einzuschränken oder zu unterlassen, muss Verhältnismäßigkeitsgrundsätzen genügen und ihr muss eine nachvollziehbare Interessenabwägung vorausgehen. Eine Ausnahme von der Benachrichtigungspflicht ist gerechtfertigt, wenn ein überwiegendes Interesse an der Vermeidung der in Absatz 2 genannten Gefahren und Nachteile im Vergleich zu dem Informationsinteresse der betroffenen Personen gegeben ist. Wenn aufgrund der konkreten Umstände des Einzelfalls das Informationsinteresse der betroffenen Personen das Geheimhaltungsinteresse überwiegt, hat dementsprechend eine Benachrichtigung zu erfolgen.

Nach Absatz 3 ist vor der Benachrichtigung der betroffenen Personen die Zustimmung der benannten öffentlichen Stellen einzuholen, damit die Informationserteilung laufende Verfahren der genannten staatlichen Stellen, etwa Ermittlungsverfahren der Staatsanwaltschaft, nicht gefährdet. Aufgrund der erweiterten Benachrichtigungspflichten und dem Gleichklang mit den Auskunftspflichten ist die entsprechende Ausnahme bereits bei der Entscheidung über eine Benachrichtigung der betroffenen Personen geboten, um die genannten Verfahren nicht schon allein durch die Benachrichtigung zu gefährden. Die Vorschrift steht in Einklang mit Erwägungsgrund Nummer 44 der Richtlinie (EU) 2016/680, der klarstellt, dass eine Unterrichtung, Auskunft, Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung unterlassen werden kann, um laufende Ermittlungsverfahren nicht zu gefährden. Dies gilt auch für Informationen von Nachrichtendiensten, deren Tätigkeit vom Anwendungsbereich der Richtlinie (EU) 2016/680 nicht erfasst wird (s. Erwägungsgrund Nummer 14).

Absatz 4 nimmt bezüglich des Ausschlusses einer Benachrichtigung gegenüber den betroffenen Personen auf die Regelungen zum Auskunftsrecht in § 54 Absatz 6 Bezug. Im Fall einer eingeschränkten Benachrichtigung sind die betroffenen Personen zu unterrichten. Dies gilt jedoch nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung, einen Nachteil oder eine Beeinträchtigung im Sinne des § 53 Absatz 2 mit sich bringen würde. Benachrichtigungen der Gefangenen oder anderer betroffener Personen können mithin entfallen, wenn im konkreten Fall schon durch die Benachrichtigung hochrangige Interessen gefährdet werden (vgl. Erwägungsgrund Nummer 44 der Richtlinie (EU) 2016/680. In diesem Fall kann im Ausnahmefall auch eine Befassung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit nicht zulässig sein. Die Justizvollzugsbehörden dokumentieren die Gründe für das Aufschieben, Einschränken oder Unterlassen der Benachrichtigung nach Absatz 2.

Zu § 54 **Auskunftsrecht der betroffenen Personen**

Die Bestimmung regelt in Umsetzung von Artikel 14 der Richtlinie (EU) 2016/680 das Auskunftsrecht der Gefangenen und anderer betroffenen Personen. Von diesen Auskunftsrechten lässt Artikel 15 der Richtlinie (EU) 2016/680 Ausnahmen zu. Schon § 40 JVOllzDSG SH sah Auskunftsrechte der Gefangenen vor, die unter bestimmten Voraussetzungen entfallen konnten.

Absatz 1 Satz 1 legt das grundsätzliche Bestehen eines Auskunftsrechtes fest. Satz 2 erweitert den Umfang der Auskunftserteilung. Der in den Nummern 1 und 4 genannte Begriff „Kategorie“ ermöglicht den Justizvollzugsbehörden eine angemessene Generalisierung der Angaben zu den verarbeiteten personenbezogenen Daten und den Übermittlungsempfängern. Die Angaben nach Nummer 1 zu den verarbeiteten personenbezogenen Daten können im Sinne einer zusammenfassenden Übersicht in verständlicher Form gemacht werden. Die Angaben müssen also nicht in einer Form gemacht werden, die Aufschlüsse über die Art und Weise der Speicherung oder Sichtbarkeit der Daten bei den Vollzugsbehörden (im Sinne einer Kopie) zulässt. Ebenso bedeutet die Pflicht zur Angabe der verfügbaren Informationen zur Datenquelle nicht, dass die Identität natürlicher Personen oder gar vertrauliche Informationen preisgegeben werden müssen. Die Justizvollzugsbehörden müssen sich bei der Angabe zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, letztlich von dem gesetzgeberischen Ziel leiten lassen, bei der betroffenen Person ein Bewusstsein über Umfang und Art der verarbeiteten Daten zu erzeugen und es ihr ermöglichen, aufgrund dieser Informationen zu ermitteln, ob die Verarbeitung rechtmäßig ist und - wenn Zweifel hieran bestehen - gegebenenfalls die Geltendmachung weiterer Betroffenenrechte auf diese Informationen stützen zu können.

Absatz 2 orientiert sich an § 19 Absatz 2 und § 33 Absatz 2 Satz 1 des Bundesdatenschutzgesetzes in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 10 Absatz 2 des Gesetzes vom 31. Oktober 2017 (BGBl. I S. 3618) geändert worden ist. In Erweiterung der bisherigen Rechtslage hat der Verantwortliche jedoch sicherzustellen, dass durch geeignete technische und organisatorische Maßnahmen eine Verwendung der Daten zu anderen Zwecken ausgeschlossen ist. Bei der Ermittlung des Aufwands hat der Verantwortliche die bestehenden technischen Möglichkeiten, gesperrte und archivierte Daten der betroffenen Personen im Rahmen der Auskunftserteilung verfügbar zu machen, zu berücksichtigen. Werden die Daten ausschließlich aufgrund von Aufbewahrungsvorschriften gespeichert, ist die Verarbeitung der Daten einzuschränken.

Eine Auskunftserteilung kann nach Absatz 3 in den Fällen unterbleiben, in denen die betroffenen Personen keine hinreichend konkreten Angaben machen, mit denen sich die verarbeiteten Daten ermitteln lassen. Macht etwa eine Besucherin oder ein Besucher keine Angaben dazu, welchen Gefangenen sie oder er besucht hat, würde die Verpflichtung zur Auskunftserteilung einen unverhältnismäßigen Aufwand der Vollzugsbehörde verursachen.

Absatz 4 übernimmt durch seinen Verweis auf § 53 Absatz 2 und Absatz 3 die Ausschlussgründe, nach denen von einer Benachrichtigung abgesehen werden kann, auch für die Auskunftserteilung. Je nach Umfang der beeinträchtigten Interessen kann die Auskunft vollständig oder teilweise eingeschränkt werden. Die Einschränkungen entsprechen Artikel 15 Absatz 1 und Erwägungsgrund Nummer 44 der Richtlinie (EU) 2016/680.

Absatz 5 Sätze 1 und 2 dienen der Umsetzung von Artikel 15 Absatz 3 Sätze 1 und 2 der Richtlinie (EU) 2016/680. Unter der Voraussetzung von Satz 2 wird den Justizvollzugsbehörden das Recht gewährt, ein Auskunftsverlangen gänzlich unbeantwortet zu lassen. Nach Satz 3 ist die Nichterteilung der Auskunft zu begründen, um den Gefangenen oder

anderen betroffenen Personen die Überprüfung der Nichterteilung der Auskunft zu ermöglichen.

Absatz 6 Satz 1 sieht in Umsetzung von Artikel 17 der Richtlinie (EU) 2016/680 als neues Verfahren zum effektiven Schutz der Rechte der betroffenen Personen die Überprüfung der Verarbeitungstätigkeit durch die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit in einem besonderen Verfahren vor. Nach Absatz 6 Satz 1 tritt die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit in die Rechte der betroffenen Personen ein. Die Justizvollzugsbehörden weisen die betroffenen Personen darauf hin, dass sie ihr Auskunftsrecht durch die oder den Landesbeauftragten für Datenschutz und Informationsfreiheit ausüben lassen können, und auf die Möglichkeit zur Inanspruchnahme gerichtlichen Rechtsschutzes (Satz 7). Machen die betroffenen Personen von ihrem Recht Gebrauch, ist der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit die entsprechende Auskunft zu erteilen. Die Sätze 4 bis 6 regeln das Verfahren der Auskunftserteilung und der Weitergabe von Ergebnissen der Prüfung an die betroffenen Personen.

Die Form der Auskunftserteilung liegt nach Absatz 7 im pflichtgemäßen Ermessen der Behörde. Die Auskunft kann auch durch Überlassung von Kopien oder Akteneinsicht erteilt werden. Das Interesse der betroffenen Person ist bei Ausübung des Ermessens zu berücksichtigen.

Absatz 8 dient der Umsetzung von Artikel 15 Absatz 4 der Richtlinie (EU) 2016/680.

Zu § 55 Akteneinsichtsrecht

Absatz 1 Satz 1 regelt über Artikel 14 der Richtlinie (EU) 2016/680 hinausgehend die Voraussetzungen des Akteneinsichtsrechts der betroffenen Personen. Satz 2 stellt klar, dass die mit einem Sperrvermerk versehenen Aktenbestandteile nicht der Akteneinsicht unterliegen.

Absatz 2 Satz 1 regelt, welche Personen bei einer Akteneinsichtnahme hinzugezogen werden können. Satz 2 gestattet die alleinige Akteneinsicht durch die Beauftragten. Um Abhängigkeiten der Gefangenen untereinander zu vermeiden und subkulturellem Verhalten im Justizvollzug vorzubeugen, sieht Satz 3 vor, dass eine Hinzuziehung oder Beauftragung von Mitgefangenen nicht zulässig ist.

Absatz 3 gewährt den betroffenen Personen das Recht, sich aus den Akten Notizen zu machen.

Absatz 4 regelt, unter welchen Voraussetzungen betroffenen Personen Ablichtungen oder Ausdrucke einzelner Dokumente zu überlassen sind.

Absatz 5 Satz 1 normiert die Unentgeltlichkeit der Akteneinsicht. Die Sätze 2 und 3 regeln die Verpflichtung zur Erstattung der Kosten für Ablichtungen und Ausdrucke und die Vorschusspflicht. Dies steht im Einklang mit Artikel 12 Absatz 4 der Richtlinie (EU) 2016/680, wonach bereits für die Erteilung von Informationen unter Berücksichtigung der Verwaltungskosten eine angemessene Gebühr erhoben werden kann. Nach Satz 4 können die Justizvollzugsbehörden in begründeten Ausnahmefällen wie beim Schriftwechsel und den Telefonaten als Ausfluss aus dem Sozialstaatsprinzip die bei ihnen anfallenden Kosten für die Gefangenen in angemessenem Umfang übernehmen, wenn diese hierzu nicht in der Lage sind.

Zu § 56 Auskunft und Akteneinsicht in Gesundheitsakten

In Umsetzung der Entscheidung des Bundesverfassungsgerichts vom 20. Dezember 2016 (2 BvR 1541/15) gewährt § 56 Satz 1 den Gefangenen einen Anspruch auf Auskunft aus ihren und Einsicht in ihre Gesundheitsakten. Durch die Verweisung in Satz 2 wird unter anderem die Hinzuziehung und Beauftragung von bestimmten Personen und die Kostenregelung bei der Akteneinsicht aus § 55 für entsprechend anwendbar erklärt.

Zu § 57 Sperrvermerke

§ 57 entspricht im Wesentlichen § 42 Absatz 1 und 2 JVollzDSG SH in der bisherigen Fassung.

Absatz 1 enthält zur Sicherung des Akteneinsichtsrechtes eine abschließende Aufzählung der Gründe, die zur Anbringung eines Sperrvermerks berechtigen. Die Bestimmung bezieht sich nur auf das Akteneinsichtsrecht nach § 55; dieses ist nicht durch die Richtlinie (EU) 2016/680 vorgegeben. Nach § 55 Absatz 1 Satz 2 unterliegen Aktenbestandteile, die mit einem Sperrvermerk versehen sind, nicht der Akteneinsicht; davon unberührt bleibt das allgemeine Auskunftsrecht nach § 54. Die Bestimmung dient der Verwaltungsvereinfachung und ermöglicht es, direkt bei der Aufnahme eines Dokuments in die Akte eine Entscheidung über eine spätere Offenlegung zu treffen.

Das Informationsinteresse der Gefangenen muss zurücktreten, wenn medizinische Gründe allein zum Wohl der Gefangenen, der Schutz der genannten Rechtsgüter oder eine gesetzliche Geheimhaltungspflicht Vorrang beanspruchen. Satz 1 verpflichtet zu einer Güterabwägung im Einzelfall, die nach Absatz 2 hinsichtlich Grund und Umfang auch zu dokumentieren ist. Nummer 1 ist eng auszulegen, um eine informationelle Bevormundung zu vermeiden. Dennoch kann in besonders gelagerten Fällen, etwa im Zusammenhang mit

psychiatrischen Behandlungen, ein Sperrvermerk auch zu Gunsten der betroffenen Personen gerechtfertigt sein.

Durch die Begrenzung des Kreises der zur Anbringung von Sperrvermerken Befugten in Satz 2 wird eine restriktive und fachgerechte Handhabung sichergestellt.

Zu § 58 Verfahren für die Ausübung der Rechte der betroffenen Person

Die Bestimmung orientiert sich an den Vorgaben des Artikels 12 der Richtlinie (EU) 2016/680.

Die Absätze 1 und 2 setzen die Vorgaben aus Artikel 12 Absatz 1 bis 3 der Richtlinie (EU) 2016/680 zu den Mitteilungen und den Modalitäten der Mitteilungen gegenüber Gefangenen und anderen betroffenen Personen um.

Absatz 3 macht von der Möglichkeit in Artikel 12 Absatz 4 der Richtlinie (EU) 2016/680 Gebrauch, bei einer offensichtlich unbegründeten oder exzessiven Antragstellung von einer Bescheidung des Antragstellers oder einer näheren Begründung abzusehen. Als Beispielfall wird die häufige sachgrundlose Wiederholung von Anträgen als möglicher Ablehnungsgrund für die Informationserteilung genannt.

Absatz 4 dient der Umsetzung von Artikel 12 Absatz 5 der Richtlinie (EU) 2016/680.
Abschnitt 9

Löschung, Einschränkung der Verarbeitung und Berichtigung

Zu § 59 Löschung

Absatz 1 Nummer 1 entspricht weitgehend § 43 Absatz 1 Nummer 1 JVollzDSG SH in der bisherigen Fassung. Absatz 1 Nummer 2 knüpft an § 43 Absatz 1 Nummer 3 JVollzDSG SH in der bisherigen Fassung an und Absatz 4 stimmt im Wesentlichen mit § 43 Absatz 3 JVollzDSG SH in der bisherigen Fassung überein.

Absatz 1 normiert den Grundsatz der verpflichtenden Löschung personenbezogener Daten, soweit nicht einer der dort aufgezählten Ausnahmefälle gegeben ist. Der Ausnahmefall, dass die personenbezogenen Daten zur Erreichung vollzuglicher Zwecke noch erforderlich sind, kann beispielsweise erfüllt sein, wenn Gefangene unter Bewährung oder unter Führungsaufsicht entlassen werden. Absatz 1 dient damit auch der Umsetzung von Artikel 4 Absatz 1 Buchstabe e) der Richtlinie (EU) 2016/680.

Absatz 2 Satz 1 verpflichtet die Justizvollzugsbehörden mindestens jährlich zu überprüfen, ob personenbezogene Daten zu löschen sind. Satz 2 regelt den Beginn der Jahresfrist. Die dort genannten sonstigen Fälle können personenbezogene Daten von anstaltsfremden Personen wie beispielsweise Besucherinnen oder Besuchern sein. Absatz 2 dient damit auch der Umsetzung von Artikel 5 der Richtlinie (EU) 2016/680 (vgl. auch Erwägungsgrund 26 am Ende). Unrechtmäßig verarbeitete Daten sind daher unverzüglich zu löschen.

In Absatz 3 Satz 1 werden jeweils für den Vollzug der Freiheitsstrafe, der Jugendstrafe, des Jugendarrestes und den anderen Freiheitsentziehungen individuelle Löschrfristen normiert. Die Norm trägt damit Artikel 6 der Richtlinie (EU) 2016/680 Rechnung, wonach so weit wie möglich zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen zu unterscheiden ist. Satz 2 bestimmt die Ausnahme zu Satz 1 für die Fälle, in denen eine besondere Vorschrift, beispielsweise die Justizaufbewahrungsverordnung eines Landes, eine längere Aufbewahrungsfrist für die Gefangenenpersonalakten vorsieht. In diesen Fällen kommt eine Einschränkung der Verarbeitung nach § 60 Absatz 1 Nummer 7 in Betracht.

Absatz 4 trägt ebenfalls der Unterscheidung nach Haftarten Rechnung, wie dies in Artikel 6 der Richtlinie (EU) 2016/680 vorgegeben ist, und folgt aus der gesetzlichen Unschuldsvermutung. Von dieser Regelung werden nicht nur die personenbezogenen Daten dieser Ge-

fangenen erfasst, sondern auch die ihrer Angehörigen und Besucherinnen und Besucher. Einer weiteren Verarbeitung dieser personenbezogenen Daten bedarf es nach der Entlassung der Gefangenen nicht mehr.

Zu § 60 **Einschränkung der Verarbeitung**

Absatz 1 Satz 1 trägt Artikel 16 Absatz 3 der Richtlinie (EU) 2016/680 Rechnung, wonach anstelle der Löschung personenbezogener Daten aus bestimmten Gründen eine Einschränkung ihrer Verarbeitung möglich ist.

Nummer 1 trägt den hochrangigen Interessen der Gefahrenverhütung, Gefahrenabwehr und Strafverfolgung Rechnung, die durch die Richtlinie (EU) 2016/680 als Verarbeitungszwecke anerkannt werden.

Nummer 2 stellt sicher, dass Interessen der Länder und betroffener Personen nach der Entlassung geltend gemacht und durchgesetzt werden können. Haben Gefangene z. B. im Vollzug gearbeitet, kann auch noch mehrere Jahre nach ihrer Entlassung der Nachweis über diese Beschäftigungen gegenüber anderen öffentlichen Stellen erforderlich werden. Ein Fall der Nummer 2 kann auch vorliegen, wenn die Geltendmachung von Amtshaftungs- oder Schadensersatzansprüchen in Betracht kommt. Ergeben sich aus der Gefangenenpersonalakte Anhaltspunkte für eine spätere Beweisbedürftigkeit einer Tatsache, ist anstelle der Löschung der personenbezogenen Daten eine Einschränkung ihrer Verarbeitung möglich.

Nummer 3 setzt den Gedanken aus Nummer 2 fort, nach dem die Löschung die Durchsetzung von Rechten der betroffenen Personen nicht beeinträchtigen oder vereiteln darf (vgl. Erwägungsgrund Nummer 47 der Richtlinie (EU) 2016/680).

Nummer 4 setzt die Ausnahmeregelung des Artikels 16 Absatz 3 Buchstabe b) der Richtlinie (EU) 2016/680 um, der weit zu verstehen ist und damit auch als Auffangtatbestand zu den Nummern 1 bis 3 dient.

Nummer 5 sieht bei abweichenden gesetzlichen Aufbewahrungsfristen eine entsprechende Ausnahme von der Löschung vor.

Absatz 1 Satz 2 verpflichtet zur Dokumentation der Gründe der Einschränkung der Verarbeitung personenbezogener Daten.

Aufgrund des Ausnahmecharakters der Einschränkung der Verarbeitung personenbezogener Daten ist die Verarbeitung dieser Daten nur unter den in Absatz 2 Satz 1 genannten Voraussetzungen möglich und zulässig. Ist die Verarbeitung dieser Daten zu Zwecken, zu denen ihre Löschung unterblieben ist, nicht mehr erforderlich, sind diese Daten unverzüglich zu löschen. Die Regelung orientiert sich an dem Verhältnismäßigkeitsgebot der Richtlinie (EU) 2016/680 und § 32 Absatz 2 Satz 3 des Bundeskriminalamtgesetzes.

Absatz 2 Satz 2 greift den Gedanken des Artikels 5 Satz 2 der Richtlinie (EU) 2016/680 auf, wonach durch verfahrensrechtliche Vorkehrungen sicherzustellen ist, dass Fristen eingehalten werden.

Absatz 3 sieht, neben der Einwilligung der betroffenen Personen in Nummer 1, in Nummer 2 den wichtigen Anwendungsfall für das Aufheben der Einschränkung der Verarbeitung personenbezogener Daten im Falle einer erneuten Inhaftierung vor. In diesem Fall können die Justizvollzugsbehörden auf die personenbezogenen Daten zum vormaligen Vollzugsverhalten oder die durchgeführten Behandlungsmaßnahmen wieder zugreifen. Die Justizvollzugsbehörden werden damit in die Lage versetzt, ohne Informationsverlust wieder an die vorherigen Vollzugsmaßnahmen der Gefangenen anzuknüpfen. Auch ist der Rückgriff auf die bereits bestehenden Daten für die Gefangenen regelmäßig weniger belastend als deren Neuerhebung. Wird die Einschränkung der Verarbeitung personenbezogener Daten wieder aufgehoben, richtet sich die Löschung dieser Daten erneut nach § 59.

Absatz 4 Satz 1 stellt klar, dass auch in den Fällen, in denen die Verarbeitung personenbezogener Daten eingeschränkt ist, die Höchstgrenzen für die Aufbewahrung nicht überschritten werden dürfen und legt in Satz 3 den Fristbeginn fest. Satz 2 sieht gleichwohl eine Ausnahme von den Höchstgrenzen für die Aufbewahrung vor, wenn ein Fall des Absatzes 1 vorliegt, also konkrete Anhaltspunkte dafür vorliegen, dass die personenbezogenen Daten zur Strafverfolgung oder zur Behebung einer Beweisnot erforderlich sind.

Zu § 61 **Berichtigung**

Die Regelung in Absatz 1 Satz 1 enthält eine Umsetzung des Grundsatzes aus Artikel 4 Absatz 1 Buchstabe a und d in Verbindung mit Artikel 7 Absatz 2 der Richtlinie (EU) 2016/680, wonach personenbezogene Daten zu berichtigen sind, wenn sie unrichtig, unvollständig oder nicht mehr aktuell sind.

Absatz 1 Satz 2 übernimmt den in Erwägungsgrund Nummer 47 der Richtlinie (EU) 2016/680 enthaltenen Gedanken. Zur Vorbeugung massenhafter und nicht erfolgsversprechender Anträge im Justizvollzug ist es geboten, klarzustellen, dass sich das Berichtigen auf die betroffene Person betreffende Tatsachen bezieht und nicht etwa auf den Inhalt von Zeugenaussagen, Beurteilungen oder Entscheidungen.

Absatz 1 Satz 3 setzt Artikel 4 Absatz 1 Buchstabe d, 1. Halbsatz, der Richtlinie (EU) 2016/680 um.

Absatz 1 Satz 4 übernimmt § 20 Absatz 1 Satz 2 des Bundesdatenschutzgesetzes in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 10 Absatz 2 des Gesetzes vom 31. Oktober 2017 (BGBl. I S. 3618) geändert worden ist und konkretisiert diesen.

Nach Absatz 1 Satz 5, der Artikel 16 Absatz 1 Satz 2 der Richtlinie (EU) 2016/680 umsetzt, kann die betroffene Person die Vervollständigung ihrer unvollständigen personenbezogenen Daten auch durch eine ergänzende Erklärung verlangen. Dies dürfte zur Wahrung der Aktenklarheit und Aktenwahrheit auch für sonstige Berichtigungen gelten.

Absatz 2 regelt einen weiteren Fall der Einschränkung der Verarbeitung. Artikel 16 Absatz 3 Buchstabe a der Richtlinie (EU) 2016/680 sieht in der (berechtigten) Berichtigung von unrichtigen Daten einen Unterfall der Löschung. In Anlehnung an § 58 Absatz 1 Satz 3 und 4 des Bundesdatenschutzgesetzes in der Fassung seiner Bekanntmachung vom 30. Juni 2017 soll der Fall der Löschung wegen Berichtigung unrichtiger Daten im Justizvollzugsdatenschutzgesetz systematisch als Fall der Berichtigung erfasst werden (vgl. auch Begründung zum Gesetzentwurf der Bundesregierung vom 24. Februar 2017, BT-Drucksache 18/11325, Seite 114). Die Aufhebung der Einschränkung der Verarbeitung nach Satz 2 führt daher entweder zur Berichtigung der Daten oder deren uneingeschränkter Verarbeitung.

Zu § 62 Rechte der betroffenen Person auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

Die Vorschrift dient der Umsetzung von Artikel 16 der Richtlinie (EU) 2016/680, soweit dieser Betroffenenrechte statuiert. Die Umsetzung der in diesem Artikel enthaltenen objektiven Pflichten der Justizvollzugsbehörden ist in §§ 59 bis 61 erfolgt.

Absatz 1 dient der Umsetzung von Artikel 16 Absatz 1 der Richtlinie (EU) 2016/680. Satz 1 setzt das in Artikel 16 Absatz 1 der Richtlinie (EU) 2016/680 gewährte Recht auf Berichtigung unrichtiger bzw. auf Vervollständigung unvollständiger Daten um. Satz 2 setzt Artikel 16 Absatz 3 Satz 2 um.

Absatz 2 setzt – in Verbindung mit § 59 – die Vorgaben des Artikels 16 Absatz 2 der Richtlinie (EU) 2016/680 um.

Absatz 3 dient der Umsetzung des Verfahrens von Artikel 16 Absatz 4 der Richtlinie (EU) 2016/680 und betrifft das zur Anwendung kommende Verfahren, wenn der Verantwortliche einem Antrag auf Berichtigung oder Löschung nicht oder nur eingeschränkt nachkommt.

Zu § 63 Mitteilungen

Die in dieser Vorschrift enthaltene Verpflichtung setzt Artikel 7 Absatz 3 und Artikel 16 Absatz 5 und 6 der Richtlinie (EU) 2016/680 um.

Absatz 1 Satz 1 sieht vor, die Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten auch anderen Stellen, an die diese Daten zuvor übermittelt wurden, zur Kenntnis zu geben, um so die Richtigkeit der Daten bei weiteren Übermittlungsvorgängen zu gewährleisten.

Die in Satz 2 geregelte Verpflichtung des Empfängers, die Berichtigung im eigenen Datenbestand vorzunehmen, folgt aus deren eigener Verantwortung, unrichtige Daten unverzüglich zu berichtigen.

Absatz 2 dient der Umsetzung von Artikel 5 Satz 2 der Richtlinie (EU) 2016/680.

Abschnitt 10

Anwendung weiterer Vorschriften

Zu § 64 Anwendung weiterer Vorschriften des allgemeinen Datenschutzrechts

Soweit für den Datenschutz im Justizvollzug in diesem Gesetz nicht etwas Abweichendes geregelt ist, findet gemäß Absatz 1 Satz 1 das allgemeine Datenschutzrecht Anwendung. Soweit Regelungen im Saarländischen Datenschutzgesetz vorhanden sind, wird konkret auf diese verwiesen.

Absatz 2 enthält rein deklaratorisch die Feststellung, dass für die Verarbeitung personenbezogener Daten durch die Vollzugsbehörden im sachlichen Anwendungsbereich der Verordnung (EU) 2016/679 deren Bestimmungen und die hierzu erlassenen Vorschriften gelten, soweit dieses Gesetz keine spezielleren Vorschriften enthält. Dies ist etwa der Fall, wenn die Datenverarbeitung von Anfang an nicht dem Anwendungsbereich des Artikels 1 Absatz 1 der Richtlinie (EU) 2016/680 unterfällt, etwa, weil sie der Verwaltung von Mitarbeiterdaten dient. Ferner kann das Recht der Verordnung (EU) 2016/679 zur Anwendung kommen, weil personenbezogene Daten, die für Zwecke des Justizvollzuges erhoben wurden, für andere Zwecke als diejenigen der Richtlinie (EU) 2016/680 weiterverarbeitet wer-

den. In diesen Fällen gilt die Verordnung (EU) 2016/679, wie Artikel 9 Absatz 2 der Richtlinie (EU) 2016/680 klarstellt, es sei denn, die Verarbeitung erfolgt im Rahmen einer Tätigkeit, die überhaupt nicht in den Anwendungsbereich des Unionsrechts fällt.

Zu Artikel 2

Zu Nummer 1 und 2:

In der Vollzugspraxis hat sich herausgestellt, dass es sinnvoll ist, den Gefangenen eine strukturierte Möglichkeit zum freiwilligen und pfändungsgeschützten Ansparen von Geld für die Entlassungsvorbereitung und die Zeit nach der Entlassung zu geben. Auch die einschlägigen internationalen Empfehlungen sehen eine Rücklagenbildung beziehungsweise Sparmöglichkeit vor. Die Resolution der Generalversammlung der Vereinten Nationen über die Mindestgrundsätze für die Behandlung der Gefangenen (Nelson-Mandela-Regeln, A/RES/70/175) sieht im Kontext „Arbeit“ (Regel 103 Ziff. 3) Folgendes vor: „Es soll auch vorgesehen werden, dass ein Teil dieses Verdienstes von der Vollzugsverwaltung als Rücklage behandelt wird, die Gefangenen bei ihrer Entlassung auszuhändigen ist.“ Eine ähnliche Regelung findet sich in den Europäischen Strafvollzugsgrundsätzen Ziff. 26.12: „Die Gefangenen sind anzuregen, einen Teil ihres Verdienstes zu sparen; diese Ersparnisse sind den Gefangenen bei der Entlassung auszuhändigen oder für andere erlaubte Zwecke zu verwenden.“ Anders als das frühere Überbrückungsgeld nach § 51 des Strafvollzugsgesetzes (StVollzG) stellt das Eingliederungsgeld keine zwangsweise Einbehaltung eines Teils der Gefangenenvergütung dar. Ein solches Ansparen ist nicht erforderlich, da die Gefangenen nach ihrer Entlassung aus dem Vollzug die regulären staatlichen Hilfen (Arbeitslosengeld I oder II, Sozialhilfe) in Anspruch nehmen können. Das freiwillig angesparte Eingliederungsgeld soll – im Unterschied zu dem früheren Überbrückungsgeld – nicht den notwendigen Lebensunterhalt nach der Entlassung sichern, sondern einen weitergehenden Bedarf decken und ist für Ausgaben zur Vorbereitung und Erleichterung der Eingliederung gedacht. Die Gefangenen dürfen nach Absatz 2 Satz 1 ein Eingliederungsgeld bilden und so einen Betrag für die Zeit nach der Entlassung ansparen, um den Start in die Freiheit zu erleichtern. Um ihre Eigenverantwortung und Selbstständigkeit zu fördern, verzichtet die Bestimmung darauf, die Gefangenen zum Ansparen des Geldes zu verpflichten. Die anzusparende Summe richtet sich nach den Erfordernissen des Einzelfalles, wird jedoch regelmäßig niedriger liegen als das früher nach § 51 StVollzG anzusparende Überbrückungsgeld. Die Höhe des Eingliederungsgeldes und mögliche Ansparraten sollen bei den Maßnahmen zur Eingliederung nach § 9 Abs. 1 Satz 1 Nr. 21 im Vollzugs- und Eingliederungsplan („Maßnahmen zur Vorbereitung von Entlassung, Eingliederung und Nachsorge“) festgelegt und im Rahmen der regelmäßigen Fortschreibung überprüft und gegebenenfalls angepasst werden. Dabei können beispielsweise die Dauer des Freiheitsentzugs, die voraussichtliche Entlassungssituation und die Einkommens- und Schuldensituation berücksichtigt werden. Das Eingliederungsgeld kann beispielsweise aus Einkünften aus einem freien Beschäftigungsverhältnis, aus einer Selbstbeschäftigung oder anderen regelmäßigen Einkünften sowie aus dem frei verfügbaren Eigengeld oder Hausgeld gebildet werden, soweit dadurch keine Bedürftigkeit im Sinne des § 57 entsteht. Das Eingliederungsgeld kann auch aus einem Teil der Vergütung, nämlich bis zu vier Siebteln, die nicht als Hausgeld verwendet werden, gebildet werden. Absatz 2 Satz 2 stellt sicher, dass die Gefangenen das Eingliederungsgeld, anders als das Überbrückungsgeld nach § 51 StVollzG, auch bereits vor der Entlassung verwenden können. Dies gilt jedoch nach Absatz 2 Satz 3 nur für konkrete Ausgaben zur Vorbereitung ihrer Eingliederung, beispielsweise die Zahlung einer Kautions bei Abschluss des Mietvertrages noch während der Haft, Anschaffungskosten für einen Personalausweis, Beschaffung von Kleidung, Kosten in Verbindung mit einer Arbeitsplatzsuche. Ebenfalls der Eingliederung dienen die Bezahlung einer Geldstrafe zur Vermeidung der Vollstreckung einer Ersatzfreiheitsstrafe und die Zahlung einer Entschädigung von den Gefangenen an die Opfer ihrer Straftaten. Insoweit kann auch den Belangen der Opfer Rechnung getragen werden. Nach Absatz 2 Satz 4 ist der Auszahlungsanspruch nicht übertragbar und damit gemäß § 851 der Zivilprozessordnung unpfändbar.

Zu Nummer 3:

Mit dieser Ergänzung wird eine konkrete Regelung zur Fixierung aufgenommen. Diese wird definiert als eine Art der Fesselung, durch die die Bewegungsfreiheit nicht nur beschränkt, sondern weitgehend aufgehoben wird, und die daher hohen Anordnungsvoraussetzungen unterliegt. Hierunter fällt bereits die Fesselung mit vier Gurten an ein sogenanntes Fesselbett. Gefordert wird eine gegenwärtige erhebliche Gefahr, sodass die Einwirkung des schädigenden Ereignisses entweder bereits begonnen haben oder unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorstehen und zudem eine Schädigung von besonderem Gewicht drohen muss, insbesondere ein besonders großer Umfang oder eine besondere Intensität des drohenden Schadens. Die Formulierung „soweit und solange“ und der Maßstab der „Unerlässlichkeit“ sichern eine strikte Verhältnismäßigkeitsprüfung derart, dass die Fixierung als letztes Mittel angewendet wird, wenn mildere Mittel nicht oder nicht mehr in Betracht kommen. Um eine möglichst schonende Durchführung der Fixierung zu gewährleisten, wird die Verwendung eines Gurtsystems vorgegeben.

Zu Nummer 4:

Für die Fälle der nicht nur kurzfristigen Fixierung wird ein Richtervorbehalt normiert und damit einfachgesetzlich die Vorgabe aus Artikel 104 Abs. 2 des Grundgesetzes umgesetzt. Sofern es sich bei der Fixierung nicht um eine kurzfristige Maßnahme handelt, die absehbar die Dauer einer halben Stunde unterschreitet, ist grundsätzlich eine vorherige richterliche Entscheidung zu beantragen. Bei Gefahr im Verzug ist eine vorläufige Anordnung und eine nachträgliche Einholung der richterlichen Entscheidung über die Fortdauer der Maßnahme zulässig; dies wird bei der Anordnung einer Fixierung zur Abwehr einer von den Gefangenen ausgehenden akuten Selbst- oder Fremdgefährdung regelmäßig der Fall sein. Bei der Anordnung einer nicht nur kurzfristigen Fixierung handelt es sich nicht mehr um eine Ausgestaltung der ursprünglichen Anordnung der Freiheitsentziehung, sondern vielmehr um eine davon losgelöste, eigenständige präventive Freiheitsentziehung. Somit handelt es sich nicht mehr um eine vollzugliche Maßnahme, der das Gericht zustimmt oder die vom Gericht genehmigt wird, sondern eine eigene Maßnahme des Gerichts. Das zuständige Gericht ist durch Bundesrecht festzulegen.

Zu Nummer 5:

Die Dokumentationspflichten bei einer Fixierung werden gesetzlich geregelt.

Zu Nummer 6:

Bei einer Fixierung wird unabhängig von deren Dauer eine Mitteilungspflicht vorgesehen.

Zu Nummer 7:

Für die Dauer der Fixierung ist eine besondere Betreuung vorgesehen, um die schädlichen Auswirkungen der Maßnahme zu minimieren. Zusätzlich ist die Anwesenheit einer oder eines geschulten Bediensteten festgelegt (z. B. zum medizinischen Personal gehörende oder sonst entsprechend geschulte Bedienstete), die oder der sich innerhalb des betreffenden Raums oder in der geöffneten Tür dieses Raumes mit Sichtkontakt zu der oder dem Gefangenen aufhält (sogenannte „Sitzwache“). Damit sollen ein menschlicher Kontakt ermöglicht sowie eventuelle Gefährdungen der fixierten Person rechtzeitig erkannt und diesen begegnet werden.

Zu Nummer 8:

Im Hinblick auf die Schwere des Grundrechtseingriffs wird die Anstalt verpflichtet, die Gefangenen nach Beendigung der Maßnahme auf die Möglichkeit hinzuweisen, die Zulässigkeit der durchgeführten Fixierung gerichtlich überprüfen zu lassen. Nur so kann gewährleistet werden, dass sich die Gefangenen bewusst sind, dass sie auch noch nach Erledigung der Maßnahme deren gerichtliche Überprüfung herbeiführen können. Das zuständige Gericht ist durch den Bund festzulegen.

Zu Artikel 3

Zu Nummer 1 und 2:

In der Vollzugspraxis hat sich herausgestellt, dass es sinnvoll ist, den Gefangenen eine strukturierte Möglichkeit zum freiwilligen und pfändungsgeschützten Ansparen von Geld für die Entlassungsvorbereitung und die Zeit nach der Entlassung zu geben. Auch die einschlägigen internationalen Empfehlungen sehen eine Rücklagenbildung beziehungsweise Sparmöglichkeit vor. Die Resolution der Generalversammlung der Vereinten Nationen über die Mindestgrundsätze für die Behandlung der Gefangenen (Nelson-Mandela-Regeln, A/RES/70/175) sieht im Kontext „Arbeit“ (Regel 103 Ziff. 3) Folgendes vor: „Es soll auch vorgesehen werden, dass ein Teil dieses Verdienstes von der Vollzugsverwaltung als Rücklage behandelt wird, die Gefangenen bei ihrer Entlassung auszuhändigen ist.“ Eine ähnliche Regelung findet sich in den Europäischen Strafvollzugsgrundsätzen Ziff. 26.12: „Die Gefangenen sind anzuregen, einen Teil ihres Verdienstes zu sparen; diese Ersparnisse sind den Gefangenen bei der Entlassung auszuhändigen oder für andere erlaubte Zwecke zu verwenden.“ Anders als das frühere Überbrückungsgeld nach § 51 des Strafvollzugsgesetzes (StVollzG) stellt das Eingliederungsgeld keine zwangsweise Einbehaltung eines Teils der Gefangenenvergütung dar. Ein solches Ansparen ist nicht erforderlich, da die Gefangenen nach ihrer Entlassung aus dem Vollzug die regulären staatlichen Hilfen (Arbeitslosengeld I oder II, Sozialhilfe) in Anspruch nehmen können. Das freiwillig angesparte Eingliederungsgeld soll – im Unterschied zu dem früheren Überbrückungsgeld – nicht den notwendigen Lebensunterhalt nach der Entlassung sichern, sondern einen weitergehenden Bedarf decken und ist für Ausgaben zur Vorbereitung und Erleichterung der Eingliederung gedacht. Die Gefangenen dürfen nach Absatz 4 Satz 1 ein Eingliederungsgeld bilden und so einen Betrag für die Zeit nach der Entlassung ansparen, um den Start in die Freiheit zu erleichtern. Um ihre Eigenverantwortung und Selbstständigkeit zu fördern, verzichtet die Bestimmung darauf, die Gefangenen zum Ansparen des Geldes zu verpflichten. Die anzusparende Summe richtet sich nach den Erfordernissen des Einzelfalles, wird jedoch regelmäßig niedriger liegen als das früher nach § 51 StVollzG anzusparende Überbrückungsgeld. Die Höhe des Eingliederungsgeldes und mögliche Ansparraten sollen bei den Maßnahmen zur Eingliederung nach § 11 Abs. 3 Satz 1 Nr. 12 im Vollzugsplan („Maßnahmen zur Vorbereitung von Entlassung, Wiedereingliederung und Nachsorge“) festgelegt und im Rahmen der regelmäßigen Fortschreibung überprüft und gegebenenfalls angepasst werden. Dabei können beispielsweise die Dauer des Freiheitsentzugs, die voraussichtliche Entlassungssituation und die Einkommens- und Schuldensituation berücksichtigt werden. Das Eingliederungsgeld kann beispielsweise aus Einkünften aus einem freien Beschäftigungsverhältnis, aus einer Selbstbeschäftigung oder anderen regelmäßigen Einkünften sowie aus dem frei verfügbaren Eigengeld oder Hausgeld gebildet werden, soweit dadurch keine Bedürftigkeit im Sinne des § 59 entsteht. Das Eingliederungsgeld kann auch aus einem Teil der Vergütung, nämlich bis zu vier Siebteln, die nicht als Hausgeld verwendet werden, gebildet werden. Absatz 4 Satz 2 stellt sicher, dass die Gefangenen das Eingliederungsgeld, anders als das Überbrückungsgeld nach § 51 StVollzG, auch bereits vor der Entlassung verwenden können. Dies gilt jedoch nach Absatz 4 Satz 3 nur für konkrete Ausgaben zur Vorbereitung ihrer Eingliederung, beispielsweise die Zahlung einer Kaution bei Abschluss des Mietvertrages noch während der Haft, Anschaffungskosten für einen Personalausweis, Beschaffung von Kleidung, Kosten in

Verbindung mit einer Arbeitsplatzsuche. Ebenfalls der Eingliederung dienen die Bezahlung einer Geldstrafe zur Vermeidung der Vollstreckung einer Ersatzfreiheitsstrafe und die Zahlung einer Entschädigung von den Gefangenen an die Opfer ihrer Straftaten. Insoweit kann auch den Belangen der Opfer Rechnung getragen werden.

Nach Absatz 4 Satz 4 ist der Auszahlungsanspruch nicht übertragbar und damit gemäß § 851 der Zivilprozessordnung unpfändbar.

Zu Nummer 3:

Mit dieser Ergänzung wird eine konkrete Regelung zur Fixierung aufgenommen. Diese wird definiert als eine Art der Fesselung, durch die die Bewegungsfreiheit nicht nur beschränkt, sondern weitgehend aufgehoben wird, und die daher hohen Anordnungsvoraussetzungen unterliegt. Hierunter fällt bereits die Fesselung mit vier Gurten an ein sogenanntes Fesselbett. Gefordert wird eine gegenwärtige erhebliche Gefahr, sodass die Einwirkung des schädigenden Ereignisses entweder bereits begonnen haben oder unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorstehen und zudem eine Schädigung von besonderem Gewicht drohen muss, insbesondere ein besonders großer Umfang oder eine besondere Intensität des drohenden Schadens. Die Formulierung „soweit und solange“ und der Maßstab der „Unerlässlichkeit“ sichern eine strikte Verhältnismäßigkeitsprüfung derart, dass die Fixierung als letztes Mittel angewendet wird, wenn mildere Mittel nicht oder nicht mehr in Betracht kommen. Um eine möglichst schonende Durchführung der Fixierung zu gewährleisten, wird die Verwendung eines Gurtsystems vorgegeben.

Zu Nummer 4:

Für die Dauer der Fixierung ist eine besondere Betreuung vorgesehen, um die schädlichen Auswirkungen der Maßnahme zu minimieren. Zusätzlich ist die Anwesenheit einer oder eines geschulten Bediensteten festgelegt (z. B. zum medizinischen Personal gehörende oder sonst entsprechend geschulte Bedienstete), die oder der sich innerhalb des betreffenden Raums oder in der geöffneten Tür dieses Raumes mit Sichtkontakt zu der oder dem Gefangenen aufhält (sogenannte „Sitzwache“). Damit sollen ein menschlicher Kontakt ermöglicht sowie eventuelle Gefährdungen der fixierten Person rechtzeitig erkannt und diesen begegnet werden.

Zu Nummer 5:

Für die Fälle der nicht nur kurzfristigen Fixierung wird ein Richtervorbehalt normiert und damit einfachgesetzlich die Vorgabe aus Artikel 104 Abs. 2 des Grundgesetzes umgesetzt. Sofern es sich bei der Fixierung nicht um eine kurzfristige Maßnahme handelt, die absehbar die Dauer einer halben Stunde unterschreitet, ist grundsätzlich eine vorherige richterliche Entscheidung zu beantragen. Bei Gefahr im Verzug ist eine vorläufige Anordnung und eine nachträgliche Einholung der richterlichen Entscheidung über die Fortdauer der Maßnahme zulässig; dies wird bei der Anordnung einer Fixierung zur Abwehr einer von den Gefangenen ausgehenden akuten Selbst- oder Fremdgefährdung regelmäßig der Fall sein. Bei der Anordnung einer nicht nur kurzfristigen Fixierung handelt es sich nicht mehr um eine Ausgestaltung der ursprünglichen Anordnung der Freiheitsentziehung, sondern vielmehr um eine davon losgelöste, eigenständige präventive Freiheitsentziehung. Somit handelt es sich nicht mehr um eine vollzugliche Maßnahme, der das Gericht zustimmt oder die vom Gericht genehmigt wird, sondern eine eigene Maßnahme des Gerichts. Das zuständige Gericht ist durch Bundesrecht festzulegen.

Zu Nummer 6:

Die Dokumentationspflichten bei einer Fixierung werden gesetzlich geregelt.

Zu Nummer 7:

Bei einer Fixierung wird unabhängig von deren Dauer eine Mitteilungspflicht vorgesehen.

Zu Nummer 8:

Im Hinblick auf die Schwere des Grundrechtseingriffs wird die Anstalt verpflichtet, die Gefangenen nach Beendigung der Maßnahme auf die Möglichkeit hinzuweisen, die Zulässigkeit der durchgeführten Fixierung gerichtlich überprüfen zu lassen. Nur so kann gewährleistet werden, dass sich die Gefangenen bewusst sind, dass sie auch noch nach Erledigung der Maßnahme deren gerichtliche Überprüfung herbeiführen können. Das zuständige Gericht ist durch den Bund festzulegen.

Zu Artikel 4

Zu Nummer 1:

Mit dieser Ergänzung wird eine konkrete Regelung zur Fixierung aufgenommen. Diese wird definiert als eine Art der Fesselung, durch die die Bewegungsfreiheit nicht nur beschränkt, sondern weitgehend aufgehoben wird, und die daher hohen Anordnungsvoraussetzungen unterliegt. Hierunter fällt bereits die Fesselung mit vier Gurten an ein sogenanntes Fesselbett. Gefordert wird eine gegenwärtige erhebliche Gefahr, sodass die Einwirkung des schädigenden Ereignisses entweder bereits begonnen haben oder unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorstehen und zudem eine Schädigung von besonderem Gewicht drohen muss, insbesondere ein besonders großer Umfang oder eine besondere Intensität des drohenden Schadens. Die Formulierung „soweit und solange“ und der Maßstab der „Unerlässlichkeit“ sichern eine strikte Verhältnismäßigkeitsprüfung derart, dass die Fixierung als letztes Mittel angewendet wird, wenn mildere Mittel nicht oder nicht mehr in Betracht kommen. Um eine möglichst schonende Durchführung der Fixierung zu gewährleisten, wird die Verwendung eines Gurtsystems vorgegeben.

Zu Nummer 2:

Für die Dauer der Fixierung ist eine besondere Betreuung vorgesehen, um die schädlichen Auswirkungen der Maßnahme zu minimieren. Zusätzlich ist die Anwesenheit einer oder eines geschulten Bediensteten festgelegt (z. B. zum medizinischen Personal gehörende oder sonst entsprechend geschulte Bedienstete), die oder der sich innerhalb des betreffenden Raums oder in der geöffneten Tür dieses Raumes mit Sichtkontakt zu der oder dem Untersuchungsgefangenen aufhält (sogenannte „Sitzwache“). Damit sollen ein menschlicher Kontakt ermöglicht sowie eventuelle Gefährdungen der fixierten Person rechtzeitig erkannt und diesen begegnet werden.

Zu Nummer 3:

Für die Fälle der nicht nur kurzfristigen Fixierung wird ein Richtervorbehalt normiert und damit einfachgesetzlich die Vorgabe aus Artikel 104 Abs. 2 des Grundgesetzes umgesetzt. Sofern es sich bei der Fixierung nicht um eine kurzfristige Maßnahme handelt, die absehbar die Dauer einer halben Stunde unterschreitet, ist grundsätzlich eine vorherige richterliche

Entscheidung zu beantragen. Bei Gefahr im Verzug ist eine vorläufige Anordnung und eine nachträgliche Einholung der richterlichen Entscheidung über die Fortdauer der Maßnahme zulässig; dies wird bei der Anordnung einer Fixierung zur Abwehr einer von den Untersuchungsgefangenen ausgehenden akuten Selbst- oder Fremdgefährdung regelmäßig der Fall sein. Bei der Anordnung einer nicht nur kurzfristigen Fixierung handelt es sich nicht mehr um eine Ausgestaltung der ursprünglichen Anordnung der Freiheitsentziehung, sondern vielmehr um eine davon losgelöste, eigenständige präventive Freiheitsentziehung. Somit handelt es sich nicht mehr um eine vollzugliche Maßnahme, der das Gericht zustimmt oder die vom Gericht genehmigt wird, sondern eine eigene Maßnahme des Gerichts. Das zuständige Gericht ist durch den Bund festzulegen.

Zu Nummer 4:

Die Dokumentationspflichten bei einer Fixierung werden gesetzlich geregelt.

Zu Nummer 5:

Bei einer Fixierung wird unabhängig von deren Dauer eine Mitteilungspflicht vorgesehen. Der Richtervorbehalt bleibt hiervon unberührt.

Zu Nummer 6:

Im Hinblick auf die Schwere des Grundrechtseingriffs wird die Anstalt verpflichtet, die Untersuchungsgefangenen nach Beendigung der Maßnahme auf die Möglichkeit hinzuweisen, die Zulässigkeit der durchgeführten Fixierung gerichtlich überprüfen zu lassen. Nur so kann gewährleistet werden, dass sich die Untersuchungsgefangenen bewusst sind, dass sie auch noch nach Erledigung der Maßnahme deren gerichtliche Überprüfung herbeiführen können. Das zuständige Gericht ist durch den Bund festzulegen.

Zu Artikel 5

Zu Nummer 1:

Zu § 26 - Vorrang des Bundesrechts; Anwendung des Saarländischen Justizvollzugsdatenschutzgesetzes und des Saarländischen Datenschutzgesetzes

Die Bestimmung entspricht im Wesentlichen § 26 des Gesetzes zur ambulanten Resozialisierung und Opferhilfe. Da die folgenden Vorschriften des Gesetzes im Bereich des Datenschutzes nicht abschließend sind, stellt Satz 3 klar, dass ergänzend die Regelungen des Saarländischen Justizvollzugsdatenschutzgesetzes und des Saarländischen Datenschutzgesetzes Anwendung finden.

Zu Nummer 2:

Zu § 27 - Zulässigkeit der Datenverarbeitung; Einwilligung

Absatz 1 bestimmt grundlegend die Zulässigkeit der Datenverarbeitung durch das Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe und das Ministerium der Justiz als für die Dienst- und Fachaufsicht zuständige Behörde und setzt damit den aus dem Rechtsstaatsgebot und der Rechtsprechung des Bundesverfassungsgerichts folgenden

Grundsatz des Vorbehalts des Gesetzes um. Absatz 1 bestimmt als bereichsspezifische Sonderregelung, dass diese Behörden personenbezogene Daten u.a. nur dann verarbeiten dürfen, wenn dies für den Anwendungsbereich dieses Gesetzes in einer anderen Rechtsvorschrift ausdrücklich erlaubt oder angeordnet ist. Zugleich wird Artikel 8 Absatz 1 der Richtlinie (EU) 2016/680 umgesetzt, wonach eine Datenverarbeitung auf eine klare und präzise Rechtsgrundlage gestützt sein muss (vgl. Erwägungsgrund 33 zur Richtlinie (EU) 2016/680).

Aus Erwägungsgrund 35 zur Richtlinie (EU) 2016/680 lässt sich entnehmen, dass eine Einwilligung auch im Geltungsbereich dieser Richtlinie die Grundlage einer Datenverarbeitung sein kann, wenn sichergestellt ist, dass eine echte Wahlfreiheit der betroffenen Person besteht. Der Erwägungsgrund gibt zwar zu erkennen, dass eine solche Wahlfreiheit in Konstellationen zweifelhaft sein kann, in denen eine Behörde die betroffene Person anweisen oder auffordern kann, einer rechtlichen Verpflichtung nachzukommen. Zugleich werden aber auch Konstellationen – auch explizit für den Bereich der Strafvollstreckung, wozu begrifflich auch die Bewährungshilfe, Führungsaufsicht und die Nachsorge gehören – aufgeführt, in denen eine betroffene Person in eine Datenverarbeitung einwilligen kann. Auch wenn in der Richtlinie (EU) 2016/680 außerhalb der Erwägungsgründe eine Einwilligung - anders als in der Verordnung (EU) 2016/679 - nicht mehr erwähnt wird, ist sie daher als Rechtsgrundlage einer Datenverarbeitung möglich. Dies entspricht auch der Wertung des Bundesgesetzgebers, der in § 46 Nummer 17 und in § 51 des Bundesdatenschutzgesetzes gesetzliche Regelungen für die Einwilligung geschaffen hat.

Absatz 2 entspricht inhaltlich § 51 des Bundesdatenschutzgesetzes. Hier werden Artikel 7 und 10 der Verordnung (EU) 2016/679 mit redaktionellen Anpassungen wiedergegeben.

Zu Nummer 3:

Zu § 28 - Erhebung personenbezogener Daten

Die Bestimmung enthält die grundlegende Regelung für die Zulässigkeit der Erhebung personenbezogener Daten durch die genannten Behörden.

Nach Absatz 1 Satz 1 ist eine Datenerhebung nur zulässig, soweit sie für die Aufgabenerfüllung erforderlich ist.

Absatz 1 Satz 2 trägt der besonderen Schutzbedürftigkeit besonderer Kategorien personenbezogener Daten, die in § 2 Nummer 14 – Artikel 10 der Richtlinie (EU) 2016/680 folgend – definiert sind, Rechnung. Die Daten sind besonders sensibel. Die mit diesen Daten verbundene gesteigerte Persönlichkeitsrelevanz, wie sie auch das Bundesverfassungsgericht betont (BVerfGE 115, 320,348), und die damit verbundene gesteigerte Intensität von Eingriffen in das Persönlichkeitsrecht der betroffenen Personen lassen eine Verarbeitung dieser Daten nur unter der engen Voraussetzung zu, dass diese zur Aufgabenerfüllung unbedingt erforderlich ist. „Unbedingt erforderlich“ ist eine Datenübermittlung, wenn sie im konkreten Einzelfall für die jeweilige Zweckerreichung unerlässlich ist.

Absatz 2 regelt in Satz 1 die Erhebung von personenbezogenen Daten bei den betroffenen Personen. Er enthält den Grundsatz der Direkterhebung, wonach eine Erhebung personenbezogener Daten grundsätzlich unter der Mitwirkung der betroffenen Person zu erfolgen hat. Dies ist unmittelbar Ausfluss des Grundrechts auf informationelle Selbstbestimmung, da die betroffene Person wissen können soll, wer sich für ihre Daten interessiert.

Absatz 2 Satz 2 regelt die Voraussetzungen, unter denen auch ohne Kenntnis und ohne Mitwirkung der betroffenen Person, ausnahmsweise eine Erhebung personenbezogener Daten zulässig ist. Diese ist nur zulässig, wenn keine Anhaltspunkte vorliegen, dass überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen. Insofern hat eine Abwägung stattzufinden.

Die Datenerhebung bei Dritten greift stärker in die Rechte der Probandinnen und Probanden ein, als dies bei einer Erhebung bei ihnen selbst der Fall wäre. Aus diesem Grunde bindet Absatz 3 diese Art der Erhebung an strenge Voraussetzungen. Der in Absatz 3 genannte Katalog ist abschließend.

Absatz 4 erweitert die Erhebungsbefugnis um die Möglichkeit, personenbezogene Daten von Probandinnen und Probanden ohne ihre Kenntnis bei ihren gesetzlichen Vertreterinnen und Vertretern zu erheben, wenn sie nicht die für die Einwilligung notwendige Einsichtsfähigkeit besitzen. Abhängig von der Kategorie von Daten müssen im Hinblick auf die besondere Kategorie personenbezogener Daten kumulativ noch die Voraussetzungen nach Absatz 1 vorliegen. Zudem wird durch den Verweis auf Absatz 2 Satz 2 klargestellt, dass – in Anbetracht dessen, dass es sich um eine Erhebung ohne Kenntnis der betroffenen Person handelt – im Einzelfall eine Abwägungsentscheidung mit den schutzwürdigen Interessen der Probandinnen und Probanden stattzufinden hat.

Aufgrund der Tatsache, dass die Datenerhebung bei Dritten einen stärkeren Eingriff in die Rechtsposition der Probandinnen und Probanden bedeutet, werden nach Absatz 5 nichtöffentliche Stellen darauf hingewiesen, aufgrund welcher Rechtsvorschrift eine Auskunftspflicht besteht, andernfalls wird auf die Freiwilligkeit der Auskunft verwiesen. Nur so ist sichergestellt, dass die nichtöffentlichen Stellen in eigener Verantwortung entscheiden können, ob und in welchem Umfang sie eine Auskunft erteilen wollen oder nicht erteilen.

Die Bestimmung setzt Artikel 6 der Richtlinie (EU) 2016/680 um, der eine Differenzierung nach unterschiedlichen Kategorien betroffener Personen vorgibt.

Zu Nummer 4:

Zu § 29 - Verarbeitung personenbezogener Daten

Absatz 1 enthält den Grundsatz der Zweckbindung für die Speicherung und Nutzung von personenbezogenen Daten nach deren zulässigen Erhebung und dient zudem der Umsetzung des in Artikel 8 Absatz 1 der Richtlinie (EU) 2016/680 normierten Erforderlichkeitsprinzips. Danach ist eine Verarbeitung personenbezogener Daten nur zulässig, soweit dies zur Aufgabenerfüllung der zuständigen Behörde erforderlich ist.

Absatz 2 regelt mit abschließendem Katalog die Voraussetzungen dafür, dass die Behörden die zulässig erhobenen personenbezogenen Daten auch zu einem anderen Zweck speichern und nutzen dürfen, als zu demjenigen, zu dem sie erhoben worden sind.

Absatz 3 regelt die Speicherung und Nutzung von besonderen Kategorien personenbezogener Daten. Die Bestimmung dient damit der Umsetzung von Artikel 10 der Richtlinie (EU) 2016/680. Dieser sieht vor, dass die Verarbeitung besonders schutzwürdiger Daten nur dann erlaubt ist, wenn dies unbedingt erforderlich ist und geeignete Garantien für die Rechte und Freiheiten der betroffenen Person vorgesehen sind. Satz 2 sieht eine Ausnahme zugunsten besonderer Kategorien personenbezogener Daten vor, die einem Amts- oder Berufsgeheimnis unterfallen (insb. Gesundheitsdaten) und in einer, eine Verschwiegenheitspflicht begründenden amtlichen oder beruflichen Funktion überlassen worden sind.

Absatz 4 trägt den Erfordernissen der Praxis Rechnung. Die Regelung ist erforderlich, da sich insbesondere bei einer aktenmäßigen Speicherung personenbezogener Daten nicht immer mit verhältnismäßigem Aufwand sicherstellen lässt, dass eine Trennung nach erforderlichen und nicht erforderlichen Daten möglich ist. Nur bei unvertretbarem Aufwand für die Trennung dürfen ausnahmsweise auch nicht für den konkreten Zweck erforderliche Daten gespeichert werden. Als Schranke ist jedoch die zusätzliche Voraussetzung zu beachten, dass das berechtigte Interesse von betroffenen Personen oder Dritten an deren Geheimhaltung offensichtlich überwiegt.

Werden nach Absatz 5 Satz 1 personenbezogene Daten ausschließlich zur Datenschutzkontrolle, zur Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert oder genutzt, greift für diese Daten eine besondere Zweckbindung. Eine zweckändernde Nutzung ist daher nur zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erlaubt. Satz 2 bezieht sich auf die weitere Verarbeitung von Protokolldaten in automatisierten Datenverarbeitungssystemen.

Zu Nummer 5:

Zu § 31 - Zweckbindung

Bei der Bestimmung handelt es sich um eine Schutzvorschrift, die den zweckgebundenen Umgang mit den personenbezogenen Daten der betroffenen Personen, auch nach der Übermittlung, gewährleistet. Dies wirkt einem etwaigen Missbrauch entgegen.

Für andere Zwecke dürfen die Empfänger die Daten nur speichern, nutzen und übermitteln, soweit sie ihnen auch für diese Zwecke hätten überlassen werden dürfen. Für die Zweckbindung bei Weiterverarbeitung von Daten durch nichtöffentliche Stellen sieht Satz 2 darüber hinaus als zusätzliche Beschränkung vor, dass das Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe der Weiterverarbeitung zugestimmt hat.

Satz 3 dient der Umsetzung von Artikel 9 Absatz 3 der Richtlinie (EU) 2016/680, wonach vorzusehen ist, dass immer dann, wenn für die Verarbeitung besondere Bedingungen gelten, die übermittelnde zuständige Behörde die Empfänger der Daten darauf hinweist, dass die Bedingungen gelten und einzuhalten sind.

Zu Nummer 6:

Zu § 32 - Schutzvorkehrungen

Die Vorschrift dient der Umsetzung von Artikel 4 Absatz 1 Buchstabe f der Richtlinie (EU) 2016/680, wonach personenbezogene Daten in einer Weise verarbeitet werden müssen, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Gleichzeitig setzt die Bestimmung auch die Vorgaben aus Artikel 19 der Richtlinie (EU) 2016/680 um, wonach der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umzusetzen hat.

Absatz 1 regelt den sicheren Umgang mit personenbezogenen Daten in Akten und Dateisystemen, um so einen unbefugten Zugang und Gebrauch auszuschließen. Für Art und Umfang der hierzu erforderlichen technischen und organisatorischen Maßnahmen verweist Absatz 1 Satz 2 auf die Vorschriften zum Verzeichnis von Verarbeitungstätigkeiten, zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen sowie zur Durchführung einer Datenschutz-Folgenabschätzung bei hohem Risiko für die Rechtsgüter von betroffenen Personen.

Absatz 2 betrifft den Umgang Bediensteter mit und deren Zugang zu personenbezogenen Daten. Jeder Bedienstete darf nur auf solche personenbezogenen Daten zugreifen, die er für die Erfüllung der ihm übertragenen Aufgaben braucht. Diese aus dem Erforderlichkeitsprinzip resultierenden Anforderungen müssen durch technische und organisatorische Schutzmaßnahmen gewährleistet werden, beispielsweise bei Anlage und Aufbewahrung von Akten.

Zu Nummer 7:

Zu § 32a - Verzeichnis von Verarbeitungstätigkeiten

Die Vorschrift, die die bisherigen datenschutzrechtlichen Vorschriften der Länder zur Führung von Verfahrensverzeichnissen ablöst, entspricht § 70 des Bundesdatenschutzgesetzes und dient der Umsetzung von Artikel 24 der Richtlinie (EU) 2016/680. Die Bestimmung verpflichtet das Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe zur Führung eines Verzeichnisses über bei ihm durchgeführte Kategorien von Datenverarbeitungstätigkeiten. Dieses Verzeichnis dient vor allem der oder dem Landesdatenschutzbeauftragten dazu, einen Überblick über die beim Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe durchgeführten Datenverarbeitungen zu erhalten.

In Absatz 1 werden die in das Verzeichnis aufzunehmenden Angaben benannt. Der Begriff „Kategorien“ von Verarbeitungstätigkeiten stellt hierbei klar, dass sich das Verzeichnis nicht auf einzelne Datenverarbeitungsvorgänge, sondern auf sinnvoll abgrenzbare und kategorisierbare Teile der beim Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe durchgeführten Datenverarbeitungen bezieht. Die Reihenfolge der Nummern nach Absatz 1 entspricht derjenigen des Artikels 30 Verordnung (EU) 2016/679. Dies dient der Praktikabilität bei der Erstellung der Verarbeitungsverzeichnisse durch die Behörden, die die Verzeichnisse auch im Geltungsbereich der Verordnung (EU) 2016/679 im Rahmen ihrer Verwaltungstätigkeit (Personal- und Wirtschaftsbereich) zu erstellen haben.

Absatz 2 trifft in Satz 1 Aussagen zur Form des Verzeichnisses. Nach Satz 2 wird das Verzeichnis der oder dem Landesdatenschutzbeauftragten auf Anforderung zur Verfügung gestellt.

Zu § 32b - Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Die Bestimmung dient der Umsetzung der Artikel 19, 20 und 29 der Richtlinie (EU) 2016/680, die Vorgaben zu den Pflichten des Verantwortlichen, zum Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen sowie zur Sicherheit der Verarbeitung treffen.

Absatz 1 entspricht der Regelung in § 64 Absatz 1 des Bundesdatenschutzgesetzes. Dem Absatz liegt der Gedanke zugrunde, dass die Erforderlichkeit der Maßnahmen daran zu bemessen ist, ob ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht.

Absatz 2 übernimmt den Anforderungskatalog, der dem Standard-Datenschutzmodell entspricht. Er setzt damit zugleich die Artikel 19, 20 und 29 Absatz 1 der Richtlinie (EU) 2016/680 um, die von den Behörden verlangen, zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst angemessene Vorkehrungen zu treffen, die geeignet sind, die Datenschutzgrundsätze wie etwa die Datensparsamkeit wirksam umzusetzen, und die sicherstellen, dass die gesetzlichen Anforderungen eingehalten und die Rechte der betroffenen Personen geschützt werden. Die zu treffenden Vorkehrungen haben den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen zu berücksichtigen. Die Gewährleistungsziele des Standard-Datenschutzmodells, denen der Anforderungskatalog entnommen ist, decken sich mit den Anforderungen der Richtlinie (EU) 2016/680 (vgl. Schlehahn, DuD 2018, 32, 36). Neben den Artikeln 19, 20 und 29 Absatz 1 lassen sich außerdem die Artikel 4, 5, 8 bis 14, 16 bis 18, 22, 24, 25, 28, 30 und 31 der Richtlinie (EU) 2016/680 diesen Zielen zuordnen. Die Umset-

zung der in Absatz 2 genannten Maßnahmen kann die Behörde in eigener Verantwortung festlegen.

Absatz 3 dient der Umsetzung von Artikel 29 Absatz 2 der Richtlinie (EU) 2016/680. Satz 1 benennt die Ziele, die im Hinblick auf automatisierte Verarbeitungen durch die Etablierung geeigneter technisch-organisatorischer Maßnahmen verfolgt und erreicht werden sollen. Gemäß Satz 2 können die Zwecke der Datenträgerkontrolle, Speicherkontrolle, Benutzerkontrolle und Zugriffskontrolle insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

Absatz 4 setzt Artikel 20 Absatz 2 der Richtlinie (EU) 2016/680 um. Es ist sicherzustellen, dass durch Voreinstellungen jeweils nur die personenbezogenen Daten verarbeitet werden, deren Verarbeitung nach dem jeweiligen bestimmten Verarbeitungszweck erforderlich ist.

Absatz 5 entspricht im Wesentlichen der Rechtslage im bisherigen Landesdatenschutzgesetz. Die Bestimmung verlangt die Erarbeitung eines Sicherheitskonzepts und die Einschätzung von Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für das Recht auf informationelle Selbstbestimmung. Im Gegensatz zur bisherigen Rechtslage sieht die Regelung in Einklang mit der neuen Terminologie und den Vorgaben aus Artikel 27 der Richtlinie (EU) 2016/680 nicht mehr eine Vorabkontrolle durch den Verantwortlichen (wie noch Artikel 20 der Richtlinie 95/46/EG) vor. Eine Vorabkontrolle sehen die Richtlinie (EU) 2016/680 und dementsprechend auch der Entwurf nur noch bei einem hohen Risiko für das Recht auf informationelle Selbstbestimmung im Rahmen der nach § 32c durchzuführenden Datenschutz-Folgenabschätzung vor. Gleichwohl soll die bewährte Praxis einer Einschätzung von Risiken für das Recht auf informationelle Selbstbestimmung anhand eines Sicherheitskonzepts auch für Verarbeitungsvorgänge unterhalb dieser Schwelle beibehalten werden. Nach Absatz 5 sollen die Folgen von Datenverarbeitungssystemen daher unabhängig von den Voraussetzungen einer Datenschutz-Folgenabschätzung bereits im Rahmen eines Sicherheitskonzepts eingeschätzt werden. Dadurch werden zugleich die Vorgaben aus Artikel 20 Absatz 1 und Artikel 29 Absatz 1 der Richtlinie (EU) 2016/680 umgesetzt, wonach der für die Datenverarbeitung Verantwortliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken zu bewerten und auf dieser Grundlage technische und organisatorische Maßnahmen zu ergreifen hat. § 32c, der die Durchführung einer umfassenden Datenschutz-Folgenabschätzung bei hohem Risiko für die Rechtsgüter betroffener Personen regelt, bleibt unberührt.

Zu § 32c - Datenschutz-Folgenabschätzung bei hohem Risiko, Konsultationspflicht

Die Vorschrift entspricht im Wesentlichen der Regelung in § 67 des Bundesdatenschutzgesetzes.

Absatz 1 dient der Umsetzung von Artikel 27 der Richtlinie (EU) 2016/680. Kriterien für die Entscheidung, ob die vorgesehene Verarbeitung qualitativ erhöhte Gefahren für die Rechtsgüter der betroffenen Personen zur Folge hat, können beispielsweise die Art der zur Datenerhebung eingesetzten Mittel oder der Kreis der zugriffsberechtigten Personen, mithin die Eingriffsintensität der mit der Verarbeitung verbundenen Maßnahmen im Sinne einer Gesamtwürdigung sein. Dabei ist zu beachten, dass das Erfordernis der Durchführung einer Datenschutz-Folgenabschätzung nur für neue nach Inkrafttreten dieses Gesetzes eingesetzte Verarbeitungssysteme oder wesentliche Veränderungen an bestehenden Systemen gilt.

Absatz 2 nimmt in Satz 1 Artikel 35 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 und in Satz 2 Artikel 35 Absatz 2 der Verordnung (EU) 2016/679 auf, die eine sinnvolle Ergänzung der Vorgaben der Richtlinie (EU) 2016/680 darstellen.

Absatz 3 legt den Inhalt der Datenschutz-Folgenabschätzung fest und konkretisiert die in Artikel 27 Absatz 2 der Richtlinie (EU) 2016/680 enthaltenen allgemeinen Angaben durch Übernahme der in Artikel 35 Absatz 7 der Verordnung (EU) 2016/679 enthaltenen Vorgaben.

Absatz 4 entspricht § 69 Absatz 1 Bundesdatenschutzgesetz.

Absatz 5 entspricht § 69 Absatz 2 Bundesdatenschutzgesetz.

Absatz 6 entspricht § 69 Absatz 3 Bundesdatenschutzgesetz.

Absatz 7 entspricht § 69 Absatz 4 Bundesdatenschutzgesetz.

Zu § 32d - Protokollierung

Die Vorschrift dient der Umsetzung von Artikel 25 der Richtlinie (EU) 2016/680 und ermöglicht eine Kontrolle der Rechtmäßigkeit der Datenverarbeitungsvorgänge.

Absatz 1 regelt in Umsetzung von Artikel 25 Absatz 1 Satz 1 der Richtlinie (EU) 2016/680 eine Pflicht zur Protokollierung von bestimmten Datenverarbeitungsvorgängen in automatisierten Verarbeitungssystemen. In Erweiterung der Vorgaben der Richtlinie (EU) 2016/680 wurde der Katalog in Nummer 1 um die Speicherung der Daten und in Nummer 6 um die Einschränkung der Verarbeitung ergänzt. Die Regelung erfasst unter anderem auch die Protokollierung automatisierter Datenübertragungen an Schnittstellen von Verfahren zu anderen Verfahren sowie Verarbeitungsvorgänge durch den Administrator. Ebenfalls erfasst wird die Protokollierung so genannter „lesender Zugriffe“, bei denen Informationen aus dem Verarbeitungssystem im Sinne des Artikels 25 Absatz 1 Satz 1 der Richtlinie (EU) 2016/680 abgefragt werden (vgl. Herbst, in: Kühling/Buchner, DS-GVO/BDSG, Artikel 4 DSGVO Rn. 27; Schaffland/Wiltfang, DS-GVO/BDSG, Artikel 4 DSGVO Rn. 74; nach anderer Auffassung handelt es sich bei dem lesenden Zugriff um einen Unterfall der Erhebung, vgl. Schild, in: BeckOK Datenschutzrecht, Artikel 4 DSGVO Rn. 47; Ernst, in: Paal/Pauly, DS-GVO/BDSG, Artikel 4 DSGVO Rn. 28).

Absatz 2 enthält konkrete Vorgaben für den Inhalt der Protokolle. Dem Erwägungsgrund Nummer 57 der Richtlinie (EU) 2016/680 lässt sich entnehmen, dass die Identität der Person, die personenbezogene Daten abgefragt oder offengelegt hat, protokolliert wird und sich daraus die Begründung für die Verarbeitungsvorgänge ableiten lassen sollte.

Absatz 3 Satz 1 befasst sich mit den Verwendungsbeschränkungen für Protokolldaten. Grundsätzlich dürfen die Protokolldaten nur zum Zwecke der Datenschutzkontrolle, Eigenüberwachung und Aufrechterhaltung der Datensicherheit verwendet werden. Die Protokollierung dient dem Schutz des Rechts auf informationelle Selbstbestimmung und ist eine den Grundrechtseingriff abmildernde Verfahrenssicherung. Unter engen Voraussetzungen dürfen die Protokolle nach Absatz 3 Satz 2 auch zur Verfolgung von Straftaten oder zur Einleitung beamtenrechtlicher oder disziplinarrechtlicher Maßnahmen im Zusammenhang mit einer Verletzung des Datengeheimnisses sowie zur Verfolgung von Straftaten von erheblicher Bedeutung verarbeitet werden. Die entsprechende Zweckänderung wird in Artikel 25 Absatz 2 der Richtlinie (EU) 2016/680 zugelassen.

Nach der Entscheidung des EuGH in der Rechtssache C-553/07 (EuGH, Urteil vom 7. Mai 2009, C-553/07) sind Protokolldaten für einen Zeitraum aufzubewahren, der es den betroffenen Personen ermöglicht, die Rechtmäßigkeit der Verarbeitung nachzuvollziehen. Das Bundesverfassungsgericht hat in seiner Entscheidung zum Bundeskriminalamtgesetz (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09) ausgeführt, dass durch technische und organisatorische Maßnahmen sichergestellt werden muss, dass die Proto-

kolldaten der oder dem Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben zu dem zu kontrollierenden Vorgang enthält. Angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle kommt ihrer regelmäßigen Durchführung besondere Bedeutung zu. Die Kontrollen sind in angemessenen Abständen – deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf – durchzuführen (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 141). Absatz 4 legt daher fest, dass die Protokolldaten erst zwei Jahre nach ihrer Generierung gelöscht werden, was eine effektivere Kontrolle der Verarbeitungsvorgänge ermöglicht.

Absatz 5 legt fest, dass die Protokolle der oder dem Landesdatenschutzbeauftragten zum Zweck der Datenschutzkontrolle zur Verfügung gestellt werden müssen. Die Vorschrift setzt Artikel 25 Absatz 3 der Richtlinie (EU) 2016/680 um.

Die Bestimmung tritt erst am 6. Mai 2023 in Kraft. Diesbezüglich wird von der entsprechenden Ermächtigung in Artikel 63 Absatz 2 der Richtlinie (EU) 2016/680 (Erwägungsgrund 96) Gebrauch gemacht.

Zu § 32e - Löschung

Absatz 1 normiert den Grundsatz der verpflichtenden Löschung personenbezogener Daten, soweit nicht einer der dort aufgezählten Ausnahmefälle gegeben ist.

Absatz 2 Satz 1 verpflichtet die Behörde jährlich zu überprüfen, ob personenbezogene Daten zu löschen sind. Satz 2 und 3 regeln den Beginn der Jahresfrist.

Absatz 3 entspricht § 32 Absatz 3 bis 5 des Gesetzes zur ambulanten Resozialisierung und Opferhilfe.

Zu § 32f - Einschränkung der Verarbeitung

Absatz 1 Satz 1 trägt Artikel 16 Absatz 3 der Richtlinie (EU) 2016/680 Rechnung, wonach anstelle der Löschung personenbezogener Daten aus bestimmten Gründen eine Einschränkung ihrer Verarbeitung möglich ist.

Nummer 1 trägt den hochrangigen Interessen der Gefahrenverhütung, Gefahrenabwehr und Strafverfolgung Rechnung, die durch die Richtlinie (EU) 2016/680 als Verarbeitungszwecke anerkannt werden.

Nummer 2 stellt sicher, dass Interessen des Landes und betroffener Personen nach der Entlassung der Probandinnen und Probanden aus dem Aufgabenbereich des Kompetenzzentrums der Justiz für ambulante Resozialisierung und Opferhilfe geltend gemacht und durchgesetzt werden können.

Nummer 3 setzt den Gedanken aus Nummer 2 fort, nach dem die Löschung die Durchsetzung von Rechten der betroffenen Personen nicht beeinträchtigen oder vereiteln darf (vgl. Erwägungsgrund Nummer 47 der Richtlinie (EU) 2016/680).

Nummer 4 setzt die Ausnahmeregelung des Artikels 16 Absatz 3 Buchstabe b) der Richtlinie (EU) 2016/680 um, der weit zu verstehen ist und damit auch als Auffangtatbestand zu den Nummern 1 bis 3 dient.

Nummer 5 sieht bei abweichenden gesetzlichen Aufbewahrungsfristen eine entsprechende Ausnahme von der Löschung vor.

Absatz 1 Satz 2 verpflichtet zur Dokumentation der Gründe der Einschränkung der Verarbeitung personenbezogener Daten.

Aufgrund des Ausnahmecharakters der Einschränkung der Verarbeitung personenbezogener Daten ist die Verarbeitung dieser Daten nur unter den in Absatz 2 Satz 1 genannten Voraussetzungen möglich und zulässig. Ist die Verarbeitung dieser Daten zu Zwecken, zu denen ihre Löschung unterblieben ist, nicht mehr erforderlich, sind diese Daten unverzüglich zu löschen. Die Regelung orientiert sich an dem Verhältnismäßigkeitsgebot der Richtlinie (EU) 2016/680 und § 32 Absatz 2 Satz 3 des Bundeskriminalamtsgesetzes.

Absatz 2 Satz 2 greift den Gedanken des Artikels 5 Satz 2 der Richtlinie (EU) 2016/680 auf, wonach durch verfahrensrechtliche Vorkehrungen sicherzustellen ist, dass Fristen eingehalten werden.

Absatz 3 sieht, neben der Einwilligung der betroffenen Personen in Nummer 1, in Nummer 2 den wichtigen Anwendungsfall für das Aufheben der Einschränkung der Verarbeitung personenbezogener Daten im Falle einer erneuten Unterstellung in den Kompetenzbereich des Kompetenzzentrums der Justiz für ambulante Resozialisierung und Opferhilfe vor. Die Behörde wird damit in die Lage versetzt, ohne Informationsverlust wieder an die vorherigen Maßnahmen anzuknüpfen. Auch ist der Rückgriff auf die bereits bestehenden Daten für die Probandinnen und Probanden regelmäßig weniger belastend als deren Neuerhebung. Wird die Einschränkung der Verarbeitung personenbezogener Daten wieder aufgehoben, richtet sich die Löschung dieser Daten erneut nach § 32e.

Absatz 4 Satz 1 stellt klar, dass auch in den Fällen, in denen die Verarbeitung personenbezogener Daten eingeschränkt ist, die Höchstgrenzen für die Aufbewahrung nicht überschritten werden dürfen und legt in Satz 3 den Fristbeginn fest. Satz 2 sieht gleichwohl eine Ausnahme von den Höchstgrenzen für die Aufbewahrung vor, wenn ein Fall des Absatzes 1 vorliegt, also konkrete Anhaltspunkte dafür vorliegen, dass die personenbezogenen Daten zur Strafverfolgung oder zur Behebung einer Beweisnot erforderlich sind.

Zu § 32g - Berichtigung

Die Regelung in Absatz 1 Satz 1 enthält eine Umsetzung des Grundsatzes aus Artikel 4 Absatz 1 Buchstabe a und d in Verbindung mit Artikel 7 Absatz 2 der Richtlinie (EU) 2016/680, wonach personenbezogene Daten zu berichtigen sind, wenn sie unrichtig, unvollständig oder nicht mehr aktuell sind.

Absatz 1 Satz 2 übernimmt den in Erwägungsgrund Nummer 47 der Richtlinie (EU) 2016/680 enthaltenen Gedanken. Zur Vorbeugung massenhafter und nicht erfolgsversprechender Anträge ist es geboten, klarzustellen, dass sich das Berichtigen auf die betroffene Person betreffende Tatsachen bezieht und nicht etwa auf den Inhalt von Zeugenaussagen, Beurteilungen oder Entscheidungen.

Absatz 1 Satz 3 setzt Artikel 4 Absatz 1 Buchstabe d, 1. Halbsatz, der Richtlinie (EU) 2016/680 um.

Absatz 1 Satz 4 übernimmt § 20 Absatz 1 Satz 2 des Bundesdatenschutzgesetzes in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 10 Absatz 2 des Gesetzes vom 31. Oktober 2017 (BGBl. I S. 3618) geändert worden ist und konkretisiert diesen.

Nach Absatz 1 Satz 5, der Artikel 16 Absatz 1 Satz 2 der Richtlinie (EU) 2016/680 umsetzt, kann die betroffene Person die Vervollständigung ihrer unvollständigen personenbezogenen Daten auch durch eine ergänzende Erklärung verlangen. Dies dürfte zur Wahrung der Aktenklarheit und Aktenwahrheit auch für sonstige Berichtigungen gelten.

Absatz 2 regelt einen weiteren Fall der Einschränkung der Verarbeitung. Artikel 16 Absatz 3 Buchstabe a der Richtlinie (EU) 2016/680 sieht in der (berechtigten) Berichtigung von unrichtigen Daten einen Unterfall der Löschung. In Anlehnung an § 58 Absatz 1 Satz 3 und 4 des Bundesdatenschutzgesetzes in der Fassung seiner Bekanntmachung vom 30. Juni 2017 soll der Fall der Löschung wegen Berichtigung unrichtiger Daten hier systematisch als Fall der Berichtigung erfasst werden. Die Aufhebung der Einschränkung der Verarbeitung nach Satz 2 führt daher entweder zur Berichtigung der Daten oder deren uneingeschränkter Verarbeitung.

Zu § 32h - Rechte der betroffenen Person auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

Absatz 1 dient der Umsetzung von Artikel 16 Absatz 1 der Richtlinie (EU) 2016/680.

Satz 1 setzt das in Artikel 16 Absatz 1 der Richtlinie (EU) 2016/680 gewährte Recht auf Berichtigung unrichtiger bzw. auf Vervollständigung unvollständiger Daten um. Satz 2 setzt Artikel 16 Absatz 3 Satz 2 um.

Absatz 2 setzt – in Verbindung mit § 32e – die Vorgaben des Artikels 16 Absatz 2 der Richtlinie (EU) 2016/680 um.

Absatz 3 dient der Umsetzung des Verfahrens von Artikel 16 Absatz 4 der Richtlinie (EU) 2016/680 und betrifft das zur Anwendung kommende Verfahren, wenn der Verantwortliche einem Antrag auf Berichtigung oder Löschung nicht oder nur eingeschränkt nachkommt.

Zu § 32i - Mitteilungen

Die in dieser Vorschrift enthaltene Verpflichtung setzt Artikel 7 Absatz 3 und Artikel 16 Absatz 5 und 6 der Richtlinie (EU) 2016/680 um.

Absatz 1 Satz 1 sieht vor, die Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten auch anderen Stellen, an die diese Daten zuvor übermittelt wurden, zur Kenntnis zu geben, um so die Richtigkeit der Daten bei weiteren Übermittlungsvorgängen zu gewährleisten.

Die in Satz 2 geregelte Verpflichtung des Empfängers, die Berichtigung im eigenen Datenbestand vorzunehmen, folgt aus deren eigener Verantwortung, unrichtige Daten unverzüglich zu berichtigen.

Absatz 2 dient der Umsetzung von Artikel 5 Satz 2 der Richtlinie (EU) 2016/680.

Zu Artikel 6

Zu Nummer 1:

Nach Satz 6 des § 2 Absatz 3 des Gesetzes sollen mindestens zwei Mitglieder und deren Stellvertreter/Stellvertreterinnen Berufsrichter/Berufsrichterinnen sein und einem oberen Landesgericht angehören. Diese Vorgabe wird dahingehend geändert, dass in Übereinstimmung mit den Verfassungsgerichtsgesetzen anderer Länder zwar weiterhin ein Mindestquorum an Berufsrichterinnen oder Berufsrichtern vorgesehen ist, dieses künftig jedoch nicht mehr an die Zugehörigkeit zu einem oberen Landesgericht geknüpft wird.

Zu Nummer 2:

Derzeit nimmt § 14a Bezug auf die Vorschriften des Saarländischen Datenschutzgesetzes. Für die Zulässigkeit der Verarbeitung von personenbezogenen Daten gelten nunmehr die Vorschriften der Datenschutz-Grundverordnung unmittelbar und daneben weiterhin die ergänzenden allgemeinen Datenschutzvorschriften des nationalen Rechts, im Saarland also das Saarländische Datenschutzgesetz. Dem trägt die Erweiterung der Bezugnahme auf „die allgemeinen datenschutzrechtlichen Vorschriften“ in § 14a Rechnung.

Zu Nummer 3:

Die Regelung in § 14b betreffend die Gewährung von Auskünften oder Akteneinsicht an Nichtverfahrensbeteiligte ist in ihren Verweisungen an das neu erlassene Saarländische Datenschutzgesetz anzupassen, um den Gleichklang mit der Parallelregelung in § 35b des Bundesverfassungsgerichtsgesetzes zu wahren.

Eine Gewährung von Auskunft oder Akteneinsicht gegenüber öffentlichen Stellen ist danach unter den Voraussetzungen des § 14b Absatz 1 Satz 1 Nummer 1 aus folgenden Anlässen zulässig:

- Erfordernis für Zwecke der Rechtspflege (§ 14b Absatz 1 Satz 1 Nummer 1 Buchstabe a des Gesetzes über den Verfassungsgerichtshof),
- Erfordernis zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit (§ 14b Absatz 1 Satz 1 Nummer 1 Buchstabe b des Gesetzes über den Verfassungsgerichtshof i.V.m. § 7 Absatz 2 Nummer 1 des Saarländischen Datenschutzgesetzes),
- Erfordernis zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person (§ 14b Absatz 1 Satz 1 Nummer 1 Buchstabe b des Gesetzes über den Verfassungsgerichtshof i.V.m. § 7 Absatz 2 Nummer 2 des Saarländischen Datenschutzgesetzes),
- Erfordernis zur Überprüfung der Angaben der betroffenen Person, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen (§ 14b Absatz 1 Satz 1 Nummer 1 Buchstabe b des Gesetzes über den Verfassungsgerichtshof i.V.m. § 7 Absatz 2 Nummer 3 des Saarländischen Datenschutzgesetzes),
- Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten, die eine Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden geboten erscheinen lassen (§ 14b Absatz 1 Satz 1 Nummer 1 Buchstabe b des Gesetzes über den Verfassungsgerichtshof i.V.m. § 7 Absatz 2 Nummer 4 des Saarländischen Datenschutzgesetzes),
- Erfordernis für Zwecke der wissenschaftlichen Forschung (§ 14b Absatz 1 Satz 1 Nummer 1 Buchstabe c des Gesetzes über den Verfassungsgerichtshof).

Die Gewährung von Auskunft oder Akteneinsicht gegenüber Privatpersonen und anderen nicht öffentlichen Stellen nach § 14b Absatz 1 Satz 1 Nummer 2 entspricht der bisherigen Regelung, wobei die Voraussetzungen der Gewährung sich nunmehr aus einer Bezugnahme auf den neuen § 4 Absatz 3 Nummer 2 des Saarländischen Datenschutzgesetzes ergeben.

Die in Satz 2 des § 14b Absatz 1 bereits enthaltene Variante, wonach Auskunft oder Akteneinsicht auch gewährt werden kann, soweit die Betroffenen eingewilligt haben, bleibt unverändert.

Gleichfalls verbleibt es bei der Ausgestaltung des § 14b Absatz 1 als Ermessensvorschrift („kann“), „um es dem Verfassungsgerichtshof zu ermöglichen, über rein datenschutzrechtli-

che Belange hinausgehende Überlegungen hinsichtlich der Interessen der Verfahrensbeteiligten oder des Gerichts selbst in die Abwägung einzubeziehen“ (LT-Drs. 12, 134, S. 6).

Zu Nummer 4:

Die Ersetzung des Wortes „nutzen“ durch „verarbeiten“ dient der Anpassung an die datenschutzrechtliche Begrifflichkeit, ohne dass hiermit eine sachliche Änderung der Rechtslage einhergeht.

Zu Artikel 7

Absatz 1 regelt das Inkrafttreten dieses Gesetzes sowie das Außerkrafttreten der jeweiligen datenschutzrechtlichen Bestimmungen in den saarländischen Vollzugsgesetzen.

Absatz 2 schafft eine Übergangsregelung für die nach Artikel 25 Absatz 1 der Richtlinie (EU) 2016/680 erforderlichen Protokollierungspflichten bei automatisierten Verarbeitungssystemen und macht damit von der entsprechenden Ermächtigung in Artikel 63 Absatz 2 der Richtlinie (EU) 2016/680 (Erwägungsgrund 96) Gebrauch, die in Ausnahmefällen, in denen die Umstellung der vor dem Inkrafttreten der Richtlinie bereits eingerichteten automatisierten Verarbeitungssysteme mit einem unverhältnismäßigen Aufwand – wie im Verfahren BASIS-Web oder SoPart – verbunden ist, ein Verschieben des Inkrafttretens bis zum 6. Mai 2023 gestattet. Die Verfahren BASIS-Web oder SoPart werden bereits seit mehreren Jahren im Saarland genutzt.

Die Pflicht zur Protokollierung von bestimmten Datenverarbeitungsvorgängen in automatisierten Verarbeitungssystemen in § 42 Justizvollzugsdatenschutzgesetz erfordert eine umfangreiche ergänzende Programmierung des Datenverarbeitungssystems im Justizvollzug BASIS-Web. Das System wird in mehreren Bundesländern eingesetzt und von einem Entwicklerverbund betreut. Vergleichbares gilt für § 32 d des Gesetzes zur ambulanten Resozialisierung und Opferhilfe und das Datenverarbeitungssystem SoPart, welches im Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe zum Einsatz kommt.